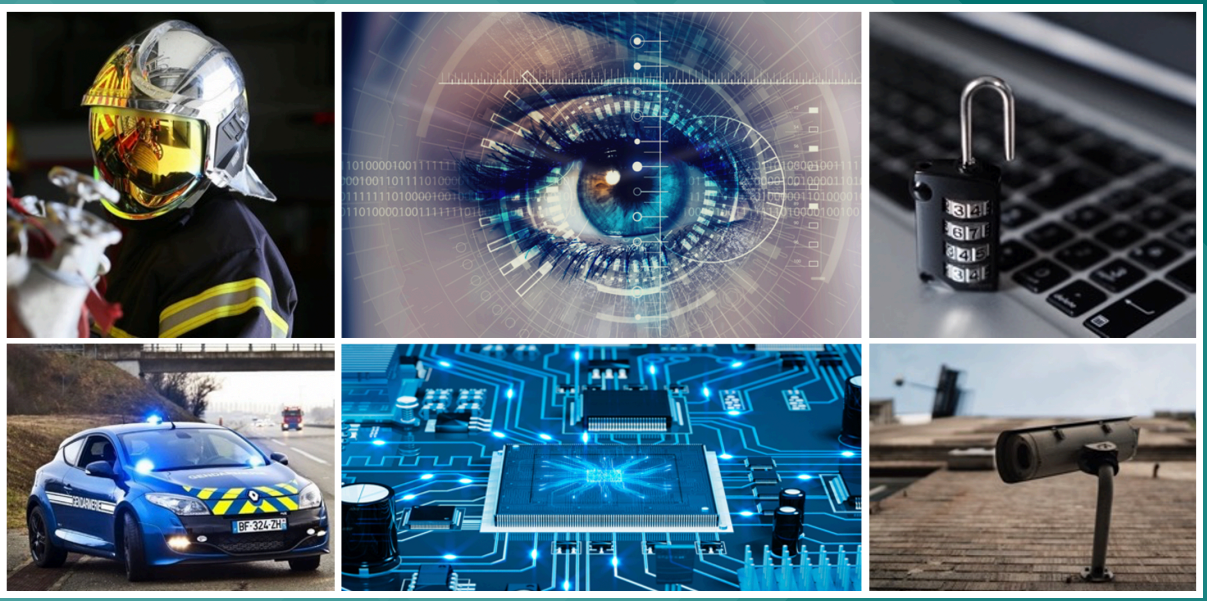
Observatoire de la Filière Industrielle de Sécurité

Juin 2020



CICS
Conseil des Industries de la Confiance et de la Sécurité

GICAT

conseil national de l'industrie

SGDSN

DMISC
Délégation Ministérielle aux Industries de Sécurité et à la Lutte contre les Cybermenaces

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES

Etude commanditée par le

Conseil des Industries de la Confiance et de la Sécurité (CICS)

CICS
Conseil des Industries
de la Confiance et de la Sécurité

11-17 rue de l'amiral Hamelin
75116 Paris
www.cics-org.fr

Etude réalisée par

DECISION Etudes & Conseil

DECISION
ETUDES & CONSEIL

11-17 rue de l'amiral Hamelin
75116 Paris
www.decision.eu

Avant-propos

La **filière industrielle de sécurité** est cruciale dans notre économie et dans notre société en pleine mutation numérique. Elle regroupe la **sécurité physique** (véhicules et plateformes, vêtements de protection, équipements et fourniture - y compris et sécurité incendie - outils d'interdiction physique d'accès)**, la sécurité électronique et numérique** (identité numérique, systèmes et sous-systèmes électroniques de confiance, de sécurité incendie, de surveillance, communication, traçage…), ainsi que la **cybersécurité** (produits / logiciels et services).

Le **CSF des Industries de Sécurité** a été constitué afin d'instaurer un dialogue concret, performant et régulier entre l'Etat, les entreprises et les représentants des salariés sur tous les sujets-clés qui permettront la reconquête de l'industrie française.

L'**Observatoire de la filière industrielle de sécurité** a pour objectif d'analyser et de mettre en commun le périmètre, le poids économique ainsi que les principales tendances de cette filière. Une précédente version de cet Observatoire a été réalisée en 2018 par DECISION Etudes & Conseil.

Sommaire

Éléments clefs

La filière industrielle de sécurité en France en 2018 c'est :

- **28,2 milliards d'euros de chiffre d'affaires**, soit 4,9% de croissance annuelle moyenne entre 2016 et 2018
- **11 milliards d'euros de valeur ajoutée**
- Un total de **139 100 employés**
- Un CA réparti à **44% pour la Sécurité électronique, 33% pour la Sécurité physique et 23% pour la Cybersécurité**

Les entreprises industrielles françaises de la sécurité représentent dans le Monde en 2018

- **36,4 milliards d'euros de chiffre d'affaires**
  (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 électronique (Thales, Airbus D&S), de la gestion des identités et des accès (Thales, Idemia), des plateformes de sécurité (Naval Group, Airbus Helicopters, Dassault Aviation), des services de cybersécurité (Thales, Atos, Orange Cyberdefense, Cap Gemini, Sopra Steria), et de la sécurisation des paiements (Atos).
- **22,4 milliards d'euros de chiffre d'affaires à l'international**, soit environ **60%** du CA total
  (CA exporté depuis la France et CA réalisé à l'étranger par des entreprises détenues par des capitaux français)
- **14 milliards d'euros de chiffre d'affaires à l'export**, soit environ **50%** du CA total

La filière industrielle de sécurité est une des filières qui bénéficie des meilleurs perspectives de croissance pour les années à venir

- **5,5%** de croissance annuelle moyenne en France sur la période 2014-2019, contre **1,4%** pour le PIB français
- Parmi les filières industrielles françaises, **c'est la filière industrielle de sécurité qui bénéficie de la croissance la plus forte**
- **La croissance annuelle moyenne de la filière est au dessus des 5% depuis 10 ans et cette tendance devrait se maintenir sur la période 2018-2023** (sauf en 2020 du fait du COVID-19) grâce à ses nombreuses innovations technologiques, aux événements d'envergure à venir en France (coupe du monde de rugby 2023 et Jeux Olympiques 2024) et à son fort taux d'exportation
- La filière a réalisé **29,7 milliards d'euros de chiffre d'affaires en 2019 (estimations).**

La filière industrielle de sécurité regroupe un écosystème d'entreprises de toutes tailles

- **4 440 entreprises** dans la filière en France
- Dont **95 grandes entreprises**
- Dont **118 ETI** (Entreprises de Taille Intermédiaire)
- Dont **1 817 PME** (Petites et Moyennes Entreprises)
- Dont **2 410 micro-entreprises**, générant moins de 2 millions de CA en 2018

Éléments clefs

FONDAMENTAUX 2018

CA MONDE	36,4 MDS €
CA HORS DE FRANCE	8,3 MDS €
CA FRANCE	28,2 MDS €
DONT CA EXPORT	14,1 MDS €
DONT CA ENTREPRISES FRANÇAISES	21,2 MDS €
VA FRANCE	11,1 MDS €
MARCHÉ FRANÇAIS	~24 MDS €

Source : DECISION Etudes & Conseil

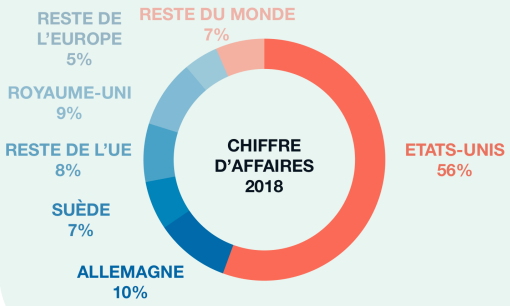
CROISSANCE 2016-2018

4,9%

139 100
EMPLOIS EN FRANCE

LES ENTREPRISES ÉTRANGÈRES PRÉSENTES EN FRANCE

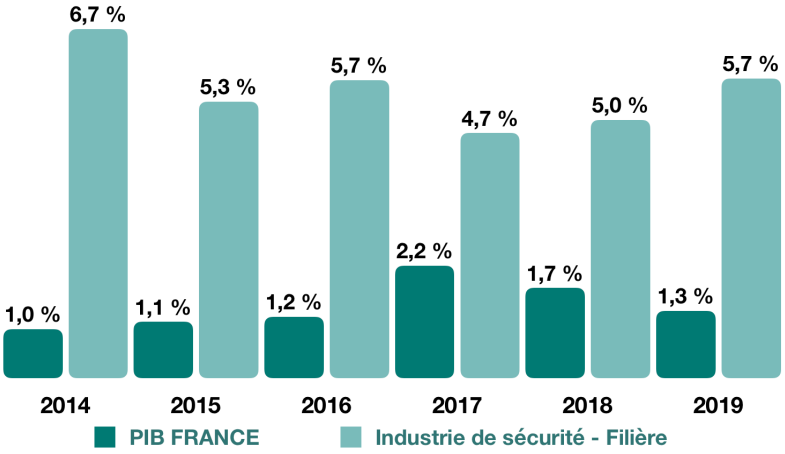
L'activité des entreprises de capitaux étrangers présentes en France correspond à 25% du CA FRANCE produit par la filière en 2018. Le diagramme ci-dessous montre la répartition de cette activité par nationalité.



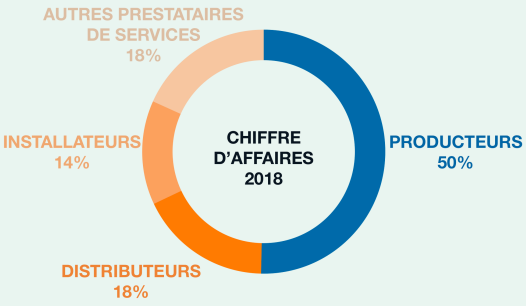
Source : DECISION Etudes & Conseil

CROISSANCES COMPARÉES 2014-2019

Source : DECISION Etudes & Conseil

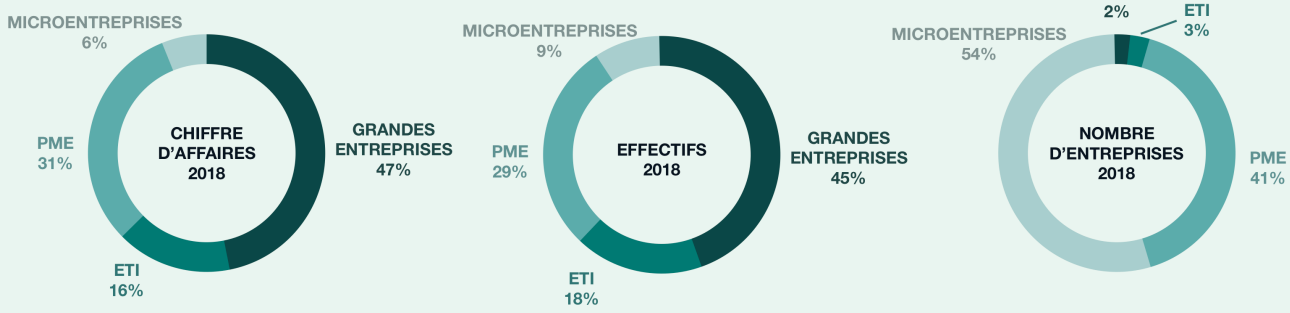


ANALYSE PAR TYPE D'ENTREPRISES



Source : DECISION Etudes & Conseil

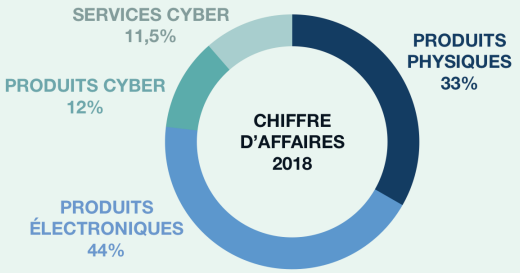
ANALYSE PAR TAILLE D'ENTREPRISES

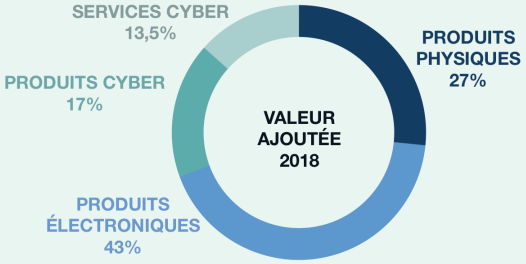


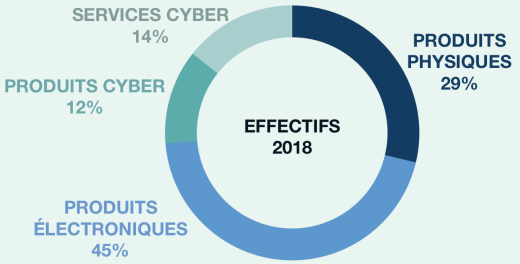
Source : DECISION Etudes & Conseil

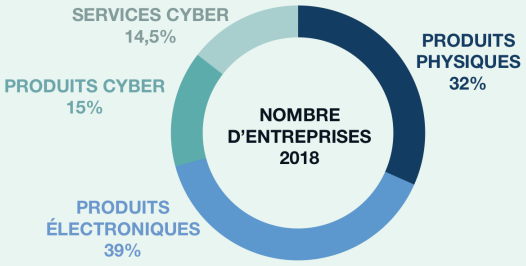
Éléments clefs

LES PRINCIPAUX SEGMENTS DE L'INDUSTRIE DE SÉCURITÉ





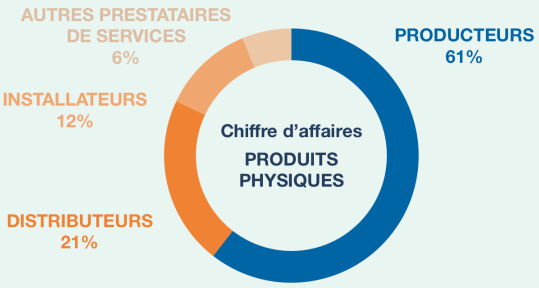


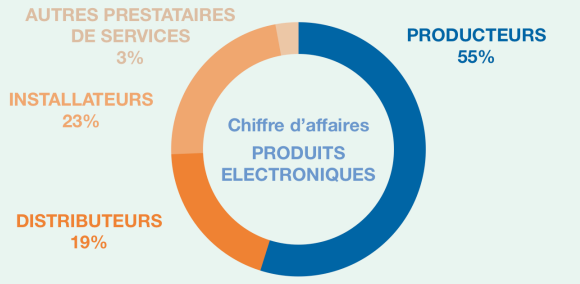


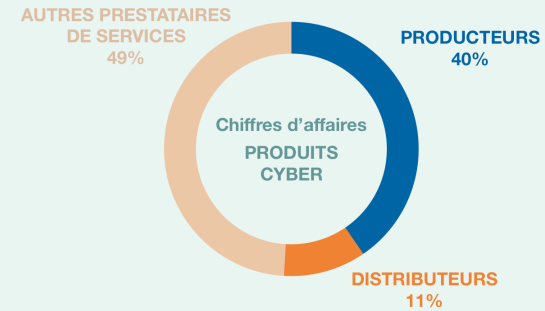
Source : DECISION Etudes & Conseil

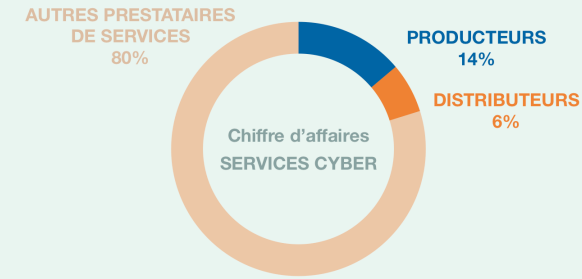
Il s'agit du nombre d'entreprises présentes sur le segment

TYPES D'ENTREPRISES SELON LES PRINCIPAUX SEGMENTS DE L'INDUSTRIE DE SÉCURITÉ





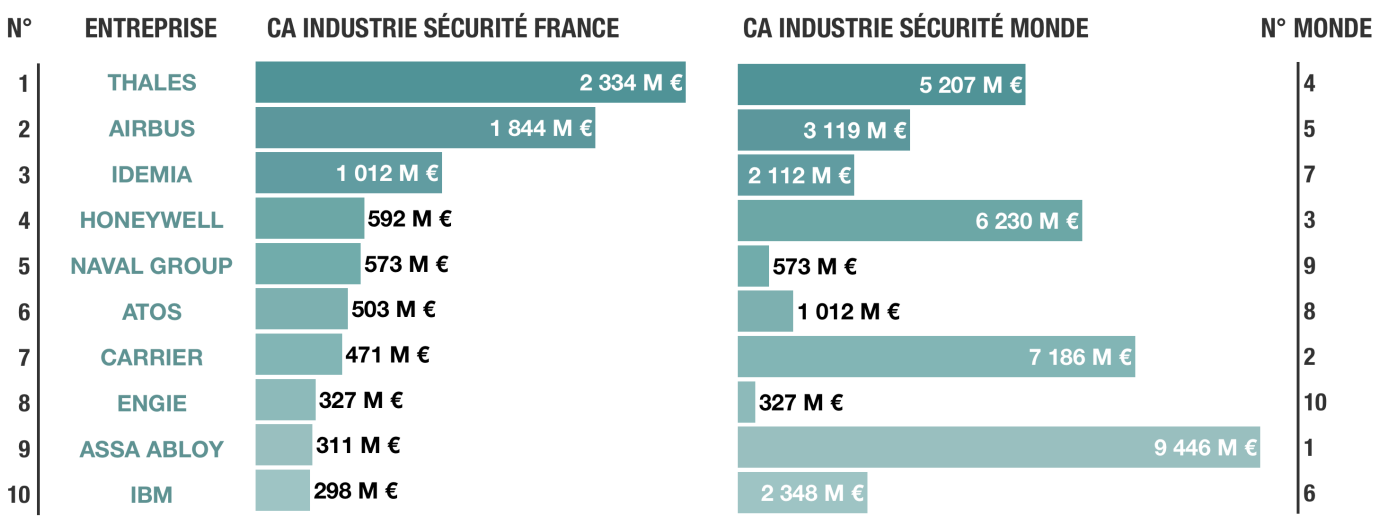




Source : DECISION Etudes & Conseil

Éléments clefs

TOP 10 ACTEURS FRANCE - 2019



Source : DECISION Etudes & Conseil

N°	TOP 10
1	**Thales** est le leader français de la sécurité à travers son activité historique *Thales Défense et Sécurité* mais aussi son activité *Thales Identité & Sécurité Numériques* devenue leader mondial en identité et sécurité numériques depuis l'acquisition de Gemalto (finalisée en 2019). Les principaux segments sur lesquels Thales est présent sont le contrôle d'accès, l'identification des personnes, l'observation locale et large zone, les communications sécurisées et la cybersécurité. Thales est notamment le leader des solutions de contrôle d'accès dans les aéroports français. Les chiffres de Thales incluent notamment ceux d'ERCOM et de Lynred (Joint Venture avec Safran regroupant les sociétés ULIS et Sofradir).
2	**Airbus** fort de sa position de leader mondial sur le segment des hélicoptères civils est le leader français sur le segment des hélicoptères de sécurité à travers sa filiale Airbus Helicopters. Airbus est également présent sur de nombreux segments de la filière à travers Airbus Defense & Space : principalement les communications sécurisées, le contrôle d'accès et la cybersécurité, mais aussi les outils électroniques de renseignement et de collecte d'information, les systèmes d'observation locale et large zone (capteurs, radars, imagerie satellite), les drones, les équipements de détection pour les produits dangereux (avec SODERN), et les dispositifs d'étiquetage et de traçage. Airbus D&S est également le leader français sur les systèmes de protection des frontières terrestres.
3	**Idemia** est la société formée en 2018 suite au rachat et à la fusion par le fond américain Advent International des deux entreprises françaises Safran Morpho et Oberthur Technologies. Idemia est avec Thales le leader français des solutions d'identification et d'authentification des personnes. Idemia a racheté Otono Networks en 2018.
4	**Honeywell** (Etats-Unis) est fortement présent en France et est l'un des leaders sur les segments des EPI*, de la détection d'intrusion et alarmes, du contrôle d'accès et de la sécurité incendie.
5	**Naval Group** est le leader français sur le segment des navires de sécurité, notamment à travers sa Joint-Venture Kership fondée en 2013 avec Piriou, mais également à travers son activité de construction de frégates et de patrouilleurs dédiés à des missions de sécurité (notamment pour la Marine française à travers la PPSM). Naval Group développe aussi des activités de cybersécurité significatives. Le CA depuis la France de l'entreprise est particulièrement important car son activité mondiale s'effectue intégralement depuis la France et est exportée par la suite.
6	**Carrier** (Etats-Unis) est un leader mondial des équipements de chauffage & climatisation et est très présent sur le segment de la sécurité incendie. Carrier appartenait jusqu'en 2019 au conglomérat américain UTC qui s'en est séparée dans le cadre de sa fusion avec Raytheon. Carrier est fortement implanté en France à travers la marque Chubb, mais aussi suite au rachat du groupe Vulcain en 2016. Chubb Delta fournit également des solutions de protection électronique des personnes et des biens.
7	**Atos** est l'un des leaders français de la cybersécurité avec Thales, Idemia, Orange Cyberdefense et IBM. Atos est notamment le leader de la sécurisation des paiements avec Atos Worldline. Atos a racheté Air-Lynx en 2018 et Idnomic en 2019.
8	**ENGIE Solutions**, créée début 2020, regroupe notamment les activités d'ENGIE dédiés à la sécurité et anciennement opérées par les marques Cofely, Ineo et Axima. ENGIE est présent sur les segments de la sécurité incendie ainsi qu'en matière d'installation d'alarmes anti-intrusion, de caméras et d'outils de contrôle d'accès.
9	**ASSA ABLOY** (Suède) est un leader mondial des solutions d'interdiction et de contrôle d'accès, physique et électronique. Assa Abloy a racheté le Suisse Nergeco en 2019. Le CA d'Assa Abloy inclut aussi ceux de Portafeu et de Nergeco.
10	**IBM** est un leader mondial en matière de cybersécurité et de confiance numérique.

* EPI : Equipements de Protection Individuels

TOP 10-20 : Ces acteurs réalisent un CA Industrie de sécurité compris entre 180 M € et 272 M €
TOP 20-30 : Ces acteurs réalisent un CA Industrie de sécurité compris entre 120 M € et 180 M €
Source : DECISION Etudes & Conseil

N°	TOP 10-30
11	**Orange Cyberdefense** est parmi les principaux acteurs français de la filière celui qui bénéficie de la croissance la plus fulgurante (>50%/an en moyenne depuis 2013)
12	**Desautel** est l'un des leaders français sur le segment de la sécurité incendie et des véhicules terrestres de sécurité à travers les marques Gallin, Socodes et Gimaex
13	**Groupe RG** est l'un des leaders français sur le segment des EPI*
14	**Safran** garde une activité de sécurité significative depuis la vente de sa filiale Morpho en 2017 (devenue Idemia), notamment en observation large zone et à travers sa Joint Venture Lynred
15	**Descours & Cabaud** est l'un des leaders français sur le segment des EPI*
16	**Somfy** est l'un des leaders français des solutions d'interdiction et de contrôle d'accès, physique et électronique (détection et alarme anti-intrusion, etc.)
17	**Siemens** (Allemagne) est fortement implanté en France sur le segment de la sécurité incendie. Siemens fourni également des systèmes de contrôle d'accès et d'alarme
18	**La DEF** est l'un des leaders français sur le segment des EPI*
19	**IN Groupe** (ex Imprimerie Nationale) est l'un des leaders français de l'identité numérique et a racheté Surys en 2019
20	**Cap Gemini** est l'un des leaders français des services de cybersécurité. Les rachats d'Altran et de l'américain Leidos Cyber en 2019 ont étoffé son offre de sécurité
21	**Sopra Steria** est l'un des leaders français des services de cybersécurité et a racheté Kentor en 20117, Bluecarat en 2018 et Sodifrance en 2020
22	**Hager Groupe** (Allemagne) fournit des solutions de sécurité incendie, de contrôle d'accès, de vidéosurveillance ainsi que des alarmes anti-intrusion
23	**Stanley Security** (Etats-Unis) fournit des solutions de sécurité incendie, de contrôle d'accès, de vidéosurveillance ainsi que des alarmes anti-intrusion
24	**Fichet Group** (Etats-Unis) fournit des solutions de contrôle d'accès, de vidéosurveillance et d'alarmes anti-intrusion mais aussi des coffres-forts et des protes et cloisons de sécurité. Le groupe Fichet, historiquement français, a été racheté par le suédois Gunnebo en 1999 puis revendu au fond américain OpenGate Capital en 2019
25	**Delta Plus** est l'un des leaders français sur le segment des EPI*
26	**CNIM** est présent sur de nombreux segments de la filière (véhicules de sécurité, électronique, cybersécurité), notamment à travers sa filiale Bertin Technologies
27	**Vinci Energie** est l'un des leaders français de la sécurité incendie avec Uxello et grâce notamment aux rachats de Tunzini, Protec Feu, Lefort et Profab
28	**Oberthur Fiduciaire** est le leader français de la production de billets de banque et l'un des principaux acteurs en matière de documents sécurisés
29	**France Sécurité** (Royaume-Uni) est l'un des leaders français sur le segment des EPI*
30	**Mirion Technologies** (Etats-Unis) est spécialisé dans la détection NRBCE. Mirion fournit également des cameras, alarmes et EPI associés à la lutte NRBCE. En 2016, Areva a lui a cédé sa filiale Canberra, spécialisée dans les instruments de détection et de mesure de radioactivité (1000 salariés).

* EPI : Equipements de Protection Individuels

Parmi les principaux acteurs de la filière, on trouve également Novoferm, Malerba, Accenture, Sogetrel, Econocom, Tessi, SPIE, Volvo (avec notamment la marque Arquus), Worldwide Europe Protection, le Groupe CS, Atlantique Automatisme Incendie, Amphenol, Nokia, GFI Informatique, DOM security, Betafence, Nexecur, Bureau Veritas…

I) Présentation de la filière

1.1 Sécurité physique, électronique et cybersécurité : trois domaines complémentaires et de plus en plus inter-corrélés

La filière des industries des sécurité regroupe l'ensemble des entreprises qui développent des produits et des services technologiques de sécurité pour répondre aux malveillances et menaces croissantes et diversifiées, tant physiques que numériques.

La filière couvre un périmètre technologique large afin de répondre aux enjeux de sécurité dans toutes ses dimensions : cybersécurité, protection des infrastructures et des réseaux, sécurité du transport, secours aux personnes, lutte contre le terrorisme et la grande criminalité, sécurité des territoires, et gestion de crise.

La filières industries de sécurité recouvre trois industries :

- La **Sécurité physique**, c'est-à-dire les produits dont la valeur ajoutée est principalement constituée d'éléments physiques : depuis les véhicules et plateformes de sécurité (voitures, camions, navires, avions, hélicoptères, robots, drones, etc.), jusqu'aux équipements physiques de sécurité incendie (extincteurs, sprinklers, etc.), en passant par les vêtements de protection (EPI). De nombreux produits physiques de sécurité intègrent des composantes électroniques (boules optroniques installées sur les avions, capteurs installés sur les drones par exemple) et des composantes de cybersécurité (à l'image des frégates de NAVAL Group conçues pour résister aux attaques informatiques, avec des défenses passives et actives, le tout géré par un système de gestion de la cybersécurité rendu possible grâce à des data centers embarqués). Le segment des véhicules et plateformes de sécurité est celui qui intègre le plus d'éléments électroniques et cyber, ce qui explique en partie le faible niveau de valeur ajoutée de la sécurité physique.
- La **Sécurité électronique**, c'est-à-dire les produits dont la valeur ajoutée est principalement constituée d'éléments électronique : depuis les systèmes de contrôle d'accès (portiques, verrouillage électronique, etc.), jusqu'aux systèmes de communication sécurisées (téléphones sécurisés type Teorem, Hoox ou encore PMR, etc.), en passant par les alarmes anti-intrusion. Les produits électroniques de sécurité intègrent presque toujours une composante physique. Le segment du contrôle d'accès est sans doute celui pour lequel la composante physique est la plus importante (bien que largement minoritaire), car il englobe les systèmes complets de contrôle d'accès (y compris les portiques physiques de sécurité, tourniquets associés, etc.). Enfin, une partie significative de la sécurité électronique consiste non pas en la production ou la distribution de biens, mais en des services d'installation sur site des systèmes électroniques (systèmes de lutte anti-incendie, de vidéosurveillance, d'alarme anti-intrusion, etc.).
- La **Cybersécurité** proprement dite, qui correspond à la sécurisation logique 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 associées (anti-virus, pare-feux, etc.). Plusieurs produits cyber ont aussi une composante physique et électronique (salles, data-centers, etc.).

Ces produits et services sont destinés aussi bien aux marchés professionnels (état et secteur public, installations critiques, entreprises, PME) que grand public (ordinateurs, smartphones, maison, véhicules et objets connectés, etc).

Produits physiques

Véhicules terrestres
Véhicules de police, d'incendie, blindés

Avions et hélicoptères

Navires

Plateformes robotiques
Robots terrestres, marins et drones

Vêtements de protection
Equipements de Protection Individuelle (EPI). Vêtements d'intervention, tenues NRBC, casques, chaussures, masques à gaz…

Equipements et fournitures
Armes, munitions, outils de déminage, de décontamination…

Interdiction physique d'accès
Clôtures, enceintes, serrurerie, coffres forts, portes blindées et coupe-feu, vitres anti-effraction…

Equipements physiques de sécurité incendie
Extincteurs, sprinklers, désenfumage, lances, tuyaux, robinets…

Produits électroniques

Contrôle d'accès
Systèmes complets

Identification & Authentification des personnes
Biométrie, cartes à puces, badges, cartes ID, reconnaissance de véhicules, lutte contre la contrefaçon

Identification & Authentification des produits
Papiers sécurisés, billets de banque…

Détection d'intrusion et alarme

Equipements électroniques de sécurité incendie
Détection, alarme…

Détection de produits dangereux
ou illicites ou de personnes dissimulées : NRBCE, scanner, diffraction X, tomographes, spectromètres…

Observation locale
Caméras et capteurs (visibles et IR, acoustique…), lidars, radars, sonars…

Observation large zone
Systèmes optroniques, radars, imagerie par satellite

Traçage et localisation
Etiquetage et traçage (RFID, code barres, Wi-Fi…), systèmes AIS, LRIT, scellements électroniques avec suivi et positionnement (GPS, RFID), etc.

Communications sécurisées
et systèmes d'alerte publique (PMR, SAIP…)

Commande contrôle Aide à la décision
Y compris shelters, postes de commandements, outils de gestion de l'information, outils de simulation, de modélisation, de cartographie…

Renseignement et Collecte d'information
Interception, écoute, localisation, analyse et visualisation des données (big data)…

Cybersécurité

Produits / Logiciels

Gouvernance cyber
Systèmes de gestion, SIEM

Gestion des identités et des accès

Sécurité des données
Chiffrement, cryptographie, signature numérique, infrastructures à clés publiques, gestion des droits numériques, filtrage des contenus, archivage sécurisé, récupération de données

Sécurité des applications
Développement logiciels, OS sécurisés

Sécurité des infrastructures
Firewalls, antivirus, anti-dos, détection d'intrusion

Sécurité des produits & équipements

Services

Audit, planning et conseil cyber

Mise en oeuvre cyber

Sécurisations de l'infogérance exploitation

Formation cyber

I) Présentation de la filière

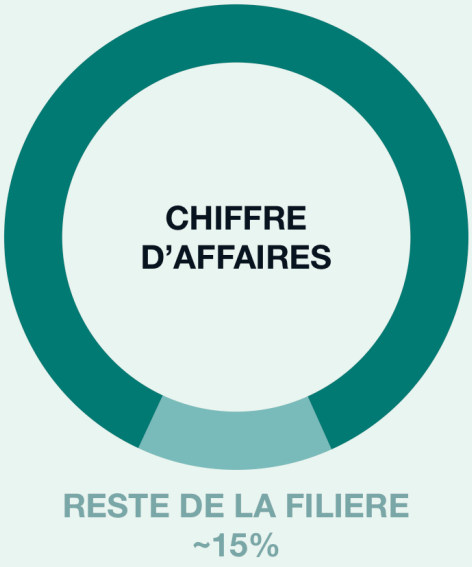
1.2 Méthodologie

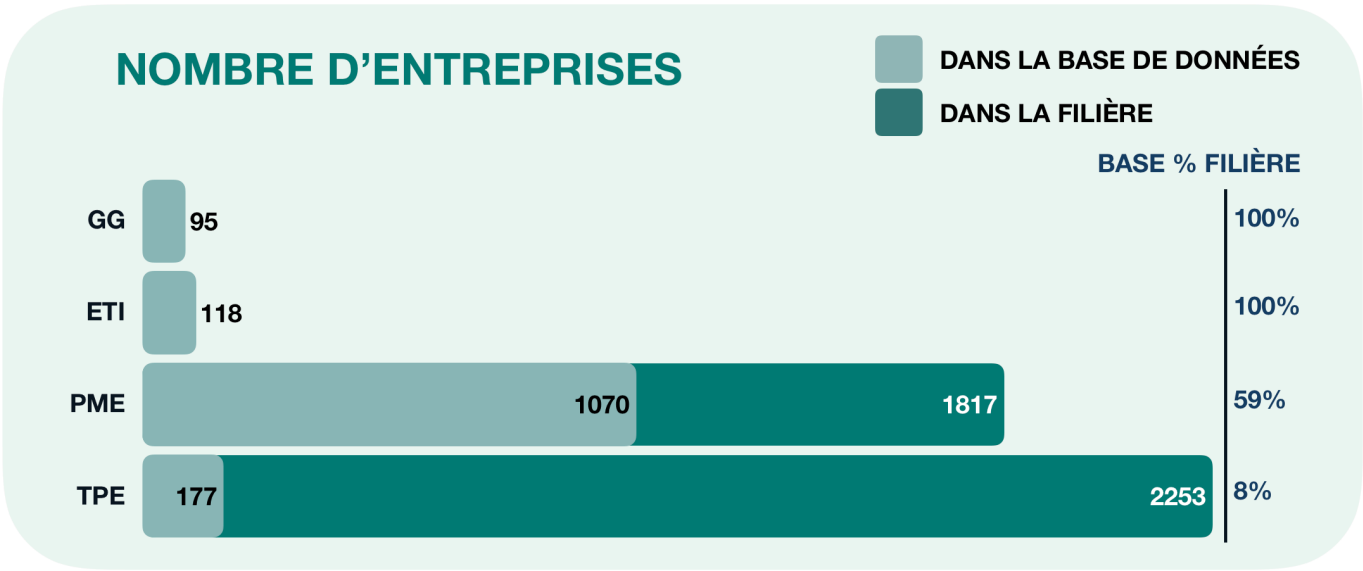
L'objectif de l'Observatoire est à la fois de définir le périmètre de la filière de l'industrie de sécurité, d'en évaluer le poids économique, de déterminer ses caractéristiques et d'analyser son évolution.

Les données présentées dans ce rapport sont issues d'une base de données recensant 1 460 entreprises parmi les 4 065 que compte la filière industrielle de sécurité. Cette base de données prend en compte :

- La totalité des grand groupes de la filière (95/95) ;
- La totalité des entreprises de tailles intermédiaires (ETI) de la filière (118/118) ;
- La majorité des PME de la filière (1 070 / 1 817) ;
- Les micro-entreprises et start-ups les plus remarquables et innovantes (177 / 2 253).

Ainsi, bien que seul 36% 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 industrielle de sécurité en France.





- **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

I) Présentation de la filière

EVOLUTIONS PAR RAPPORT AU PRÉCÉDENT OBSERVATOIRE

- Le segment des services privés de sécurité n'est plus analysé dans cet Observatoire qui se concentre uniquement sur l'industrie de sécurité en France.
- 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 sécurité et de mieux les segmenter. En conséquence de ces évolutions, **les chiffres de l'Observatoire 2020 ne sont pas directement comparables avec ceux de l'Observatoire précédent**. Les chiffres de cet Observatoire sont en année de base 2018 et en fonction de la nouvelle segmentation des acteurs. Les chiffres 2016 actualisés sont présentés page 19 de ce rapport.
- Le chiffre d'affaire tel qu'il est mesuré -c'est-à-dire acteur par acteur- ne permet pas de prendre en compte les activités d'intégration qui font partie de la filière et qui sont principalement regroupées dans les segments des véhicules et plateformes de sécurité (véhicules terrestres, navires, avions, hélicoptères et robots). Dans le précédent Observatoire, les chiffre d'affaires des 4 principaux segments de la filière avaient donc été corrigés de façon à représenter exclusivement les ventes de produits finis (l'objectif étant par exemple qu'une boule optronique intégrée dans un hélicoptère ne soit comptabilisé que dans le segment « hélicoptère » et non dans le segment « observation large zone », étant donné que la vente « finale » a lieu dans le segment des hélicoptères). Concrètement, cet ajustement avait consisté à baisser le chiffre d'affaires de la sécurité électronique au profit de la sécurité physique. Cet exercice d'ajustement n'a pas été reproduit dans le nouvel observatoire pour deux raisons corrélées : pouvoir faire apparaitre un CA cohérent aussi bien au niveau agrégé que selon les 30 segments de la sécurité et faciliter à l'avenir les comparaisons avec d'autres filières sur la base d'une variable « standard » de chiffre d'affaires (et non pas d'un chiffre d'affaires *ajusté* que cet observatoire est le seul à fournir). En conséquence, le sécurité électronique apparait comme étant plus importante que la sécurité physique dans cet observatoire. Si en termes de chiffre d'affaires ces chiffres sont corrects, le lecteur doit avoir à l'esprit qu'en pratique une petite partie du chiffre d'affaires réalisé par la sécurité électronique est intégrée puis vendue par des acteurs de la sécurité physique.
- Un travail a également été effectué pour prendre en compte les mouvements de fusion-acquisition qui ont eu lieu au sein de la filière sur la période. En conséquence, les nouveaux chiffres correspondant aux nombres d'entreprises sur les différents segments de la filière ne sont pas simplement le fruit de l'estimation des faillites et des créations d'entreprises sur la période 2016-2018, mais également des mouvements de concentration de la filière.

NOTES MÉTHODOLOGIQUES

Critère de nationalité des capitaux des entreprises de la filière. Dans cet Observatoire comme dans le précédent, nous analysons les entreprises selon la nationalité de leurs capitaux. Le critère retenu à cet effet est celui de la nationalité du/des *actionnaire(s) principal/aux en tête de pont*.

- ***En tête de pont***. En tête de pont signifie que nous remontons les filiales et les liens capitalistiques entre entités financières pour retenir l'entité en bout de chaîne.
- ***Actionnaires principaux***. Si l'actionnaire principal de l'entité détient les capitaux sous la forme de capitaux fixes, alors sa nationalité est directement retenue comme étant la nationalité de l'entité. Si les principaux actionnaires détiennent les capitaux sous forme flottante, alors nous considérons parmi les 10 principaux actionnaires flottants la nationalité qui détient les parts les plus importantes. Dans le cas d'une Joint Venture, la JV est considérée comme appartenant simultanément aux nationalités de ses deux actionnaires si elles sont distinctes (formant alors un doublon de nationalité).

Chiffre d'affaires à l'export de la filière. Le taux d'export (50% et le taux à l'international (60%) affichés dans ce rapport suivent la même méthodologie que pour le précédent Observatoire. Cependant, après un approfondissement de l'analyse, il semble que les taux effectifs soient plutôt de 30-35% à l'export et 50% à l'international. Il y a deux raisons à cela :

1. La surreprésentation des grandes entreprises et ETI de sécurité physique et électronique (qui exportent significativement plus que la moyenne) dans l'échantillon initial de calcul.

2. Un taux d'export qui inclue parfois dans son calcul des activités réalisées à l'étranger à travers des filiales, générant un double comptage lors de la mesure du CA à l'international puisque certaines activités réalisées à l'étranger à travers des filiales sont donc également comptabilisées dans le CA export.

II) Une filière importante et dynamique

COMPARAISON DES FILIÈRES INDUSTRIELLES FRANÇAISES

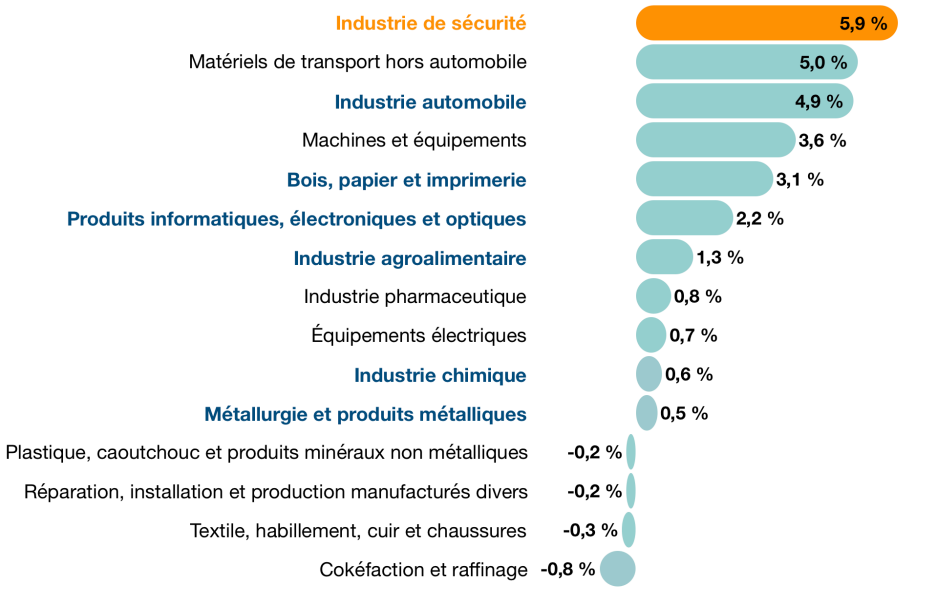
Dans ce chapitre, la filière industrielle de sécurité est comparée aux autres industries françaises. La comparaison s'effectue sur la base des chiffres publiés par Eurostat et l'OCDE sur les industries manufacturières françaises.

La segmentation utilisée par Eurostat et l'OCDE identifie 14 industries manufacturières en France (segmentation NACE rev2 C). Par ailleurs, le Conseil National de l'Industrie (CNI) -auprès duquel l'industrie de sécurité dispose d'un Comité Stratégique de Filière (CSF) depuis 2018- segmente l'industrie française en 18 filières stratégiques, dont le champ recoupe partiellement la nomenclature utilisée par Eurostat et l'OCDE. En conséquence, 11 filières industrielles disposent d'un CSF auprès du CNI mais ne disposent pas d'un segment dédié auprès de la segmentation de l'OCDE et Eurostat. Il s'agit des industries suivantes : Eau, Infrastructure du numérique, Mode et luxe, Santé, Aéronautique, Mer, Nouveaux systèmes énergétiques, Construction, Ferroviaire, Nucléaire et Transformation et valorisation des déchets. Les chiffres de ces 11 filières recoupent plus ou moins fortement les chiffres de certains segments utilisés par Eurostat et l'OCDE : Industrie pharmaceutique ; Textile, habillement, cuir et chaussures ; etc.

2.1 L'industrie de sécurité est l'industrie française qui a la croissance la plus forte

Sur la période 2013-2016, l'industrie de sécurité est la filière industrielle française avec le plus fort taux de croissance avec 5,9% par an. L'industrie automobile et l'industrie des matériels de transport hors automobile (Naval, Ferroviaire, Aéronautique et spatiale, Défense et tout type de motocycles), sont les deux autres industries ayant un taux de croissance similaire sur la période. L'industrie manufacturière française dans son ensemble a stagné à 0,1% de croissance annuelle moyenne entre 2013 et 2018 d'après l'INSEE.

CROISSANCE ANNUELLE MOYENNE DES FILIÈRES FRANÇAISES SUR LA PÉRIODE 2013-2016



Orange = Industrie de sécurité (qui dispose d'un CSF auprès du CNI mais pas d'un segment OCDE)

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

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

Sources : DECISION, OCDE

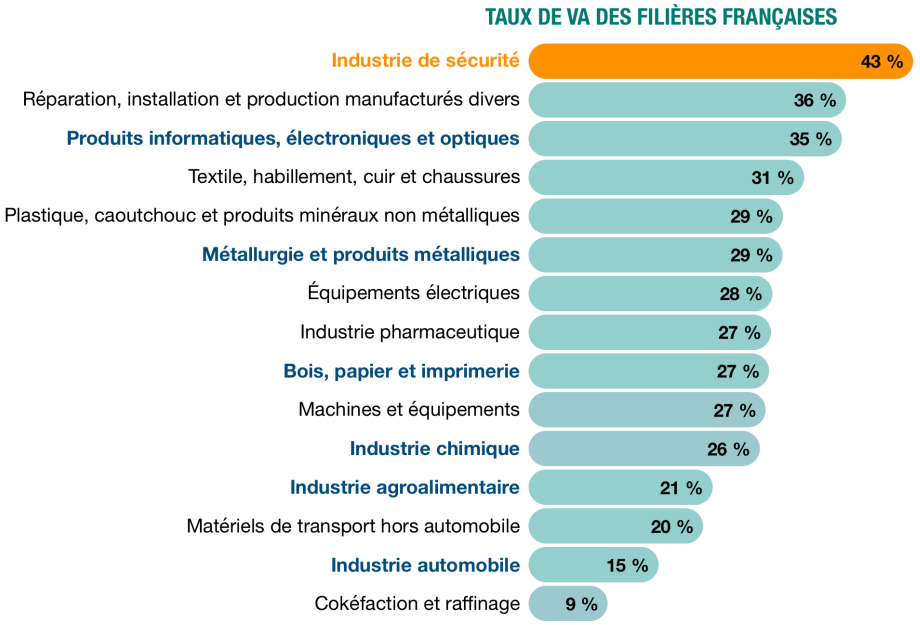
II) Une filière importante et dynamique

2.2 L'industrie de sécurité est la filière industrielle avec le plus fort taux de valeur ajoutée

L'industrie de sécurité est la filière la plus productive avec un taux de valeur ajoutée de 43% (Valeur Ajoutée / Chiffre d'affaires). En d'autres termes, l'industrie de sécurité 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 sécurité, que se soit à travers les activités d'installation de matériels physiques et électroniques (14% du CA total en 2018), ou à travers les services de cybersécurité (conseil, audit, formation, etc. qui ont représenté 12% 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 de sécurité correspondent à 44% du chiffre d'affaires total de la filière de sécurité, 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 sécurité qui maintien autant que faire se peu 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 électronique de sécurité est réalisée depuis la France, le taux de valeur ajoutée augmente.
- Enfin, la cybersécurité dans son ensemble correspond à près de 25% du CA total de la filière de sécurité en 2018. Or, les services de cybersécurité mais également les produits de cybersécurité impliquent une très grande partie de travail humain hautement qualifié (développement de logiciels, etc.), et correspondent donc à un taux de valeur ajoutée très élevé.



Orange = Industrie de sécurité (qui dispose d'un CSF auprès du CNI mais pas d'un segment Eurostat)

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)

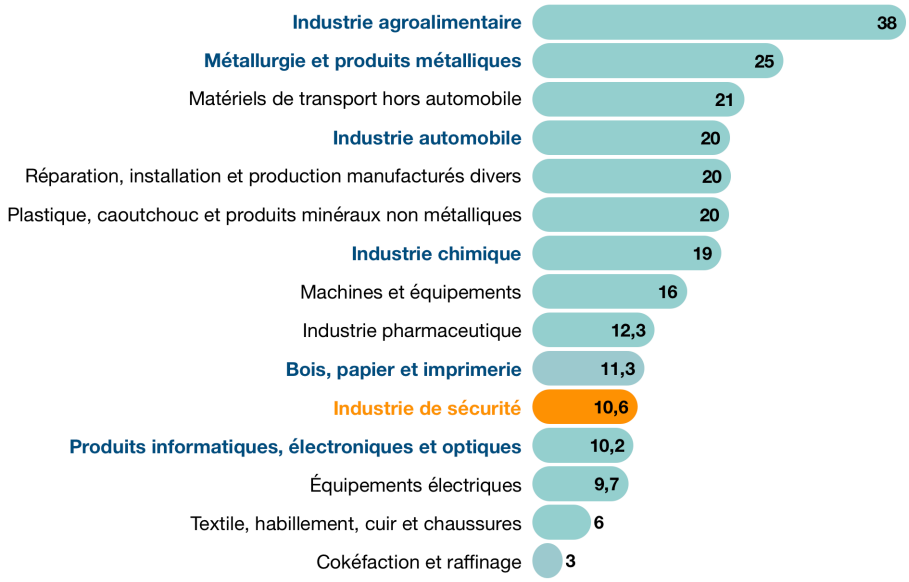
Sources : DECISION, Eurostat

II) Une filière importante et dynamique

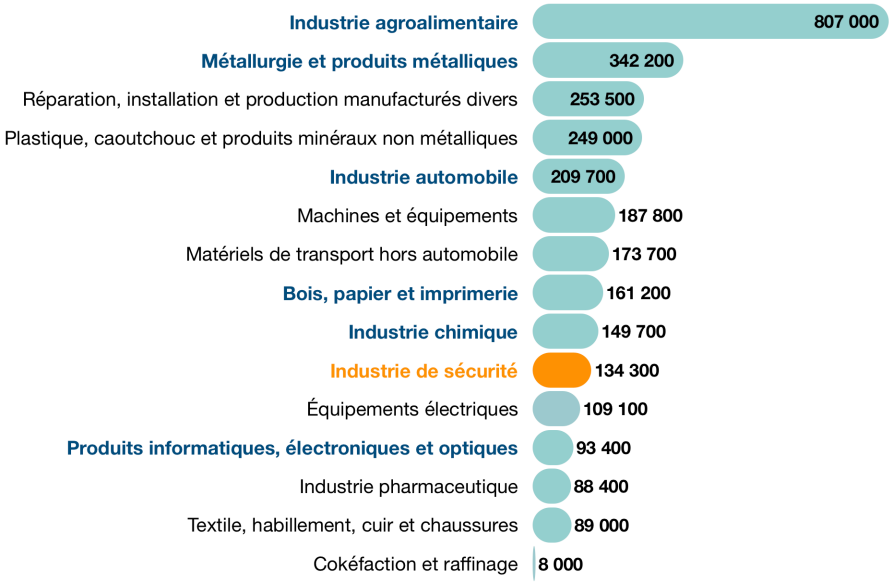
2.3 L'industrie de sécurité est une filière industrielle française à part entière

En termes de valeur ajoutée, la filière industrielle de sécurité se place à la 11ème place des industries manufacturières françaises (sur 15), entre la filière bois et la filière électronique. En termes d'emploi, la filière industrielle de sécurité se place à la 10ème place des industries manufacturières françaises (sur 15), entre l'industrie chimique et l'industrie des équipements électriques. Etant donné la croissance de l'industrie française de sécurité, celle-ci devrait dépasser en valeur ajoutée la filière Bois, papier et imprimerie ainsi que l'industrie pharmaceutique dans un horizon proche.

VA DES FILIÈRES FRANÇAISES EN 2017 (MILLIARDS D'EUROS)



EMPLOIS DES FILIÈRES FRANÇAISES EN 2017



Orange = Industrie de sécurité (qui dispose d'un CSF auprès du CNI mais pas d'un segment Eurostat)

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)

Sources : DECISION, Eurostat

II) Une filière importante et dynamique

2.4 Les acteurs français à la pointe en matière de compétences et de R&D

Grâce notamment à l'excellence française en matière de recherche et développement, une grande partie des entreprises françaises de l'industrie de sécurité 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 l'industrie de sécurité s'inscrit dans une dynamique mondiale

Au niveau mondial, la croissance de l'industrie de sécurité est portée par quatre facteurs, dont trois 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 sécurité et sur lesquels 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 locales et large zone, blockchain…

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 quatre tendances mondiales et ainsi construire une solide filière industrielle de sécurité.

La croissance est cependant encore plus forte dans les industries de sécurité américaine et surtout chinoise. Nous estimons ces croissances à respectivement 6,7% et 9,1% par an sur la période 2016-2018.

2.6 Une concurrence croissante de la part des acteurs étrangers

Les acteurs de nationalité française génèrent 75% du chiffre d'affaires de l'industrie de sécurité en France, soit 21 milliards d'euros en 2018. Autrement dit, les acteurs étrangers de la filière réalisent 25% du chiffre d'affaires de la filière en France, soit environ 7,1 milliards d'euros en 2018. Ce chiffre correspond uniquement au chiffre d'affaires généré par les filiales d'acteurs étrangers en France (y compris à des fins de distribution), et n'inclut pas les exportations des acteurs étrangers vers la France.

II) Une filière importante et dynamique

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 2018-2023 face à la présence de plus en plus forte d'acteurs étrangers, principalement chinois ou américains. La crise actuelle du COVID-19 va en particulier mécaniquement entrainer un fort risque de rachat d'une partie du tissu industriel français par des acteurs étrangers. Pour faire face à cette problématique, le CSF des Industries de sécurité propose un plan de relocalisation en France (numérique souverain, de confiance et résilient; technologies clés pour la résilience et le gestion de crise).

De même que pour la production en France, le poids des acteurs étrangers sur le marché français est important : il est estimé entre 35% et 45%*. Autrement dit, le marché national reste largement influencé par des solutions étrangères et non européennes, alors que la filière française dispose d'offres dans tous les segments et compte dans ses rangs des fleurons technologiques et de nombreux acteurs déjà de taille à couvrir à minima l'ensemble du marché national.

Des rachats significatifs d'entreprises françaises par des acteurs étrangers ont également été signalés dans la plupart des segments de l'industrie de sécurité sur la période 2013-2018. Parmi les rachats significatifs, figurent celui d'Arismore par Accenture (Etats-Unis), de DenyAll par Rohde & Schwarz Cybersecurity (Allemagne), ou encore d'Oberthur Technologies et Morpho par le fond américain Advent International pour former la marque Idemia en 2018.

Enfin et surtout, de nombreux acteurs de l'industrie de sécurité 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.

** Ce chiffre est obtenu en estimant les importations d'acteurs étrangers depuis la France. Cette estimation -combinée aux données de production depuis la France et d'exportation issues de la base de données de DECISION- permet d'estimer la taille du marché français et par la même occasion le poids des acteurs de capitaux étrangers qui réalisent 100% des importations vers la France et 25% du chiffre d'affaires depuis la France, pour un total équivalent à 35% à 45% du marché français. La marge d'erreur de 10% est maintenue car le montant exact des importations demeure incertain.*

2.7 Conclusion - Une filière à très fort potentiel

L'Industrie de sécurité 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 ;
- L'industrie de sécurité est une industrie française de premier plan, désormais reconnue par le Conseil National de l'Industrie à travers la création du comité stratégique de filière ;
- Les acteurs français sont à la pointe en matière de compétences et de R&D ;
- Le potentiel de croissance est durablement supérieur à celui des 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 La filière française par rapport aux autres filières de sécurité mondiale

Au niveau mondial, l'industrie de sécurité a cru de 7% par an en moyenne sur la période 2014-2019, soit un peu plus que la filière française.

L'industrie de sécurité mondiale est dominée par les **Etats-Unis**. Cela se reflète dans tous les segments de la filière où les Etats-Unis disposent :

- Soit d'une position de leadership, c'est-à-dire de la première place (éventuellement à égalité avec un autre pays) : vêtements de protection, équipements et fournitures, sécurité incendie, contrôle d'accès, détection d'intrusion et alarmes, détection de produits dangereux, observation large zone, renseignement et collecte d'information, tous les segments des produits cyber et pour finir tous les segments des services cyber.
- Soit de parts de marchés significatives, c'est-à-dire dans le top 5 mondial : plateformes physiques de sécurité, interdiction physique d'accès, identification & authentification des personnes, identification & authentification des produits, observation locale, traçage et localisation, communications sécurisées, et commande/contrôle/aide à la décision.

En cybersécurité, les Etats-Unis bénéficient notamment des synergies avec le leadership américain dans le domaine numérique (incarné par les GAFAMI : Google, Apple, Facebook, Amazon, Microsoft, IBM - dont plusieurs sont directement des leaders de la cybersécurité). L'industrie de sécurité américaine bénéficie également des synergies avec son industrie de défense (les Etats-Unis concentrent 36% des budgets mondiaux consacrés à la défense, l'OTAN compte pour 53% du total et la Chine, deuxième pays du monde, pour environ 14%).

L'**industrie Chinoise** est d'ores-et-déjà la deuxième mondiale. Elle croit très fortement et pourrait dans un horizon proche concurrencer sérieusement le leadership des Etats-Unis.

- La Chine est déjà en position de leadership sur plusieurs segments : drones, vêtements de protection, contrôle d'accès, détection d'intrusion et alarmes et observation locale.
- La Chine a déjà une position forte sur la plupart des autres segments de la filière de sécurité : navires de sécurité, plateformes robotiques terrestres et marines, interdiction physique d'accès, identification & authentification des produits, détection d'intrusion et alarmes, traçage et localisation, communications sécurisées, renseignement et collecte d'information ainsi que l'ensemble des segments de la cybersécurité pour laquelle la Chine nourrit de fortes ambitions.

Pour concurrencer les Etats-Unis sur le segment de la cybersécurité, la Chine peut compter sur le seul écosystème d'entreprises du numérique capable de concurrencer celui des Etats-Unis au niveau mondial, avec des acteurs emblématiques (comme Baidu, Alibaba, Tencent, Xiaomi, Huawei, BBK Electronics, etc.) et des investissements massifs de l'état Chinois pour placer la Chine au meilleur niveau sur de nombreuses technologies ayant trait à la sécurité électronique et cyber : intelligence artificielle (réseaux de neurones artificielles, edge AI, etc.), informatique quantique, photonique, calcul de haute performance (HPC), éléments sécurisés (Shanghai Huahong, Shanghai Fudan Microelectronics, etc.), etc.

L'**industrie française**, bien que clairement distancée au niveau agrégé par les industries chinoise et surtout américaine, se situe à un très bon niveau sur la quasi-totalité des segments de la filière et en particulier dans les segments des hélicoptères de sécurité, de l'identification & authentification des personnes, des éléments sécurisés, de l'observation large zone et des communications sécurisées.

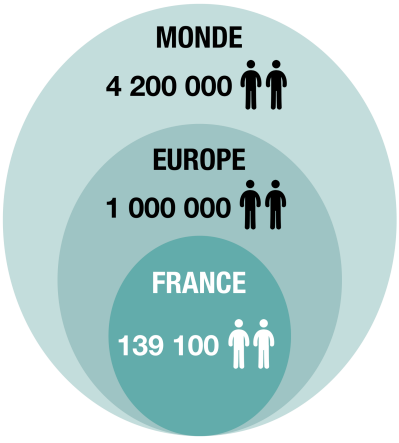
LES CHIFFRES DE LA FILIÈRE AU NIVEAU MONDIAL

Chiffre d'affaires

Pays / Region	Chiffre d'affaires (Milliards d'euros)		Taux de Croissance Annuelle Moyenne 2016-2018
	2016	2018	
Europe	103	112	4,1 %
Etats-Unis	136	155	6,7 %
Chine	75	89	9,1 %
Reste du Monde	161	176	4,5 %
Monde	400	470	8,4 %

Source : DECISION Etudes & Conseil

Effectifs en 2018



III) Les chiffres clés de la filière

Parmi les **autres acteurs importants** au niveau mondial, on trouve :

- Dans le monde : le Japon, la Corée du Sud, Israël et dans une moindre mesure le Canada.
- En Europe, les deux principales industries à l'exception de la France sont l'Allemagne et le Royaume-Uni. On trouve ensuite la Suède et l'Italie puis les Pays-Bas, l'Espagne et la Belgique.

La France se situe donc entre la 3ème et la 7ème place au niveau mondial, à une position proche de celle des industries japonaise, allemande anglaise et dans une moindre mesure sud-coréenne.

Le premier marché mondial de la sécurité ne se situe plus aux Etats-Unis mais dans le reste du monde et de plus en plus en Asie. La Chine est par exemple le premier marché mondial de la vidéosurveillance (près de 50% selon les estimations), avec notamment près de 450 millions de caméras de sécurité publiques et privées avec reconnaissance faciale installées en 2020. En 2015, ce chiffre atteignait déjà 176 millions, contre seulement 62 millions installées aux Etats-Unis en 2016.

3.2 Les principaux segments de la filière française

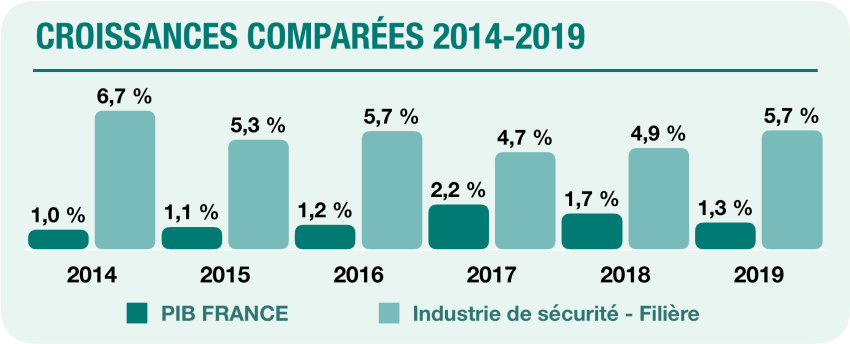
Le diagramme page 19 regroupe tous les chiffres des principaux segments de la filière de sécurité sur la période 2016-2019. Les produits électroniques demeurent le premier segment de la filière avec 43% du chiffre d'affaires en 2019. Cependant, avec une croissance annuelle moyenne de 11,8% sur la période 2016-2018, la cybersécurité prend de plus en plus d'importance dans la filière et représente en 2019 près d'un quart de son chiffre d'affaires total, soit 7,3 milliards d'euros. En comparaison, la cybersécurité représentait moins de 5% du chiffre d'affaires de la filière au début des années 2000 et pourrait égaler en chiffre d'affaires les produits électroniques à horizon 2025.

Ces tendances laisseraient supposer qu'il existe une séparation nette entre les différents segments -aussi bien en termes de produits que d'acteurs- et que la croissance de la cybersécurité serait décorrélée de celle des produits électroniques et physiques. Il n'en est rien et au contraire, les produits de sécurité intègrent de plus en plus une composante physique, une composante électronique et une composante cyber. De façon similaire, les acteurs de la filière se positionnent de plus en plus sur ces trois segments. Leurs croissances sont donc fortement corrélées, en particulier celles de l'électronique et de la cybersécurité. En d'autres termes, l'unification de la filière est en train de s'opérer par les produits. La cybersécurité, qui comprend une très forte part de travail humain, augmente mécaniquement le taux de valeur ajoutée de la filière.

Le diagramme ci-dessous montre les taux de croissance annuels moyens comparés du PIB français et du chiffre d'affaires de la filière industrielle de sécurité. En moyenne, la filière a cru de 5,5% par an sur la période 2014-2019 contre 1,4% pour le PIB français. Cette croissance a été portée principalement par :

- La forte croissance de la demande de produits et services de cybersécurité, elle-même portée par la transformation digitale
- Le développement des objets connectés (safe city, sécurisation des objets connectés), portés à la fois par la transformation digitale, la miniaturisation et la baisse des coûts des composants électroniques
- De nombreuses innovations technologiques : sécurisation des objets connectés, identité numérique, développements en matière de cryptographie, d'éléments sécurisés, d'intelligence artificielle (biométrie comportementale, agrégation et analyse de données, etc.), plateformes robotiques, blockchain, analyse en temps réel des données d'observations locales et large zone, etc.
- Un fort taux d'exportation de la filière dans son ensemble
- Enfin, par les mesures d'adaptation du public, des entreprises et des citoyens français aux attentats terroristes qui ont eu lieu sur la période.

Sur la période 2019-2023, cette croissance devrait se maintenir en dépit de la récession associée au coronavirus pour l'année 2020. En effet, les fondamentaux de la croissance de la filière demeurent : demande de produits et de services de cybersécurité, développement des objets connectés, fort taux d'exportation et innovations technologiques générant de nouvelles applications. La tenue en France de la coupe du monde de rugby en 2023 et des Jeux Olympiques d'été en 2024 va également soutenir la croissance de la filière.



Source : DECISION Etudes & Conseil

III) Les chiffres clés de la filière

CHIFFRES DES PRINCIPAUX SEGMENTS DE LA FILIERE SUR LA PERIODE 2016-2019

	TOTAL FILIERE INDUSTRIELLE	PRODUITS PHYSIQUES	PRODUITS ELECTRONIQUES	PRODUITS CYBER	SERVICES CYBER
Chiffre d'affaires (M€)					
2019*	29 700 M€ (100%)	9 700 M€ (32,5%)	12 780 M€ (43%)	3 750 M€ (12,6%)	3 550 M€ (12%)
Croissance 2018-2019	5,8%	3,6%	4,1%	13,9%	10,3%
2018	28 150 M€ (100%)	9 360 M€ (33%)	12 280 M€ (44%)	3 300 M€ (11,7%)	3 220 M€ (11,4%)
TCAM** 2016-2018	4,9%	2,8%	3,3%	14%	9,6%
2016	25 580 M€ (100%)	8 860 M€ (35%)	11 510 M€ (45%)	2 540 M€ (10%)	2 680 M€ (10%)
Nombre d'employés					
2018	139 100 (100%)	39 900 (28,7%)	62 500 (45%)	16 750 (12%)	19 900 (14,3%)
Valeur Ajoutée (M€)					
2018	11 100 M€ (100%)	2 950 M€ (27%)	4 740 M€ (43%)	1 915 M€ (17%)	1 490 M€ (13%)

* Estimations, chiffres non consolidés
** Taux de Croissance Annuel Moyen (TCAM)

Source : DECISION Etudes & Conseil

III) Les chiffres clés de la filière

3.3 Analyse par sous-segment

Dans ce chapitre, les infographies des pages suivantes détaillent les chiffres de la filière selon 30 segments détaillés. On y trouve les chiffre d'affaires des années 2016 et 2018, les emplois en 2018 ainsi que le nombre d'entreprises présentes sur chacun des segments en 2018.

Sur la période 2016-2018, la croissance des différents segments de la filière est très hétérogène, depuis le segment des outils électroniques d'identification et authentification des objets (1.2.1.3), qui subit une récession de -20,9% par an jusqu'au segment des produits cyber de sécurisations des infrastructures (pare-feux, antivirus, anti-dos, détection d'intrusion, traçage, suivi, sécurité des communications téléphoniques, des visioconférences, des mails et messageries, VPN, etc.), qui bénéficie d'une croissance de +17,5% par an en moyenne.

Trois segments en particulier ont fait l'objet d'une croissance inhabituelle sur la période.

- **Identification et authentification des objets**. Ce segment, qui comprend l'authentification (billets de banque, etc.) et la traçabilité (code EAN, etc.) des objets, a été marqué sur la période 2016-2018 par la forte contre-performance de ses deux leaders en termes de production depuis la France, à savoir Oberthur Fiduciaire et Arjowiggins Security. L'usine française d'Arjowiggins située en Seine-et-Marne, qui représentait encore près de 100 M€ de chiffre d'affaires de sécurité en 2016, a vu son activité baisser régulièrement jusqu'à la fermeture définitive de l'usine début 2019. Le chiffre d'affaires déclaré en France d'Oberthur Fiduciaire a quant à lui chuté de 40% entre 2016 et 2018. Les bonnes performances des autres acteurs présents sur ce segment (IN Groupe, Surys, etc.), ne suffisent pas à contrebalancer cette tendance. Précisons que ce segment ne correspond pas à la sécurisation des objets connectés.

- **Navires de sécurité**. Le segment des navires de sécurité à quant à lui bénéficié d'une croissance particulièrement importante sur la période 2016-2018 grâce à de belles performances à l'export combinées à une augmentation du nombre et de la taille des contrats associés aux pouvoirs publics français pour renouveler la flotte navale en partie vieillissante : Naval Group (5 frégates multi-missions FREMM livrée entre 2015 et 2020 et partiellement dédiées à des missions de sécurité), Socarenam (3 patrouilleurs Antilles-Guyane livrés en 2017 et 2019, 2 bateaux-pompes légers livrés en 2018 et 2019, 5 vedettes grade-côtes livrées en 2016 et 2018), Piriou/Kership* (6 patrouilleurs ou BSA livrés entre 2017 et 2019 à la Marine Nationale), etc. Cette tendance a commencée en 2014-2015 et devrait se poursuivre à minima jusqu'en 2023 aux vues des contrats à venir (4-5 frégates FDI de Naval Group, 12 vedettes VPDMP d'Ufast, 2 vedettes garde-côtes FPB 100 et un patrouilleur type OPV 150 commandées à Ocea, etc.). A l'exportation, les perspectives sont également favorables sur la période, notamment pour Naval Group / Kership* (contrats récemment signés avec l'Argentine, Chypre, le Sénégal, etc.) et CMN (contrat signé en 2019 de fourniture de 39 intercepteurs du type HSI 32 à l'Arabie Saoudite pour un montant environnant les 500 M€, etc.).

- **Avions et hélicoptères de sécurité**. La stagnation de ce segment sur la période 2016-2018 ne devrait pas se poursuivre sur la période 2018-2023 car une partie significative de la flotte vieillissante des avions des services publics de sécurité français devrait être remplacée sur la période 2018-2025 : en particulier en ce qui concerne la sécurité civile (10 H160 et 2 H145), la gendarmerie (10 H160) et les douanes (16 H125). Les services d'entretien du parc existant sont également comptabilisés dans ce segment.

NOTE METHODOLOGIQUE

Pour la première fois, l'Observatoire de la filière de sécurité présente le détail des chiffres des 30 segments de la filière au niveau agrégé. En d'autres termes, ces chiffres ne sont pas seulement ceux de la base de données de DECISION, mais sont extrapolés pour être représentatifs de la filière française dans son ensemble. En conséquence, ces chiffres ne sont pas comparables à ceux présentés dans les précédents Observatoires. Les chiffres ont systématiquement été reconstitués de façon à fournir toute l'information utile aussi bien pour l'année 2018 que pour l'année 2016 au sein de cet Observatoire.

Une partie du chiffre d'affaires générée par certains segments de la filière correspond à des produits qui sont intégrés comme sous-systèmes dans des produits d'autres segments de la filière, générant un double comptage. Ce double comptage est significatif en particulier entre les produits électroniques et physiques (certains produits électroniques étant intégrés dans des produits physiques), mais aussi entre différents segments électroniques. Le chapitre sur la méthodologie fournit plus de détail (voir page 11).

** Kership est une co-entreprise crée en 2013 par Naval Group et Piriou dans le but de fournir en France et à l'international une offre distincte de patrouilleurs et autres navires de taille moyenne (jusqu'à 95 mètres) dédiés à 90% à des missions de sécurité : marines, garde-côtes, douanes…*

III) Les chiffres clés de la filière

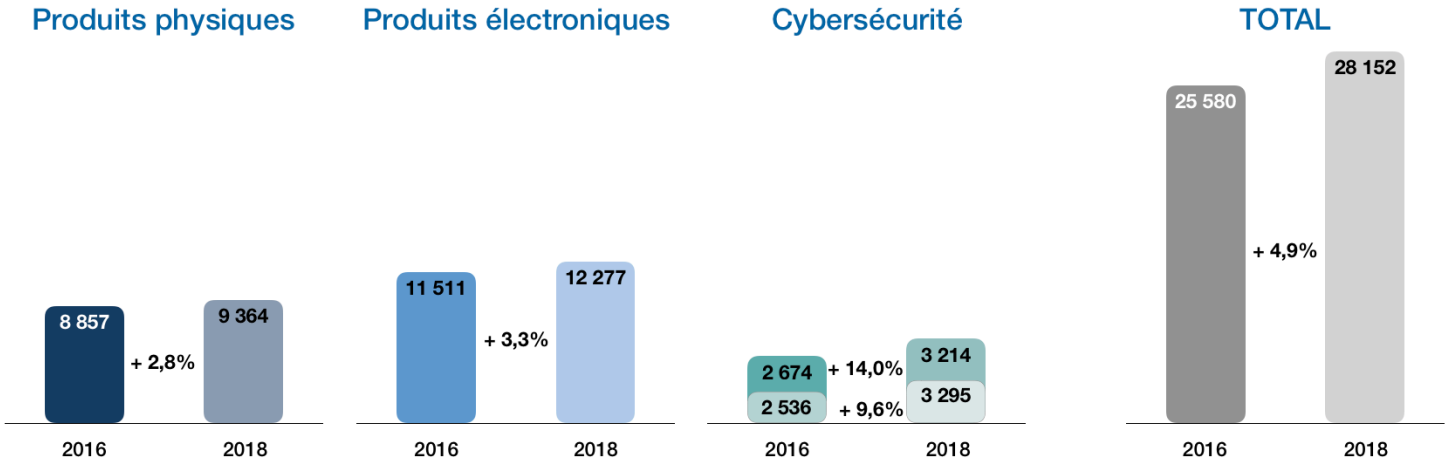
3.2.1 Taille et croissance 2016-2018

CHIFFRE D'AFFAIRES DE LA FILIÈRE INDUSTRIELLE DE SÉCURITÉ EN FRANCE PAR SEGMENT 2016-2018

	N°	SEGMENT	CHIFFRE D'AFFAIRES SÉCURITÉ EN MILLIONS D'EUROS	TCAM* 2016-2018
PRODUITS PHYSIQUES 9 377 M€	1.1.1.1	VÉHICULES TERRESTRES DE SÉCURITÉ	643 655	+ 1,0%
	1.1.1.2	AVIONS, HÉLICOPTÈRES DE SÉCURITÉ	799 820	+ 0,8%
	1.1.1.3	NAVIRES DE SÉCURITÉ	502 543	+ 4,0%
	1.1.1.4	PLATEFORMES ROBOTIQUES	166 219	+ 15,1%
	1.1.2	VÊTEMENTS DE PROTECTION	2 157 2 327	+ 3,8%
	1.1.3	EQUIPEMENTS ET FOURNITURES	1 106 1 116	+ 0,5%
	1.1.4	INTERDICTION PHYSIQUE D'ACCES	1 902 2 007	+ 2,7%
	1.1.5	ÉQUIPEMENTS DE SECURITE INCENDIE	1 582 1 685	+ 3,2%
PRODUITS ÉLECTRONIQUES 12 266 M€	1.2.1.1	SYSTEMES ET CONTRÔLE D'ACCÈS ÉLECTRONIQUE	1 283 1 427	+ 5,4%
	1.2.1.2	IDENTIFICATION DES PERSONNES	1 679 1 904	+ 6,5%
	1.2.1.3	IDENTIFICATION ET AUTHENTIFICATION DES OBJETS	282 451	- 20,9%
	1.2.2	SYSTEMES DE DÉTECTION	1 427 1 536	+ 3,7%
	1.2.3	ALARME INCENDIE - EXTINCTION	1 403 1 470	+ 2,4%
	1.2.4	INSPECTION DE PRODUITS OU DE PERSONNES	654 707	+ 4,0%
	1.2.5	OBSERVATION ET SURVEILLANCE LOCALE	1 217 1 336	+ 4,8%
	1.2.6	OBSERVATION ET DETECTION LARGE ZONE	471 515	+ 4,5%
	1.2.7	SUIVI - TRAÇAGE - LOCALISATION	441 471	+ 3,4%
	1.2.8	COMMUNICATIONS	1 578 1 633	+ 1,7%
	1.2.9	COMMANDE - CONTRÔLE - AIDE À LA DÉCISION	559 601	+ 3,6%
	1.2.10	RENSEIGNEMENT - COLLECTE D'INFORMATION	347 394	+ 6,5%
PRODUITS DE CYBERSÉCURITÉ 3 293 M€	2.0.1	GOUVERNANCE	427 537	+ 12,1%
	2.0.2	GESTION DES IDENTITÉS ET DES ACCÈS	423 546	+ 13,6%
	2.0.3	SÉCURITÉ DES DONNÉES	637 855	+ 15,8%
	2.0.4	SÉCURITÉ DES APPLICATIONS	190 225	+ 8,7%
	2.0.5	SÉCURITÉ DES INFRASTRUCTURES	594 821	+ 17,5%
	2.0.6	SÉCURITÉ DES PRODUITS & ÉQUIPEMENTS	264 311	+ 8,6%
SERVICES DE CYBERSECURITE 3 214 M€	3.0.1	AUDIT - PLANNING - CONSEIL	1 152 1 400	+ 10,2%
	3.0.2	MISE EN OEUVRE CYBERSÉCURITÉ	858 1 028	+ 9,4%
	3.0.3	INFOGÉRANCE - EXPLOITATION	571 685	+ 9,4%
	3.0.4	FORMATION EN CYBERSÉCURITÉ	95 104	+ 4,6%

Source : DECISION Etudes & Conseil

*TCAM = TAUX DE CROISSANCE ANNUEL MOYEN



Source : DECISION Etudes & Conseil

LES TAUX DE CROISSANCE INDIQUÉS SONT DES TAUX DE CROISSANCE ANNUEL MOYEN (TCAM) SUR LA PÉRIODE 2016-2018

III) Les chiffres clés de la filière

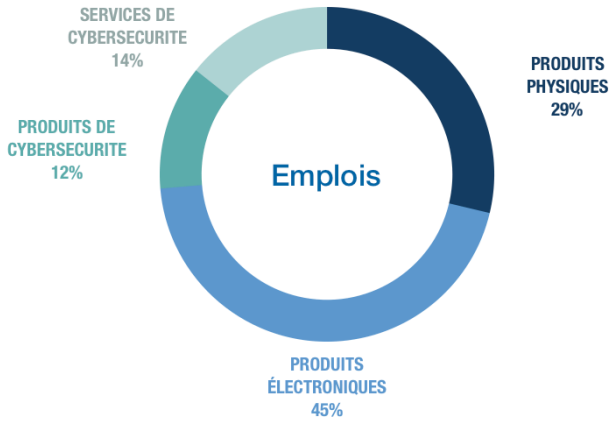
3.2.2 Emplois 2018

EMPLOIS DANS LA FILIÈRE INDUSTRIELLE DE SÉCURITÉ EN FRANCE PAR SEGMENT EN 2018

	N°	SEGMENT	EMPLOIS DANS LA FILIÈRE SÉCURITÉ PAR SEGMENT
PRODUITS PHYSIQUES 39 940	1.1.1.1	VÉHICULES TERRESTRES DE SÉCURITÉ	3 050
	1.1.1.2	AVIONS, HÉLICOPTÈRES DE SÉCURITÉ	2 700
	1.1.1.3	NAVIRES DE SÉCURITÉ	2 560
	1.1.1.4	PLATEFORMES ROBOTIQUES	1 420
	1.1.2	VÊTEMENTS DE PROTECTION	7 040
	1.1.3	EQUIPEMENTS ET FOURNITURES	4 320
	1.1.4	INTERDICTION PHYSIQUE D'ACCES	8 710
	1.1.5	ÉQUIPEMENTS DE SECURITE INCENDIE	10 140
PRODUITS ÉLECTRONIQUES 62 500	1.2.1.1	SYSTEMES ET CONTRÔLE D'ACCÈS ÉLECTRONIQUE	6 280
	1.2.1.2	IDENTIFICATION DES PERSONNES	8 140
	1.2.1.3	IDENTIFICATION ET AUTHENTIFICATION DES OBJETS	1 840
	1.2.2	SYSTEMES DE DÉTECTION	8 930
	1.2.3	ALARME INCENDIE - EXTINCTION	9 130
	1.2.4	INSPECTION DE PRODUITS OU DE PERSONNES	3 020
	1.2.5	OBSERVATION ET SURVEILLANCE LOCALE	7 930
	1.2.6	OBSERVATION ET DETECTION LARGE ZONE	2 420
	1.2.7	SUIVI - TRAÇAGE - LOCALISATION	2 380
	1.2.8	COMMUNICATIONS	7 120
	1.2.9	COMMANDE - CONTRÔLE - AIDE À LA DÉCISION	3 220
	1.2.10	RENSEIGNEMENT - COLLECTE D'INFORMATION	2 100
PRODUITS DE CYBERSECURITE 16 750	2.0.1	GOUVERNANCE	3 350
	2.0.2	GESTION DES IDENTITÉS ET DES ACCÈS	2 510
	2.0.3	SÉCURITÉ DES DONNÉES	4 590
	2.0.4	SÉCURITÉ DES APPLICATIONS	1 030
	2.0.5	SÉCURITÉ DES INFRASTRUCTURES	4 030
	2.0.6	SÉCURITÉ DES PRODUITS & ÉQUIPEMENTS	1 230
SERVICES DE CYBERSECURITE 19 940	3.0.1	AUDIT - PLANNING - CONSEIL	8 880
	3.0.2	MISE EN OEUVRE CYBERSÉCURITÉ	6 690
	3.0.3	INFOGÉRANCE - EXPLOITATION	3 480
	3.0.4	FORMATION EN CYBERSÉCURITÉ	890

Source : DECISION Etudes & Conseil

139 100 EMPLOIS DANS LA FILIÈRE SÉCURITÉ EN FRANCE



III) Les chiffres clés de la filière

3.2.3 Nombre d'entreprises 2018

NOMBRE D'ENTREPRISES DANS LA FILIÈRE INDUSTRIELLE DE SÉCURITÉ EN FRANCE PAR SEGMENT EN 2018

PRODUITS PHYSIQUES
1 447
703 | 729

PRODUITS ÉLECTRONIQUES
1 794
795 | 978

PRODUITS DE CYBERSECURITE
669
306 | 363

SERVICES DE CYBERSECURITE
664
267 | 397

N°	SEGMENT	ENTREPRISES DANS LA FILIÈRE PAR SEGMENT:		TOTAL
1.1.1.1	VÉHICULES TERRESTRES DE SÉCURITÉ	110	61	172
1.1.1.2	AVIONS, HÉLICOPTÈRES DE SÉCURITÉ	77	46	124
1.1.1.3	NAVIRES DE SÉCURITÉ	91	49	141
1.1.1.4	PLATEFORMES ROBOTIQUES	127	125	254
1.1.2	VÊTEMENTS DE PROTECTION	187	194	385
1.1.3	ÉQUIPEMENTS ET FOURNITURES	241	277	524
1.1.4	INTERDICTION PHYSIQUE D'ACCÈS	251	279	537
1.1.5	ÉQUIPEMENTS DE SECURITE INCENDIE	194	204	403
1.2.1.1	SYSTÈMES ET CONTRÔLE D'ACCÈS ÉLECTRONIQUE	133	188	321
1.2.1.2	IDENTIFICATION DES PERSONNES	184	294	478
1.2.1.3	IDENTIFICATION ET AUTHENTIFICATION DES OBJETS	102	105	209
1.2.2	SYSTÈMES DE DÉTECTION	308	410	727
1.2.3	ALARME ET DÉTECTION INCENDIE	187	231	423
1.2.4	DÉTECTION DE PRODUITS DANGEREUX	121	138	262
1.2.5	OBSERVATION ET SURVEILLANCE LOCALE	346	436	792
1.2.6	OBSERVATION ET SURVEILLANCE LARGE ZONE	95	94	189
1.2.7	SUIVI - TRAÇAGE - LOCALISATION	125	95	220
1.2.8	COMMUNICATIONS SÉCURISÉES	138	169	310
1.2.9	COMMANDE - CONTRÔLE - AIDE À LA DÉCISION	158	107	265
1.2.10	RENSEIGNEMENT - COLLECTE D'INFORMATION	129	82	211
2.0.1	GOUVERNANCE CYBER	128	69	197
2.0.2	GESTION DES IDENTITÉS ET DES ACCÈS	121	75	196
2.0.3	SÉCURITÉ DES DONNÉES	192	121	313
2.0.4	SÉCURITÉ DES APPLICATIONS	97	56	153
2.0.5	SÉCURITÉ DES INFRASTRUCTURES	188	124	312
2.0.6	SÉCURITÉ DES PRODUITS & ÉQUIPEMENTS	96	57	153
3.0.1	AUDIT - PLANNING - CONSEIL CYBER	229	391	620
3.0.2	MISE EN OEUVRE CYBERSÉCURITÉ	176	249	425
3.0.3	INFOGÉRANCE - EXPLOITATION	120	211	331
3.0.4	FORMATION EN CYBERSÉCURITÉ	122	84	206

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

Source : DECISION Etudes & Conseil

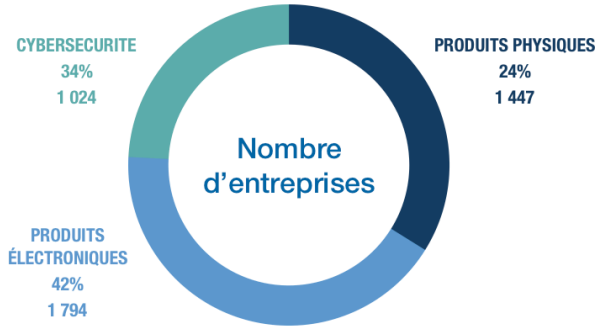
AUTRES ENTREPRISES
CA TOTAL 2018 > 2M€ ET EFFECTIFS TOTAUX 2018 > 9

TRÈS PETITE ENTREPRISES (TPE)
CA TOTAL 2018 < 2M€ ET EFFECTIFS TOTAUX 2018 < 10

4 440 ENTREPRISES DANS LA FILIÈRE EN FRANCE

DONT
- **95** GRANDES ENTREPRISES
- **118** ENTREPRISES DE TAILLE INTERMÉDIAIRE
- **1 817** PETITES ET MOYENNES ENTREPRISES
- **2 410** TRÈS PETITES ENTREPRISES

Source : DECISION Etudes & Conseil



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

IV) Les tendances

4.1 Tendances de marché sur la période 2017-2020

4.1.1 De nombreux mouvements de fusions-acquisitions

Au sein de la filière industrielle de sécurité, 94 rachats d'entreprises concernant des sièges d'entreprises localisés en France ont été recensés sur la période 2017-2020 (soit en moyenne 31 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.

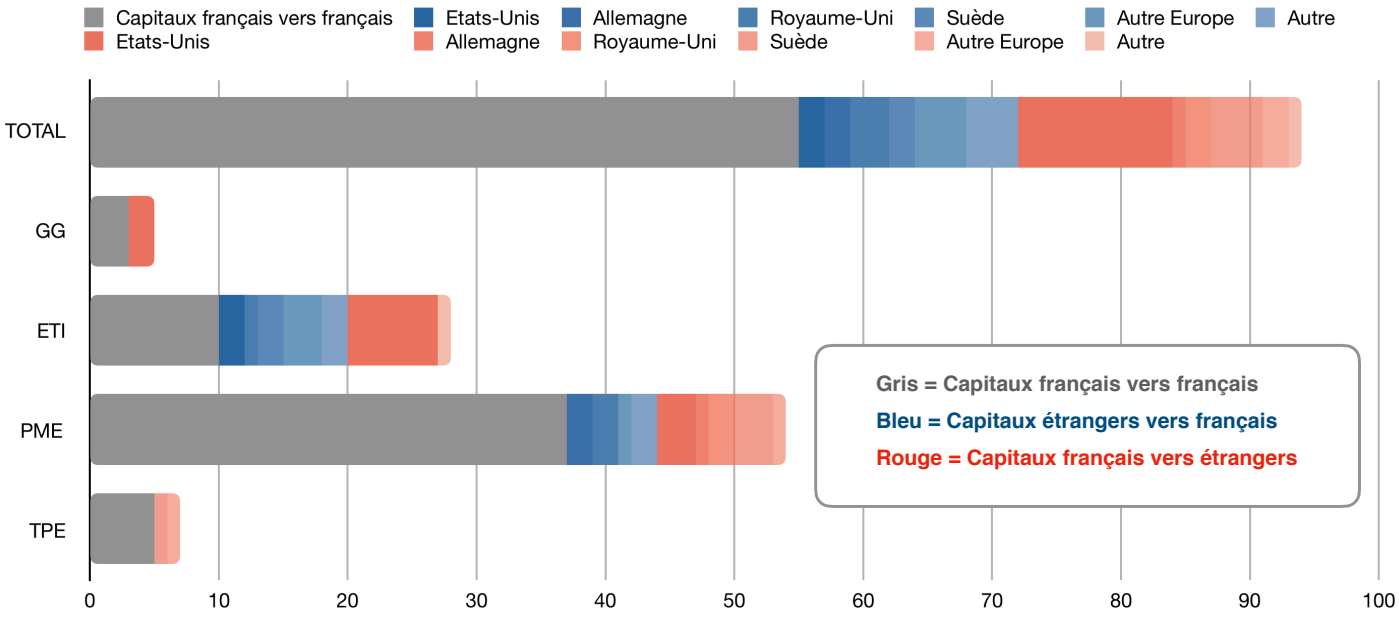
Parmi eux:

- 55 rachats d'entreprises françaises par d'autres entreprises françaises (59%)
- 17 rachats d'entreprises étrangères par des entreprises françaises (18%)
- 22 rachats d'entreprises françaises par des entreprises étrangères (23%)

La grande majorité des entreprises rachetées sont des PME (57%) et des ETI (30%), en croissance.

Le nombre de rachats d'entreprises françaises par des capitaux étrangers est supérieur de 30% 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, plus de la moitié des rachats d'entreprises françaises par des entreprises étrangères s'opère au profit de capitaux américains (55%). 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 : Safran Morpho, Oberthur Technologies, Hensoldt, Arismore, Orexad-Anfidis, Nexeya, Fichet Group, nCipherSecurity, Oldham, etc. Les 92 mouvements de rachats sont résumés dans le diagramme ci-dessous :



Source: DECISION Etudes & Conseil

- **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

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 rachetée		
	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
2020	**Atos Worldline**	GG	Ingenico	GG	Paiements en ligne, terminaux de paiements, sécurisation des paiements
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	**Vinci Energies**	GG	Sysoco	PME	Intégration et la sécurisation de systèmes de radiocommunication
2018	**Butler Industries**	Fond	NextiraOne (NXO)	ETI	Conseil en transformation numérique. Une partie de l'activité est dédiée au conseil en cybersécurité
2018	**Desautel**	ETI	Gimaex	ETI	Fabricant de véhicules de lutte anti-incendie
2018	**Armoric Holding**	ETI	Sidès	ETI	Fabricant de véhicules de lutte anti-incendie
2018	**Atos**	GG	Air-Lynx	PME	Solutions tactiques de communication LTE (Long Term Evolution)
2017	**Sopra Steria**	GG	Galitt	ETI	Logiciels de paiement / transactions sécurisées
2017-2020	**Anaveo**	ETI	RM Sécurité, VAE, Galilée, Themis Sécurité et Azman	PMEs	Anaveo a racheté cinq PME françaises sur le segment de l'installation de matériel électronique de sécurité (contrôle d'accès, détection d'intrusion, caméras…) sur la période 2017-2020, formant notamment la marque Neoexpert développant une offre sur-mesure à destination des grands comptes.
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 infrarouge, fusionnent pour former Lynred. Les deux entreprises ainsi réunies étaient et demeurent la propriété de Thales et de Safran.
- En 2018, le Groupe Marck, spécialisé dans les Equipements de Protection Individuelle (EPI), fusionne ses deux filiales Balsan et VTN.
- 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.

IV) Les tendances

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

Année	Entreprise acheteuse			Entreprise rachetée			
	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
2019	**Stella Group**	ETI	France	CRH S&A *(Division volets & stores)*	ETI	Irlande	Portes, sécurité du périmètre
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	**Lyreco**	ETI	France	Elacin et Intersafe	ETIs	Pays-Bas	Equipements de Protection Individuelle. Lyreco devient ainsi un acteur important au niveau Européen.
2017	**Sopra Steria**	GG	France	Kentor	ETI	Suède	Conseil en cybersécurité

IV) Les tendances

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

Année	Entreprise acheteuse			Entreprise rachetée			
	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	**Entrust Datacard**	ETI	Etats-Unis	nCipher Security (ex filiale de Thales)	ETI	France	L'activité de modules de sécurité matériels à usage général (GP HSM) de Thales a été regroupée sous la marque nCipher Security en 2019 puis vendue pour répondre à l'engagement envers plusieurs autorités de la concurrence de préserver la concurrence sur ce marché suite au rachat de Gemalto par Thales.
2019	**HAGER Groupe**	GG	Allemagne	Atral System	PME	France	Installateur de systèmes électroniques de sécurité : caméras, détection d'intrusion
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	**Marque Idemia** ***(Fond Advent International)***	GG	Etats-Unis	Safran Morpho (Identity & Security)	GG	France	Identification et authentification, biométrie, sécurité digitale, analyse de données et de vidéos
2017	**Marque Idemia** ***(Fond Advent International)***	GG	Etats-Unis	Oberthur Technologies	ETI	France	
2017	**Hensoldt** ***(Fond américain KKR)***	GG	Etats-Unis	Activité « Defence Electronics » d'Airbus D&S, renommée Hensoldt	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	**Marque Rubix** ***(Fond Advent International)***	GG	Etats-Unis	Orexad-Anfidis *(Fond Pai Partners)*	ETI	France	Equipements de Protection Individuelle (EPI)
2017	**Accenture**	GG	Etats-Unis	Arismore	ETI	France	Services de cybersécurité*
2014-2019	**Racheté par ISF en 2014 Puis Tyco en 2015 Puis Johnson Controls en 2016 Puis 3M en 2017 Puis Teledyne en 2019**	GG	Etats-Unis	Oldham	PME	France	Equipements de Protection Individuelle (EPI)

* 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.

IV) Les tendances

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 filière industrielle de sécurité, qui bénéfice 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.

En 2018, le groupe allemand Dräger fusionne ses deux filiales Dräger Safety et Dräger Medical.

4.1.2 Les fonds spécialisés

Il semble que les fonds spécialisés soient encore peu nombreux en Europe. La BPI en a identifié trois en 2019, spécialisés dans la cybersécurité et de plus en plus actifs.

Nom du fonds (et de la Société de gestion associée)	Nationalité de la Société de Gestion	Montant levé	Investisseurs	Prises de participations sur la période 207-2019
Brienne III - (ACE Management)	France	80 M€	• **Financiers:** Tikehau Capital (40M€), Bpifrance (20M€) • **Industriels:** EDF, Naval Group et Sopra Steria	**TrustInSoft** - 5 M€ (Recherche de vulnérabilité dans les logiciels)
				EGERIE - 4 M€ (Gestion des risques de cybersécurité)
				Dust Mobile - 3 M€ (Opérateur de téléphonie mobile sécurisée)
eCapital Cybersecurity - (eCapital)	Allemagne	30 M€	• **Financiers:** NRW.BANK • **Industriels:** RAG Foundation • **Institutionnels:** ERP Fund (European Recovery Programme, fonds de fonds géré par le FEI)	**UltraSoC** - 5 M£ (Système sur une puce (hardware) de collecte et d'analyses de données)
				VMRay - 10 M$ (Outils automatisés d'analyse et de découverte de malwares)
				BlueID - 3 M€ (Clés mobiles sécurisées et gestion des droits d'accès)
Paladin European Cyber Fund - (Paladin Capital Group)	Etats-Unis	29 M€	• **Institutionnels :** Luxembourg Future Fund, Fonds Européen d'Investissement	**DPOrganizer (suédois)** - 3 M$ (Outils automatisés d'analyse et de découverte de malwares)
				Elliptic (anglais) - 5 M€ (Gestion des risques liés aux cryptomonnaies)

Par ailleurs, parmi les fonds identifiés comme ayant des investissements significatifs dans la filière industrielle de sécurité, on trouve : Advent International (américain), KKR (américain), Eurazeo (français), Latour Capital (français), etc.

IV) Les tendances

4.1.3 Les levées de fond des start-ups

La BPI estime qu'en 2019, les startups françaises de la cybersécurité lèvent un total d'environ **35 M€** auprès des investisseurs français, ce chiffre étant stable depuis 2017. Le tableau ci-dessous regroupe les levées de fonds identifiées en 2019.

Startup	Montant levé	Fonds impliqués	Activité de l'entreprise
Dust Mobile	3 M €	Brienne III et Omnes	Communications sécurisées
EGERIE	4 M €	Brienne III	Gestion des risques cyber
TrustInSoft	5 M €	Brienne III et Idinvest Partners	Logiciels d'audit de cybersécurité
Bleckwen	9 M €	Ring Capital, Bpifrance, Tempocap et Ineo	Lutte contre la fraude bancaire
Citalid	1,2 M €	Axeleo Capital, BNP Paris Développement	Audit de cybersécurité
Alsid	13 M €	Idinvest Partners, 360 Capital & Axeleo Capital	Audit et gestion des accès cyber
GitGuardian	12 M $	Balderton Capital, Bpifrance, Scott Chacon et Solomon Hykes	Audit de cybersécurité
Sqreen	14 M $	Greylock Partners, Y Combinator, Alven et Point Nine	Sécurité des applications
Odaseva	11,7 M $	Partech, Salesforce Ventures et Serena Capital	Sécurité des données

4.1.4 Les principales entreprises en faillite

Année	Taille de l'entreprise	Entreprise	Activité
2019	ETI	**ARJOWIGGINS**	Spécialisée dans la fabrication de papier pour l'impression de billets de banque et documents officiels, l'usine Arjowiggins Security de Jouy-sur-Morin (Seine-et-Marne) a été mise en liquidation judiciaire par décision du tribunal de commerce de Nanterre (Hauts-de-Seine) le 17 janvier 2019. Cette liquidation a conduit à la fermeture de l'unique usine qui employait encore 200 salariés en janvier 2019 (contre 350 en 2014). Le chiffre d'affaires imputé à cette usine en France est passé de 208 M € en 2013 à 85 M € en 2017. Depuis la liquidation, les salariés et les élus locaux proposent des plans de relance.
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). Cependant, poursuite et croissance de l'activité d'Agueris, co-entreprise crée avec le Groupe CMI en 2015.
2019	PME	**Durisotti**	Numéro 2 français de la carrosserie automobile, Durisotti a été racheté par le groupe britannique Liberty House en mars 2019 dans le cadre d'un redressement judiciaire. L'entreprise avait réalisé en 2018 un chiffre d'affaires de 37 millions d'euros avec 200 salariés. Elle était en difficultés depuis quelques années puisqu'elle avait déjà connu un redressement judiciaire en 2012.
2018	ETI	**MANURHIN DEFENSE**	Fabricant de munitions. En difficulté pour se financer depuis plusieurs années malgré un carnet de commande rempli et un savoir-faire préservé, questionnements autour du soutien apporté à l'entreprise par l'actionnaire majoritaire Slovaque Delta Defence, entré au capital en 2011.
2018	PME	**SAFETIC** ***(ETUDE ET DEVELOPPEMENTS EN ELECTRONIQUE)***	Solutions de contrôle d'accès, y compris biométrique. Clôture définitive suite à des difficultés depuis 2012.
2018	PME	**ARMATURE TECHNOLOGIES**	Conseil en cybersécurité. Plan de sauvegarde en 2018.
2017	PME	**VEHIXEL CARROSSIER CONSTRUCTEUR**	Producteur de véhicules terrestres de sécurité : bus, camion et utilitaires blindés, ambulances et transport de fond. Reprise de l'activité en 2017 par l'ETI Trouillet.

IV) Les tendances

4.2 Les tendances technologiques

L'innovation technologique est le principal moteur de la croissance de l'industrie de sécurité 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 filière de sécurité de deux manières différentes et complémentaires.

4.2.1 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 l'industrie de sécurité.

- **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 sécurité : caméras, alarmes, 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 l'industrie de sécurité.

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 2013-2018, 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 électronique et de la cybersécurité en lien avec les objets connectés sur la période 2013-2018. 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.

IV) Les tendances

- **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 sécurité 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.

IV) Les tendances

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

En parallèle -et étant donné que l'industrie de sécurité est elle-même constituée majoritairement de solutions électroniques et numériques- **les innovations issues de l'industrie de sécurité** 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 entrain 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.

IV) Les tendances

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**.

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

4. **Plateformes robotiques (dont drones)**. Bien que sa croissance soit en phase de décélération, le segment des plateformes robotiques a cru en moyenne de 15,1% sur la période 2016-2018, ce qui correspond à la plus forte croissance sectorielle hors cybersécurité sur cette période. La croissance du nombre d'acteurs de la filière qui se sont positionnés sur ce segment ces dernières années est particulièrement importante (en particulier pour les drones), entrainant d'ailleurs un guerre des prix et des faillites nombreuses -en particulier pour un segment bénéficiant d'une telle croissance.

IV) Les tendances

Le potentiel de croissance demeure très important pour les applications actuelles (prises de vues aériennes pour l'inspection d'ouvrages, surveillance aérienne de sites, robots rondiers terrestre semi-autonomes, etc.) comme pour les applications futures dont le secteur foisonne (équipes cobotiques d'intervention sur le terrain pour les forces de l'ordre, la sécurité civile ou les services privés avec robots semi-autonomes capables de traiter des données et de produire des analyses de situation ; essaims de drones pilotés à distance indoor/outdoor ; amélioration des outils de connectivité et d'interaction avec les autres plateformes (navires, véhicules terrestres…) et les équipes pour une meilleure intégration dans les opérations…). La France dispose des acteurs et du savoir-faire technologique pour bénéficier des développements technologiques associés aux plateformes robotiques.

5. **Blockchain**. D'abord associée aux cryptomonnaies et au Bitcoin en particulier, la blockchain s'impose comme un nouvel outil indispensable de la sécurité. 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 sécurité 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 industrielle de sécurité mondiale. Par exemple, des innovations ont lieu en matière de **séquençage ADN**, qui coûte en moyenne déjà moins de 50€ et devrait d'ici quelques années s'opérer quasiment à la volée. Ou encore le développement autour de l'identité numérique : **captcha et challenges pour logiciels, QR codes, reconnaissance d'iris, de la forme des veines, mot de passe dynamique**…

IV) Les tendances

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, l'industrie de sécurité est impactée par deux facteurs majeurs (déjà évoqués page 30) :

- **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.

4.3.2 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.

IV) Les tendances

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 conséquence est le développement progressif d'équipes internes dédiées dans chacune des unités opérationnelles chez les clients.

4.4 Les 5 projets structurants du Comité stratégique de filière

L'industrie de sécurité est depuis 2018 l'une des 18 filières industrielles labélisées par le Conseil national de l'industrie.

Ce nouveau cadre, très opérationnel, donne une impulsion forte à la filière. Sous le comité stratégique de filière qui réunit l'État, l'industrie et les utilisateurs, c'est à travers le contrat de filière 2020-2022 entre l'État et l'industrie que les enjeux sont adressés. Signé le 29 et 30 janvier 2020, il comporte 5 projets structurants dont l'impact recherché est majeur :

Projet	Enjeu et poids économique
Sécurité des grands évènements et des JO Paris 2024 : Développer une offre nationale globale et compétitive	Supérieur à 1 Md€, soit un potentiel de croissance de 4% pour l'ensemble de la filière découlant uniquement de l'organisation des JO 2024. Ce projet est donc le plus porteur pour la filière de sécurité, car les 4% estimés ne correspondent pas à la taille des sous-segments impactés, mais au gain de croissance pour l'ensemble de la filière (presque tous les segments étant impactés par les JO 2024).
Cybersécurité et sécurité de l'IoT : Réaliser le potentiel exceptionnel de la France et assurer les besoins souverains	Enjeu vital pour la résilience et la souveraineté du numérique. Les activités de cybersécurité et les activités de sécurité associées au déploiement des IoTs représentent au total ~20% du CA de la filière en France
Identité numérique : Permettre le développement rapide du déploiement et de l'utilisation de l'identité numérique en France	Garder la maitrise de l'identité numérique, en alternative aux solutions des GAFAM, est un enjeu majeur. Les activités associées à l'identité numérique représentent ~5% du CA de la filière en France
Territoires de confiance : Solutions et notamment plateformes permettant le développement de nouveaux services et usages au bénéfice des acteurs du territoire	Essentiel pour le pilotage et la résilience des territoires. Estimé à plusieurs Mds€ d'ici 2025, soit plus de 4% du CA de la filière en 2018
Numérique de confiance : Cloud et outils collaboratifs de confiance	Essentiel pour sécuriser les données sensibles ou hautement valorisables, publiques comme privées. Les activités associées représentent ~14% du CA de la filière en France

Ce contrat qui vise tout particulièrement la souveraineté et la résilience, y compris par un volet d'actions européennes, répond par anticipation aux orientations tirées des enseignements de la crise COVID-19, et sera renforcé suivant ces lignes.

IV) Les tendances

4.5 La filière face au COVID-19

La filière a subi fortement l'impact de la crise sanitaire mondiale COVID-19, avec des Taux d'Activité (TA*) descendus à 50% et des Taux d'Emploi (TE) descendus à 65% en moyenne en avril 2020. Les segments physique et électronique, plus dépendants de l'export, ont été encore plus fortement touchés (TA de 30% et TE de 50%). Cette fragilisation de l'industrie porte le risque d'accroitre la prédation capitalistique du tissu industriel sensible de la filière.

Mais la crise a démontré une fois encore que la filière est essentielle pour la résilience de la nation face aux différents risques et menaces de tous ordres, notamment sur le plan numérique et cyber – le numérique étant le moyen majeur ayant permis le maintien des liens commerciaux, professionnels, sociaux et familiaux pendant le confinement, mais aussi pour la sécurité des biens et des personnes.

En matière numérique, la crise a montré une très forte dépendance de la France aux solutions étrangères, notamment américaines. Cette dépendance s'est aggravée et atteint maintenant un niveau « critique » selon les organisations d'utilisateurs (CDSE, CIGREF, CESIN…). La crise du COVID appelle donc un plan spécifique de résilience et relocalisation des outils numériques (cloud de confiance, outils collaboratifs, infrastructures numériques, etc.). La filière industrielle de sécurité a un rôle essentiel à jouer dans le cadre d'un tel plan grâce sa capacité à sécuriser de manière souveraine les outils numériques à développer et relocaliser.

Le CSF Industries de sécurité a donc fait des propositions qui visent à :

- Accélérer le contrat de filière et accroitre son soutien, dans une dynamique de souveraineté et de résilience, à travers des solutions, des outils et une chaine de valeur de confiance ;
- Compléter le contrat de filière sur les thèmes des technologies pour la résilience et la gestion de crise d'une part, et de la biosécurité en lien avec le CSF Industries et technologies de santé d'autre part.

Le CSF souligne que les réponses seront nationales et européennes, et qu'il y a lieu d'accélérer les initiatives et stratégies européennes en matière d'autonomie stratégique, de maitrise des chaines de valeur et de souveraineté.

Le CSF a en particulier formulé une proposition phare par projet du contrat de filière:

- **Numérique de confiance** : accélérer le développement, la certification et le déploiement public et privé d'une offre de Cloud de confiance afin de protéger les données sensibles et les outils collaboratifs ;
- **Identité numérique** : accélérer le déploiement de la Carte Nationale d'Identité Electronique (CNIE) de 10 ans à 3 ans afin de permettre les transactions à distance sécurisées par l'identité numérique, nécessaire à la continuité économique en temps de crise ;
- **Territoires de confiance** : déployer des plateformes d'intégration de données de sécurité, pour la résilience des collectivités locales, qui fédèrent les données produites sur le territoire et, en s'appuyant sur les technologies disponibles, permettent le développement de nouveaux services et usages (pilotage de la ville, résilience, mobilité, …) ;
- **Sécurité des grands événements et des JOP Paris 2024** : lancer dès 2020 les expérimentations du programme de sécurité des Jeux Olympiques et Paralympiques (JOP) Paris 2024 proposé par la filière et bénéficier immédiatement de ses avancées en matière de résilience et gestion de crise ;
- **Cybersécurité et sécurité de l'IoT** : financer un plan d'équipement cyber et continuité d'activité des 178 CHU, construit autour d'une offre et d'une chaine de valeur de confiance.

---

* Correspondant à la production / chiffre d'affaires

IV) Les tendances

4.6 Matrice FFOM de la Filière Industrielle de Sécurité en France

Forces	Faiblesses
Structures • Une filière industrielle forte avec des leaders mondiaux et des spécialistes au meilleur niveau dans certains secteur • Un système de promotion de l'innovation et de la recherche performant (CIR, etc.) • Des structures fédératrices : CSF Industries de Sécurité, CICS, ACN, 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, imagerie, radars, cryptographie, machine learning, deep learning, sécurisation des IoT et dans une moindre mesure blockchain, etc.) • Une filière de formation forte pour les compétences d'ingénierie et de développement logiciel avec notamment la création récente de plusieurs chaires cybersécurité en partenariats publics-privés	**Structures** • Les PME industrielles françaises sont majoritairement spécialisées dans un sous-segment spécifique avec des offres sur-mesure. En conséquence, elles travaillent 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 entre elles (mise en commun des compétences, offres commerciales conjointes, etc.), sur le modèle d'Hexatrust en cybersécurité ou encore de Global securalliance ou du Consortium Sécurité Privée pour la sécurité privée. Sans cela, elles tendent à demeurer dans des offres haut de gamme et sur-mesure auprès de quelques grandes entreprises et administrations • Commande publique faible dans de nombreux segments en raison des politiques d'austérité mises en oeuvre • Une filière encore trop segmentée • Manque de standards européens sur les marchés émergents **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 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.) demeure 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, dans des contextes de difficultés budgétaires. Les offreurs français souffrent de cette situation

IV) Les tendances

Opportunités

Structures

- 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, les entreprises françaises ont des offres souvent moins lisibles et trop sur-mesure, en particulier en comparaison des offres américaines. 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.
- Plateformes robotiques
- Blockchain
- Plateformes d'open hardware/software pour l'edge computing et les IoTs
- Analyse en temps réel des données d'observation locale et large zone
- Innovations relatives à l'identité numérique

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'Israël, d'Allemagne, de Grande Bretagne, de Suède, du Japon et de Corée du Sud
- 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

- Acquisition significative d'entreprises françaises par des capitaux américains sur la période 2016-2018
- Forte pénétration des entreprises asiatiques et en premier lieu chinoises sur les marchés « de masse », que les PME françaises ne peuvent concurrencer sur les prix. Montée en gamme des entreprises asiatiques et en premier lieu chinoises, particulièrement en matière de produits cyber

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 du CICS

Le CICS est l'association industrielle, créée en 2013, qui coordonne l'ensemble de la filière industrielle et constitue l'interlocuteur principal de l'État pour le CSF. Son président préside également le comité stratégique de filière. Le CICS regroupe les fédérations et groupements actifs dans le domaine de la sécurité, ses membres sont aujourd'hui : l'ACN, l'AN2V, la FIEEC, le GICAT, le GICAN, HEXATRUST.

A travers ses adhérents, le CICS représente plus de 1000 entreprises actives en sécurité réalisant plus de 80% du CA de la filière :

ACN :
Alliance pour la confiance numérique

AN2V :
Association nationale de vidéoprotection

FIEEC :
Fédération des industries électriques, électroniques et de communication

GICAT :
Groupement des industries de défense et de sécurité terrestres et aéroterrestres

GICAN :
Groupement des industries de constructions et activités navales

HEXATRUST :
Groupement d'entreprises du Cloud computing et de la cybersécurité

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

CICS
Conseil des Industries
de la Confiance et de la Sécurité

www.cics-org.fr

Jacques Roujansky, Délégué Général
jroujansky@cics-org.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