

Observatoire de la Filière Industrielle de Sécurité

2022



Etude commanditée par le **GICAT**, l'**ACN**, le **Ministère de l'Intérieur**,
le **SGDSN** et la **DGE**

en appui aux travaux du Conseil Stratégique de la Filière des Industries de Sécurité.



Etude réalisée par

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. De précédentes versions de cet Observatoire ont été réalisées en 2020 et 2018 par DECISION Etudes & Conseil.



Sommaire

Éléments clefs.....	3
I) Présentation de la filière.....	8
1. Sécurité physique, électronique et cybersécurité - trois domaines complémentaires et de plus en plus inter-corrélés.....	8
2. Méthodologie	10
II) Une filière importante et dynamique	12
1. L'industrie de sécurité est l'industrie française qui a la croissance la plus forte	12
2. L'industrie de sécurité est la filière industrielle la plus productive.....	13
3. L'industrie de sécurité est une filière industrielle française à part entière	14
4. Les acteurs français sont à la pointe en matière de compétences et de R&D	15
5. La croissance d'industrie de sécurité s'inscrit dans une dynamique mondiale.....	15
6. Une concurrence de plus en plus forte de la part de acteurs étrangers	15
7. Conclusion - Une filière à très fort potentiel	16
III) Les chiffres clés de la filière.....	17
1. La filière française par rapport aux autres filières de sécurité mondiale.....	17
2. Les principaux segments de la filière française	18
3. Analyse par sous-segment.....	20
1. Taille et croissance 2018-2021	21
2. Emplois en 2021	22
3. Nombre d'entreprises en 2021	23
4. Tendances de marché sur la période 2018-2021	24
1. De nombreux mouvements de fusions-acquisitions.....	24
2. Les levées de fonds des start-ups	28
3. Les principales entreprises en faillites.....	28
IV) Les tendances	29
1. Une filière résiliente face à la crise du COVID.....	29
1. 2020 : La filière face à la crise.....	29
2. Depuis 2021, la filière renoue avec une forte croissance portée par des tendances structurelles solides et durables.....	30
3. 6 nouvelles opportunités de croissance pour les années à venir	31
2. Les enjeux des grands événements.....	32
3. Les tendances technologiques	33
4. Transformation digitale & miniaturisation : Vers des offres globales de Security as a Service	38
5. Les 5 projets structurants du Comité stratégique de filière	39
6. Matrice FFOM de la Filière Industrielle de Sécurité en France	40
A propos du CSF.....	42
A propos de DECISION Études & Conseil	43



Éléments clefs

La filière industrielle de sécurité en France en 2021 c'est :

- **31,9 milliards d'euros de chiffre d'affaires**, soit 4,3% de croissance annuelle moyenne entre 2016 et 2021
- **12,9 milliards d'euros de valeur ajoutée**
- Un total de **157 000 employés**
- Un CA réparti à **40% pour la Sécurité électronique**, **31% pour la Sécurité physique** et **29% pour la Cybersécurité**

Les entreprises industrielles françaises de la sécurité représentent dans le Monde en 2021

- **43,4 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, Capgemini, Sopra Steria), et de la sécurisation des paiements (Worldline).
- **20,7 milliards d'euros de chiffre d'affaires à l'international**, soit environ **48%** du CA total
(CA exporté depuis la France et CA réalisé à l'étranger par des entreprises détenues par des capitaux français)
- **9,2 milliards d'euros de chiffre d'affaires à l'export**, soit environ **29%** du CA total

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

- **4,3%** de croissance annuelle moyenne en France sur la période 2016-2021, contre **0,6%** pour le PIB français
- Parmi les filières industrielles françaises, **c'est la filière industrielle de sécurité qui bénéficie de la croissance la plus forte derrière l'industrie chimique.**
- **La croissance annuelle moyenne de la filière est au dessus des 5% depuis 10 ans sauf en 2020 du fait de la pandémie de la COVID 19. Toutefois l'industrie a bien rebondi en 2021 avec 5% de croissance annuel. Cette tendance devrait se maintenir sur la période 2022-2025** 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 **33,4 milliards d'euros de chiffre d'affaires en 2022 (estimations).**

La filière industrielle de sécurité regroupe un écosystème d'entreprises de toutes tailles en 2021

- **4 402 entreprises** dans la filière en France
- Dont **90 grandes entreprises**
- Dont **91 ETI** (Entreprises de Taille Intermédiaire)
- Dont **1 723 PME** (Petites et Moyennes Entreprises)
- Dont **2 498 micro-entreprises**, générant moins de 2 millions de CA en 2021



Éléments clefs

FONDAMENTAUX 2021

CA MONDE	43,4 MDS €
CA HORS DE FRANCE	11,5 MDS €
CA FRANCE	31,9 MDS €
DONT CA EXPORT	9,2 MDS €
DONT CA ENTREPRISES FRANÇAISES	23,6 MDS €
VA FRANCE	12,9 MDS €
MARCHÉ FRANÇAIS	~30 MDS €

Source : DECISION Etudes & Conseil

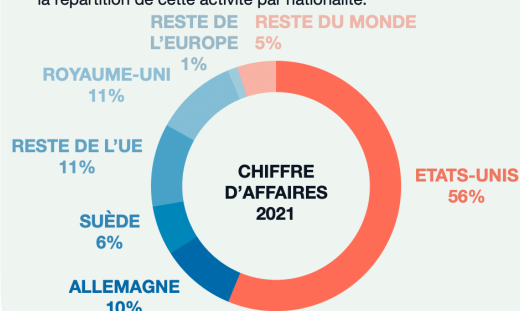
CROISSANCE 2018-2021

3,8%

157 000
EMPLOIS EN FRANCE

LES ENTREPRISES ÉTRANGÈRES PRÉSENTES EN FRANCE

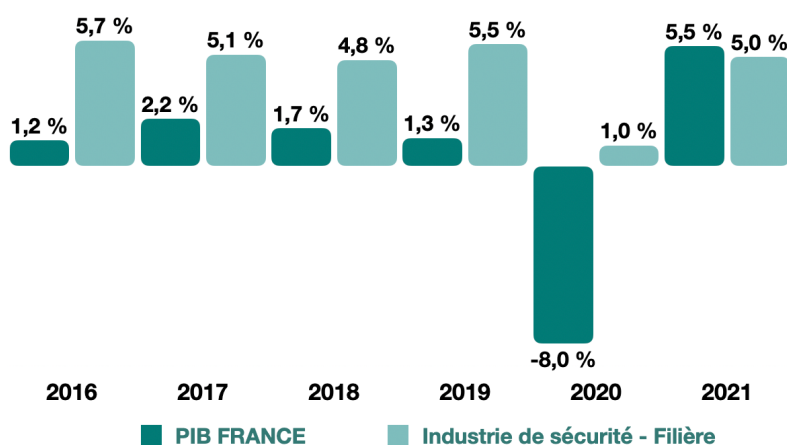
L'activité des entreprises de capitaux étrangers présentes en France correspond à 26% du CA FRANCE produit par la filière en 2021, soit 8,3 milliards d'euros. Le diagramme ci-dessous montre la répartition de cette activité par nationalité.



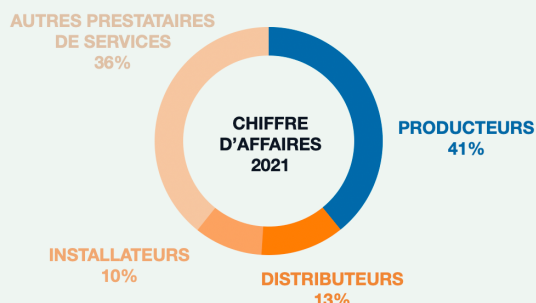
Source : DECISION Etudes & Conseil

CROISSANCES COMPARÉES 2016-2021

Source : DECISION Etudes & Conseil

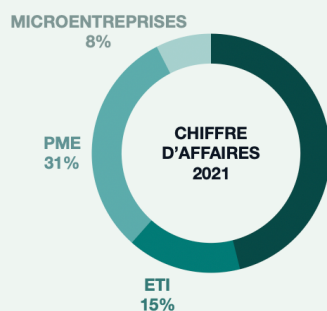


ANALYSE PAR TYPE D'ENTREPRISES

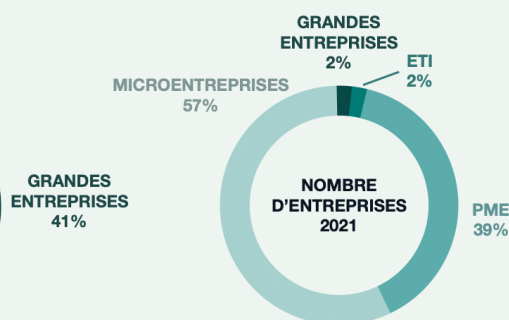
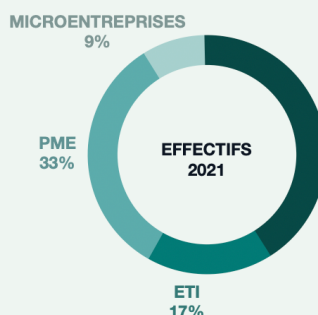


Source : DECISION Etudes & Conseil

ANALYSE PAR TAILLE D'ENTREPRISES



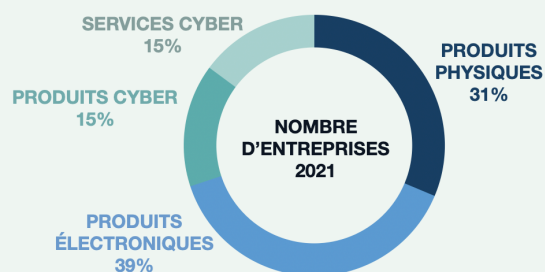
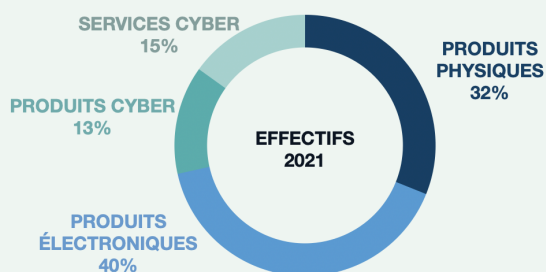
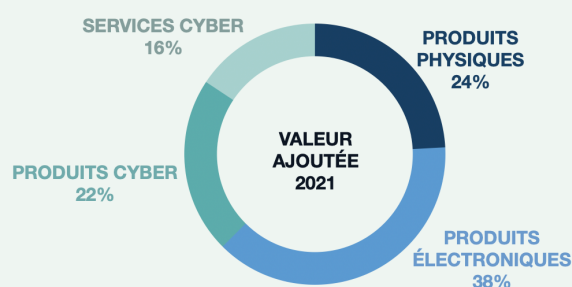
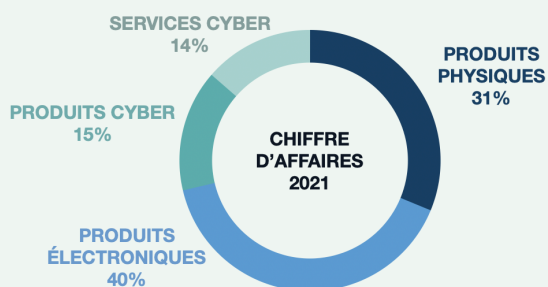
Source : DECISION Etudes & Conseil





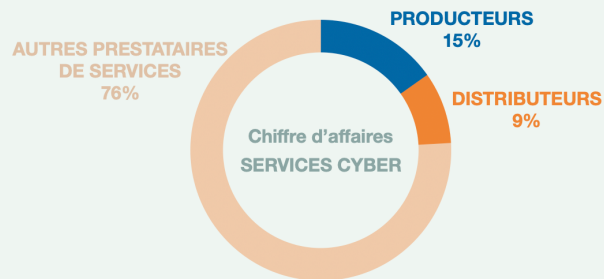
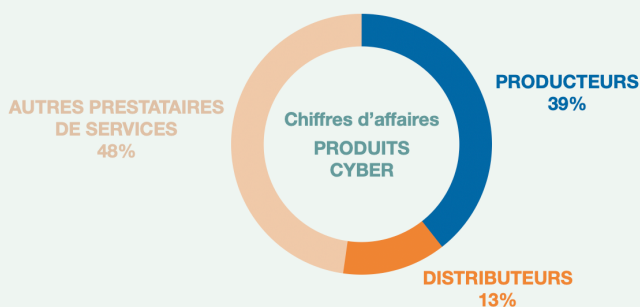
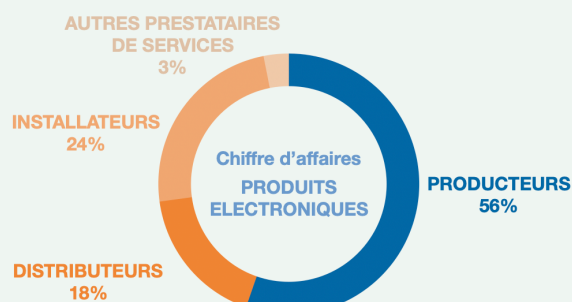
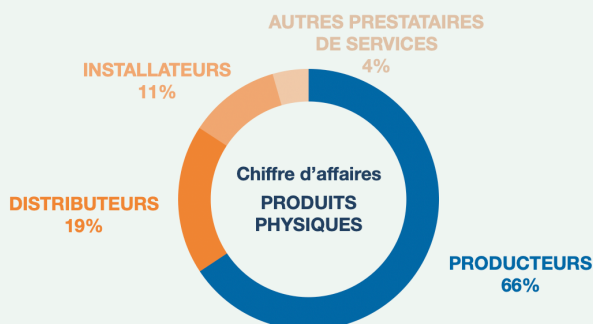
Éléments clefs

LES PRINCIPAUX SEGMENTS DE L'INDUSTRIE DE SÉCURITÉ



Source : DECISION Etudes & Conseil

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



Source : DECISION Etudes & Conseil



Éléments clefs

TOP 10 ACTEURS FRANCE - 2021

NATIONALITÉ	N°	ENTREPRISE	CA INDUSTRIE SÉCURITÉ FRANCE	CA INDUSTRIE SÉCURITÉ MONDE	N° MONDE
	1	THALES	2319 M€	5872 M€	3
	2	AIRBUS	1858 M€	3235 M€	4
	3	NAVAL GROUP	504 M€	504 M€	10
	4	HONEYWELL	499 M€	6450 M€	2
	5	ATOS	453 M€	1149 M€	7
	6	IDEMIA	380 M€	2200 M€	6
	7	ORANGE CYBERDEFENSE	369 M€	883 M€	9
	8	ASSA ABLOY	363 M€	10330 M€	1
	9	DESCOURS & CABAUD	360 M€	1380 M€	8
	10	API GROUP	359 M€	2813 M€	5

Source : DECISION Etudes & Conseil

N°	TOP 10
1	Thales est le leader français de la sécurité à travers son activité historique <i>Thales Défense et Sécurité</i> mais aussi son activité <i>Thales Identité & Sécurité Numériques</i> 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 de Moog (activités liées à l'aide à la navigation uniquement), de Onewelcome, d'Advanced Acoustic Concept, de S21sec, et d'Excelium, tous les 5 rachetés en 2021 et 2022.
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. Sa filiale Apsys est prise en compte.
3	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.
4	Honeywell (Etats-Unis) est fortement présent en France et est l'un des leaders sur les segments des EPI (Equipements de Protection Individuels), de la détection d'intrusion et alarmes, du contrôle d'accès et de la sécurité incendie à travers ses marques Security, Safety et Analytics.
5	Atos est l'un des leaders français de la cybersécurité avec Thales, Idemia, Orange Cyberdefense et IBM, à travers sa BU Big Data & Cybersecurity. Atos s'est séparé de Worldline, leader mondial de la sécurisation des paiements, entre 2019 et 2022. Atos a racheté Air-Lynx en 2018 et Idnomic en 2019. Atos a été très actif récemment avec le rachat de 7 sociétés de la filière entre 2020 et 2022, notamment Paladion ainsi que la BU Digital Security d'Econocom.
6	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.
7	Orange Cyberdefense (OCD) est une filiale d'Orange spécialisée dans les prestations de services en cybersécurité. En 2021, l'entreprise comptait 2 300 collaborateurs de par le monde et bénéficie d'une croissance fulgurante depuis 2013 (>50% /an en moyenne depuis 2013). En 2019, OCD a fait l'acquisition de l'entreprise néerlandaise SecureLink.
8	ASSA ABLOY (Suède) est un leader mondial des solutions d'interdiction et de contrôle d'accès, physiques et électroniques. En 2020-2021, Assa Abloy a racheté 3 entreprises de la filière : Agta record, Tagsys, et Alcea.
9	Descours & Cabaud est un groupe familial français de distribution de fournitures à destination d'une clientèle de professionnels de l'industrie et du bâtiment. Descours & Cabaud distribue en particulier des équipements de protection individuelle (EPI). Entre 2020 et 2022, le groupe a racheté Sintimex, BTN-Henny Van Ommeren et Safeline.
10	API group est un spécialiste de la sécurité incendie avec plus de 200 implantations dans le monde. Grâce au rachat de Chubb en 2021 auprès de Carrier, l'entreprise devient un acteur incontournable en France. Ce rachat lui permet aussi d'accéder à la dixième place de notre classement.

TOP 1-10 ACTEURS FRANCE



TOP 10-20 ACTEURS FRANCE



TOP 20-30 ACTEURS FRANCE



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

TOP 10-20 : Ces acteurs réalisent un CA Industrie de sécurité compris entre 250 M € et 350 M €

TOP 20-30 : Ces acteurs réalisent un CA Industrie de sécurité compris entre 180 M € et 250 M €

Source : DECISION Etudes & Conseil

DECISION
ETUDES & CONSEIL

N°	TOP 10-30
11	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. Desautel a signé un contrat historique en mai 2021 pour la livraison de 370 camions de pompiers pour 300 M€ livrés à l'Ukraine.
12	Sopra Steria est l'un des leaders français des services de cybersécurité et a racheté entre 2020 et 2022 SodiFrance, EVA Group et CS Group.
13	Groupe RG est l'un des leaders français sur le segment des EPI*. Il a racheté 5 entreprises en 2020-2022, dont l'ETI EPI Center.
14	IBM est un leader mondial en matière de cybersécurité et de confiance numérique. Il a racheté en 2020-2022 Spanugo, StackRox et ReaQta.
15	Equans (Bouygues) - Anciennement ENGIE Solutions , 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.
16	Docapost fait partie de la branche numérique du groupe La Poste. Créée en 2007, l'entreprise propose des services d'échanges sécurisés de documents. L'entreprise a racheté 5 PME de la filière entre 2020 et 2022.
17	IN Groupe (ex Imprimerie Nationale) est l'un des leaders français de l'identité numérique et a racheté Nexus en 2020.
18	La DEF est l'un des leaders français sur le segment des EPI*.
19	Delta Plus est l'un des leaders français sur le segment des EPI*. Sur la période 2020-2022, l'entreprise a racheté 5 PME de la filière.
20	Oberthur Fiduciaire est le leader français de la production de billets de banque et l'un des principaux acteurs en matière de documents sécurisés.
21	Siemens (Allemagne) est fortement implanté en France sur le segment de la sécurité incendie. Siemens fournit également des systèmes de contrôle d'accès et d'alarme.
22	Accenture est une société de conseil spécialisée notamment en cybersécurité. En 2020-2022, Accenture a racheté 3 entreprises, dont AFD.TECH.
23	Safran garde une activité de sécurité significative depuis la vente de sa filiale Morpho en 2017 (devenue Idemia), notamment en observation large zone et en optronique. Safran détient Lynred à travers une Joint Venture avec Thales. Entre 2020 et 2022, Safran a racheté Orolia et CILAS.
24	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.)
26	Spie est présent sur les segments de la sécurité industrielle et notamment de la sécurité face aux incendies.
25	Vinci est l'un des leaders français de la sécurité incendie mais est également présent sur différents segments électronique et cyber. Vinci a racheté Sysoco en 2019 ainsi que les activités IT (dont cyber) de l'allemand Kontron en 2022. Vinci a également repris les activités de SIEPEL suite à un redressement judiciaire en 2021 à travers Cegelec défense.
27	Securitas est une multinationale suédoise qui exerce depuis 1934 dans le domaine de la sécurité privée. Elle propose à l'international des prestations de gardiennage, mise à disposition de patrouilles permanentes et ponctuelles. En 2021 la firme a racheté le grand groupe Stanley Security pour se positionner sur la sécurité électronique.
28	France Sécurité est l'un des leaders français sur le segment des EPI*. L'entreprise appartient au groupe Bunzl (Royaume-Uni).
29	Dassault Aviation est le leader français des avions de sécurité, notamment utilisés par les douanes.
30	Legrand est un groupe industriel français présent sur les segments de la sécurité incendie et du contrôle d'accès.

* EPI : Equipements de Protection Individuels

Parmi les principaux acteurs de la filière, on trouve également Legrand, Hager Group, Mirion Technologies, Exail Technologies (Groupe Gorgé), Rexel, Sonepar, Econocom, Carrier, Worldline, Lyreco, Dirickx, Cap Gemini, Tessi, Dormakaba, 3M France, Fichet Group (Gunnebo), Scutum, Exclusive Group, Dom security (Group SFP), ST Microelectronics, Coverguard, Fortal, et CNIM Group.



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 filière 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 (type Teorem, Hoox ou encore PMR), 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 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.). En 2021, 22% du CA de la sécurité électronique est ainsi réalisé par des installateurs.
- 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 (audit et conseil, conception, mise en place, exploitation, formation), et les produits cyber (logiciels et solutions associées) : anti-virus, pare-feux, etc. Plusieurs produits cyber ont aussi une composante physique et électronique (éléments sécurisés, HSM, 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...

Interdiction physique d'accès

Clôtures, enceintes, serrurerie, coffres forts,
portes blindées et coupe-feu, vitres anti-
effraction...

Equipements et fournitures

Armes, munitions, outils de déminage, de
décontamination...

Equipements physiques de sécurité incendie

Extincteurs, sprinklers, désenfumage, lances,
tuyaux, robinets...

Produits électroniques

Contrôle d'accès

Systèmes complets

Détection de produits dangereux

ou illicites ou de personnes dissimulées :
NRBCE, scanner, diffraction X, tomographes,
spectromètres...

Communications sécurisées

et systèmes d'alerte publique (PMR, SAIP...)

Identification & Authentification des personnes

Biométrie, cartes à puces, badges, cartes ID,
reconnaissance de véhicules, lutte contre la
contrefaçon

Observation locale

Caméras et capteurs (visibles et IR,
acoustique...), lidars, radars, sonars...

Commande contrôle Aide à la décision

Postes de commandements, outils de gestion
de l'information, outils de simulation, de
modélisation, de cartographie... Y compris
shelters

Identification & Authentification des produits

Papiers sécurisés, billets de banque...

Observation large zone

Systèmes optroniques, radars, imagerie par
satellite

Détection d'intrusion et alarme

Traçage et localisation

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

Renseignement et Collecte d'information

Interception, écoute, localisation, analyse et
visualisation des données (big data)...

Equipements électroniques de sécurité incendie

Détection, alarme...

Cybersécurité

Produits / Logiciels

Gouvernance cyber

Systèmes de gestion, SIEM

Gestion des identités et des accès

Sécurité des données

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

Sécurité des applications

Développement logiciels, OS sécurisés, plateformes de bug bounty

Sécurité des infrastructures

Firewalls, antivirus, anti-dos, détection d'intrusion, cyberthreat, sécurité
des communications (téléphonie, visioconférence et messagerie),
plateformes sécurisées de télétravail, Cloud de confiance, blockchain

Sécurité des produits & équipements

Elements sécurisés, HSM, sécurité des IoT

Services

Audit, planning et conseil cyber

Mise en oeuvre cyber

Sécurisation de l'infogérance et exploitation

Tiers de confiance, gestion du contenu et de la réputation, gestion de
la continuité et récupération

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 1 471 entreprises parmi les 4 402 que compte la filière industrielle de sécurité. Cette base de données prend en compte :

- La totalité des grands groupes de la filière (90/90);
- La totalité des entreprises de tailles intermédiaires (ETI) de la filière (91/91);
- La majorité des PME de la filière (1 088 / 1 723);
- Les micro-entreprises et start-ups les plus remarquables et innovantes (202 / 2 498).

Ainsi, bien que seul 33% 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.

BASE DE DONNÉES

~85%



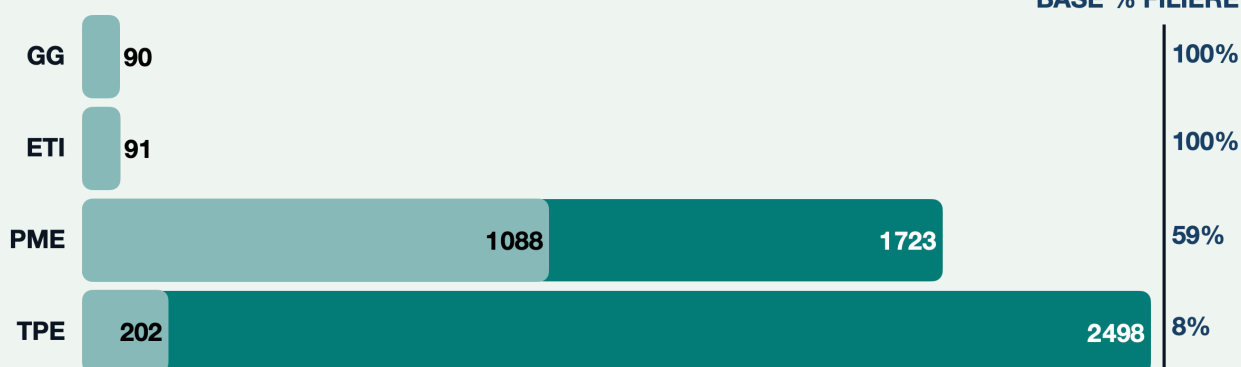
**CHIFFRE
D'AFFAIRES**

RESTE DE LA FILIERE

~15%

NOMBRE D'ENTREPRISES

Segmentées dans la Filière industrielle de sécurité
(Hors services privés)



+ 1265 TPE et PME dans la filière mais non segmentées

- **GG** = Grande entreprise (Groupe) : Dans le monde, CA > 1,5 milliard d'euros ou nombre d'employés > 1 500
- **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

NOTE MÉTHODOLOGIQUE

Critère de nationalité des capitaux des entreprises de la filière. Cet Observatoire analyse les entreprises selon la nationalité de leurs capitaux. Le critère retenu à cet effet est celui de la nationalité du ou des *actionnaire(s) principal(aux) en tête de pont*.

- ▶ **En tête de pont** signifie que DECISION remonte 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 DECISION considère 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).



II) Une filière importante et dynamique

COMPARAISON DES FILIÈRES INDUSTRIELLES FRANÇAISES

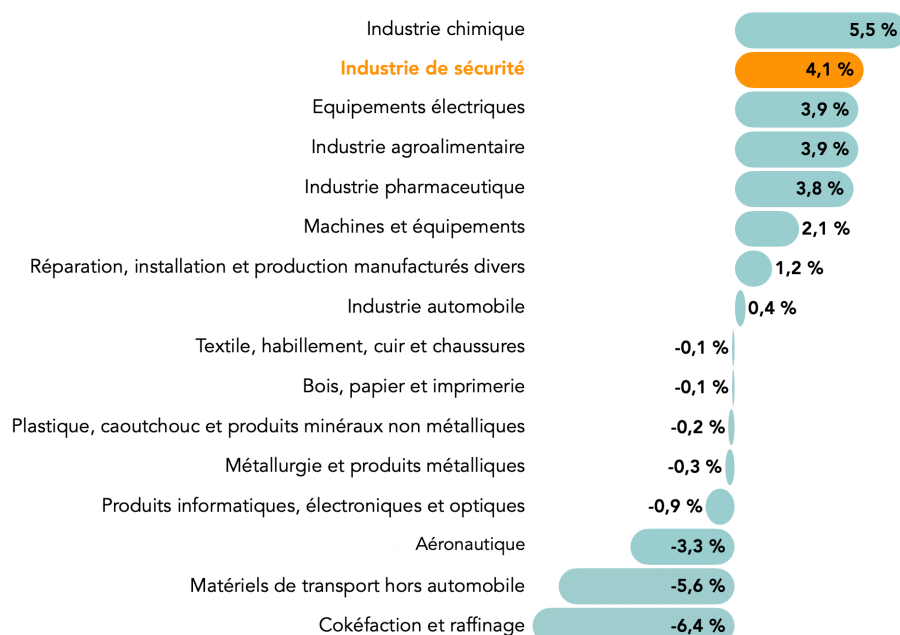
Dans ce chapitre, la filière industrielle de sécurité est comparée aux autres industries françaises sur la base des chiffres publiés par Eurostat et l'OCDE sur les industries manufacturières françaises.

La segmentation utilisée par Eurostat 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 derrière l'industrie chimique

Sur la période 2016-2020, l'industrie de sécurité est la filière industrielle française avec le second plus fort taux de croissance (4,1% par an). Toutefois, ce chiffre est en baisse par rapport à la période 2013-2016 où l'industrie de sécurité affichait en moyenne un taux de croissance de 5,9%, soit le plus important taux des différentes industries. L'industrie chimique la devance durant la période 2016-2020 avec un taux de croissance moyen de 5,5%. Trois autres secteurs sont au coude à coude avec l'industrie de la sécurité sur cette période: les équipements électriques, l'industrie agroalimentaire et l'industrie pharmaceutique. L'industrie manufacturière française dans son ensemble a crû à 0,8% de croissance annuelle moyenne entre 2016 et 2020 d'après l'INSEE.

CROISSANCE ANNUELLE MOYENNE DES FILIÈRES FRANÇAISES SUR LA PÉRIODE 2016-2020



Sources : DECISION, Eurostat, GIFAS



II) Une filière importante et dynamique

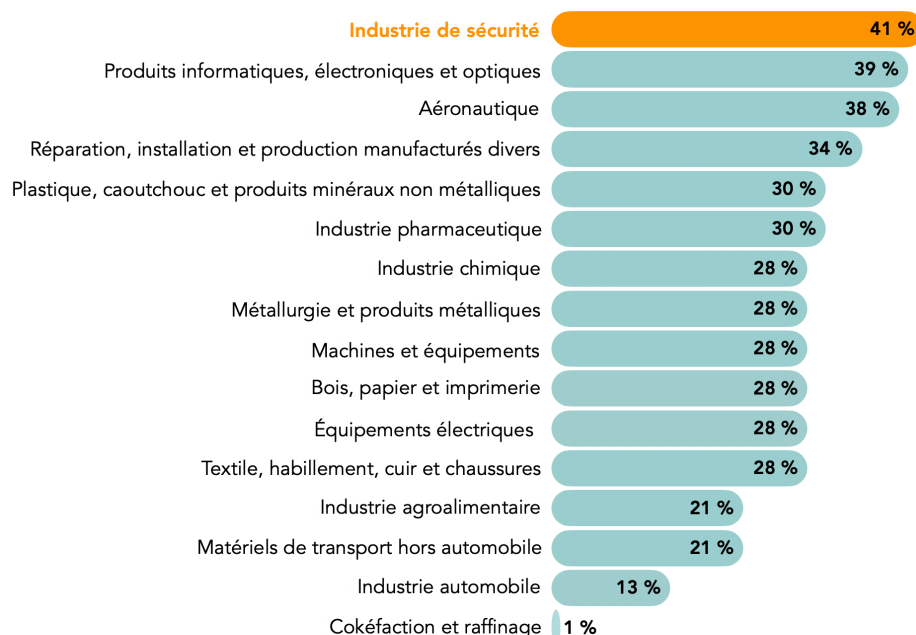
2.2 L'industrie de sécurité est la filière industrielle avec le plus fort taux de valeur ajoutée

L'industrie de sécurité est la filière la plus productive avec un taux de valeur ajoutée de 41% en 2020. (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 (13% du CA total en 2021), ou à travers les services de cybersécurité (conseil, audit, formation, etc. qui ont représenté 14% du CA total en 2021). 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 facteurs décrits ci-dessous sont les principales raisons pour lesquelles l'industrie de sécurité occupe la première place.
- Les produits électroniques de sécurité correspondent à 40% du chiffre d'affaires total de la filière de sécurité en 2021. 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 chaîne de valeur est réalisée en Asie, ce phénomène ne s'applique que peu au segment de la sécurité qui maintient autant que faire se peut toutes les étapes de la production en France en raison de sa proximité avec les secteurs régaliens. D'autres filières françaises se concentrent plus fortement sur des activités d'intégration en amont de la chaîne de valeur et sur des activités d'ingénierie pure (design, développement, etc.). Etant donné qu'une grande partie de la chaîne de valeur de l'industrie électronique de sécurité est réalisée depuis la France, le taux de valeur ajoutée augmente.
- Enfin, la cybersécurité dans son ensemble correspond à près de 29% du CA total de la filière de sécurité en 2021. 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.) expliquant un taux de valeur ajoutée très élevé.

TAUX DE VALEUR AJOUTÉE (VA/CA) DES FILIÈRES FRANÇAISES EN 2020



Sources : DECISION, Eurostat, GIFAS

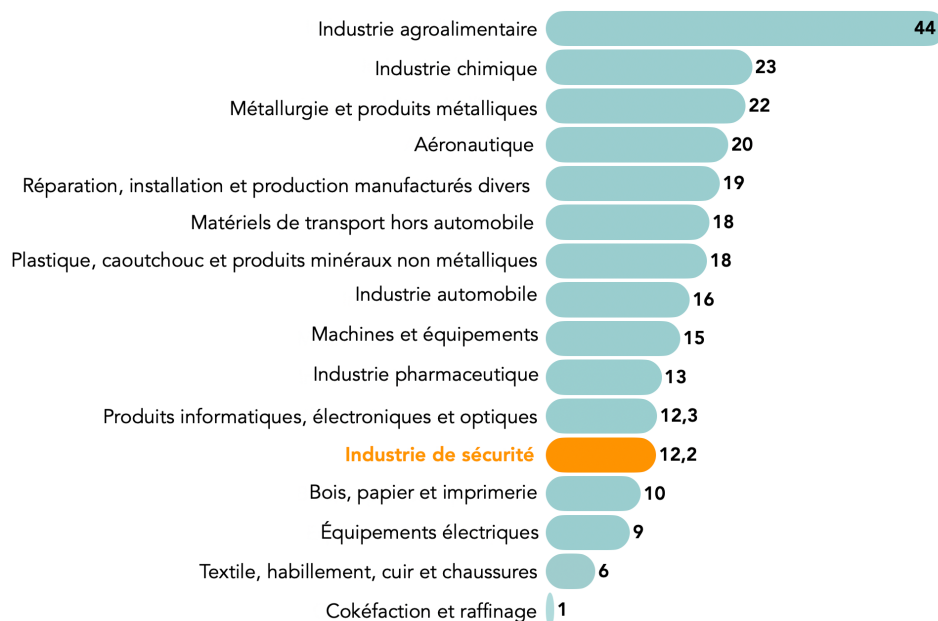


II) Une filière importante et dynamique

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

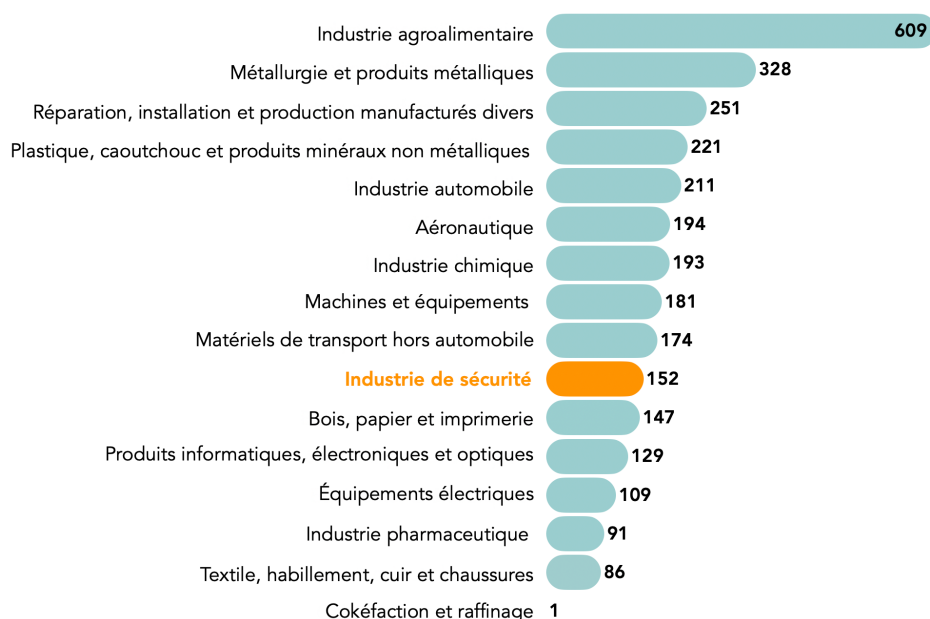
En 2020, en termes de valeur ajoutée, la filière industrielle de sécurité reste par rapport à 2017 à la 12ème place des industries manufacturières françaises (sur 16), entre la filière produits informatiques, électroniques et optiques, et la filière Bois, papier et imprimerie. En termes d'emploi, la filière industrielle de sécurité reste aussi par rapport à 2017 à la 10ème place des industries manufacturières françaises (sur 16), entre l'industrie Bois, papier et imprimerie et l'industrie produits informatiques, électroniques et optiques.

VALEURS AJOUTÉES DES FILIÈRES FRANÇAISES EN 2020 (MDS €)



Sources : DECISION, Eurostat, GIFAS

EMPLOIS DES FILIÈRES FRANÇAISES EN 2020 (EN MILLIERS D'EMPLOIS)



Sources : DECISION, Eurostat, GIFAS



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, la majorité des grandes entreprises et ETI 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 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 joue notamment un rôle clef dans l'élaboration de l'infrastructure européenne de communication quantique (EuroQCI).

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**. Accélérée par la crise du COVID-19 en 2020, les entreprises et administrations du monde entier digitalisent leurs processus et interconnectent les réseaux de données. Cette transformation génère de la croissance auprès des industries de sécurité pour deux raisons. D'une part, la cybersécurité devient progressivement 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 lesquelles la France est souvent très bien positionnée aussi bien en termes d'acteurs industriels que de savoir-faire scientifique : biométrie comportementale, innovations associées aux éléments sécurisés, développements cryptographiques, analyse en temps réel des données d'observation locale 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. DECISION estime ces croissances à respectivement 5,6% et 10,6% par an sur la période 2018-2021.

2.6 Une concurrence croissante de la part des acteurs étrangers

Les acteurs de nationalité française génèrent 74% du chiffre d'affaires de l'industrie de sécurité en France, soit 23,6 milliards d'euros en 2021. Autrement dit, les acteurs étrangers de la filière réalisent 26% du chiffre d'affaires de la filière en France, soit 8,3 milliards d'euros en 2021. 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 elle peut paraître encore assez élevée, **la part de la richesse produite en France par des acteurs français baisse régulièrement** depuis 2013 et devrait continuer à baisser sur la période 2021-2025 face à la présence de plus en plus forte d'acteurs étrangers, principalement chinois et américains.

De même que pour la production en France, **le poids des acteurs étrangers sur le marché français est important** : il est estimé entre 40% et 50%*. 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.

En revanche, **si des rachats significatifs d'entreprises françaises par des acteurs étrangers ont marqué la période 2016-2020, cette tendance c'est inversée sur la période 2020-2022**. En effet, depuis 2020, les entreprises françaises ont acheté des entreprises étrangères en nombre et pour des montants bien supérieurs aux achats d'entreprises françaises par des entreprises étrangères.

Les rachats les plus significatifs d'entreprises françaises par des entreprises étrangères sur la période 2020-2022 sont ceux d'Akka Technologies par Adecco (Suisse), de Finsecur par Jade Bird Fire (Chine), d'AFD.TECH par Accenture (Etats-Unis) et de Cover Guard par CSW Industries (Etats-Unis).

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 conduit naturellement les entreprises et les administrations françaises à se tourner vers des offres étrangères. En effet, dans un contexte général de stagnation de la croissance 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 (en raison de subventions, d'économies d'échelles 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 tend à 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).

La crise du COVID et en particulier les pénuries de matériels médicaux et de semi-conducteurs ont généré **une prise de conscience**, y compris dans l'administration, **de la nécessité de préserver une souveraineté industrielle française**. **Les entreprises de la filière ne constatent cependant pour le moment pas d'évolution notable dans les pratiques** notamment à l'occasion des JO 2024. Un lobby est également à l'oeuvre de la part d'entreprises étrangères pour se faire considérer comme françaises dès lors qu'elles disposent de sièges sociaux en France.

Le **trijumpe standardisation-certification-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. Si ce trijumpe est en place dans la plupart des segments de la filière (sécurité incendie, cybersécurité avec l'ANSSI et l'ENISA), un manque de commande publique forte et unifiée se fait ressentir dans la plupart des segments. A cet égard, **la création d'un équivalent de la DGA et de la BITD en matière de sécurité permettrait de structurer une commande publique forte et d'assurer un suivi de la base industrielle française permettant de répondre à la demande**.

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, 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 6% par an en moyenne sur la période 2018-2021, contre 3,8% pour la France.

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 37% des budgets mondiaux consacrés à la défense en 2021, l'OTAN compte pour 53% du total et la Chine, deuxième pays du monde, pour environ 13%).

L'industrie Chinoise est d'ores-et-déjà la deuxième mondiale. Elle croît 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) (Sugon), éléments sécurisés (Shanghai Huahong, Shanghai Fudan Microelectronics, 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.

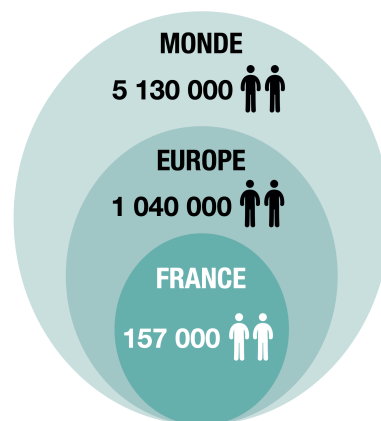
LA FILIÈRE AU NIVEAU MONDIAL

Chiffre d'affaires

Pays / Region	Chiffre d'affaires (Milliards d'euros)		Taux de Croissance Annuelle Moyenne 2018-2021
	2018	2021	
Europe	112	128	4,5 %
Etats-Unis	155	183	5,6 %
Chine	89	120	10,6 %
Reste du Monde	176	201	4,6 %
Monde	532	632	5,9 %

Source : DECISION Etudes & Conseil

Effectifs en 2021





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 et la Turquie.
- En Europe, la France dispose de la plus importante filière sécurité, les deux autres principales industries étant celles de l'Allemagne et du Royaume-Uni. On trouve ensuite la Suède et l'Italie puis les Pays-Bas, l'Espagne et la Belgique.

La France se situe donc à la 3^{ème} place au niveau mondial, loin derrière les Etats-Unis et la Chine, à une position proche de celle des industries japonaise, allemande et anglaise et challengée par les industries sud-coréenne et israélienne en forte croissance.

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 340 millions de caméras de sécurité publiques et privées installées sur son territoire en 2020 (dont certaines avec reconnaissance faciale) et 50 millions de nouvelles caméras installées rien que pour l'année 2021.

3.2 Les principaux segments de la filière française

Le diagramme page suivante regroupe tous les chiffres des principaux segments de la filière de sécurité sur la période 2018-2021. Les produits électroniques demeurent le premier segment de la filière avec 40% du chiffre d'affaires en 2021. Cependant, avec une croissance annuelle moyenne près de 10% sur la période 2018-2021, la cybersécurité prend de plus en plus d'importance dans la filière et représente en 2021 près de 30% de son chiffre d'affaires total, soit 9,1 milliards d'euros. En comparaison, la cybersécurité représentait moins de 5% du chiffre d'affaires de la filière au début des années 2000 et devrait égaler en chiffre d'affaires les produits électroniques à l'horizon 2025-2030.

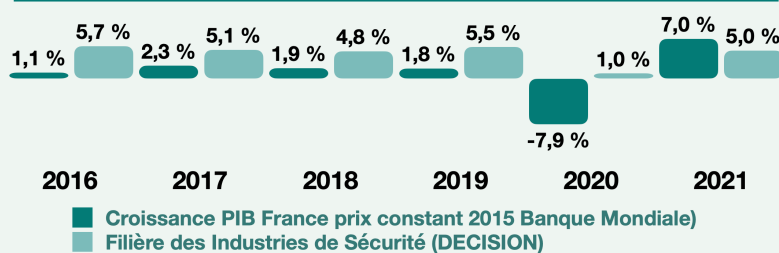
Ces tendances laisseraient supposer qu'il existe une séparation nette entre les différents segments -aussi bien en termes de produits que d'acteurs- et que la croissance de la cybersécurité serait décorrélée de celle des produits électroniques et physiques. Il n'en est rien et au contraire, les produits 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 4,5% par an sur la période 2016-2021 contre 1,0% 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;
- Un fort taux d'exportation de la filière dans son ensemble vers des pays en forte croissance;
- 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.), de plateformes robotiques, de blockchain, d'analyse en temps réel des données d'observations locales et large zone, etc.;
- La crise du COVID en 2020 a été un moteur de croissance important pour le segment des vêtements de protection (Equipements de Protection Individuels EPI);
- Enfin, le besoin des sécuriser les objets connectés et en particulier les automobiles connectées (les perspectives sur les autres marchés d'objets connectés tardant quant à elles à se concrétiser depuis plusieurs années : safe city, etc.).

Sur la période 2021-2025, cette croissance devrait se maintenir en dépit des probables récessions associées aux pénuries énergétiques. En effet, les fondamentaux de la croissance de la filière demeurent : demande de produits et de services de cybersécurité, fort taux d'exportation et innovations technologiques générant de nouvelles applications, développement des objets connectés. La tenue en France de la coupe du monde de rugby en 2023 et des Jeux Olympiques d'été en 2024 devrait également soutenir la croissance de la filière.

CROISSANCES COMPARÉES 2016-2021



Source: DECISION Etudes & Conseil



III) Les chiffres clés de la filière

CHIFFRES DES PRINCIPAUX SEGMENTS DE LA FILIERE SUR LA PERIODE 2018-2021

	TOTAL FILIERE INDUSTRIELLE	PRODUITS PHYSIQUES	PRODUITS ELECTRONIQUES	PRODUITS CYBER	SERVICES CYBER
Chiffre d'affaires (M€)					
2021	31 900 M€ (100%)	10 000 M€ (31%)	12 780 M€ (40%)	4 800 M€ (15%)	4 340 M€ (14%)
Croissance 2020-2021	5,8%	3,6%	4,1%	13,9%	10,3%
2020	30 370 M€ (100%)	9 600 M€ (32%)	12 400 M€ (41%)	4 360 M€ (14%)	4 040 M€ (13%)
TCAM* 2018-2020	4,9%	2,8%	3,3%	14%	9,6%
2018	28 500 M€ (100%)	9 500 M€ (33%)	12 100 M€ (42%)	3 500 M€ (12%)	3 500 M€ (12%)
Nombre d'employés					
2021	157 000 (100%)	48 800 (31%)	63 500 (40%)	21 100 (13%)	23 700 (15%)
Valeur Ajoutée (M€)					
2021	12 900 M€ (100%)	3 100 M€ (24%)	4 930 M€ (38%)	2 800 M€ (22%)	2 020 M€ (16%)
* Taux de Croissance Annuel Moyen (TCAM)					

Source : DECISION Etudes & Conseil



III) Les chiffres clés de la filière

3.3 Analyse par sous-segment

Ce chapitre présente les chiffres de la filière selon les 30 segments détaillés. On y trouve les chiffres d'affaires des années 2018 à 2021, les emplois en 2021 ainsi que le nombre d'entreprises présentes sur chacun des segments en 2021.

La période 2018-2021 est bien sur marquée par la crise du COVID qui a affecté l'ensemble des segments de la filière.

- **Produits physiques.** Fait rare, la croissance du segment de la sécurité physique égale presque celle du segment électronique sur la période 2018-2021. En cause : la filière physique a mieux résisté à la crise du COVID que la filière électronique. Si certains segments se sont effondrés en 2020 (équipements et fournitures, interdiction physique d'accès, équipements physiques de sécurité incendie), le segment des vêtements de protection a vu sa croissance exploser du fait des applications sanitaires de Équipements de Protection Individuels (EPI). Cette croissance a bénéficié aux leaders français sur le segment des EPI : Groupe RG, Delta Plus et France sécurité. Les autres segments de la sécurité physique, très axés sur des applications régaliennes dont les commandes dépendent de projets pluriannuels dont le nombre et les montants croient depuis 2018, ont vu leur croissance préservée durant l'année 2020 (véhicules terrestres, hélicoptères, navires et plateformes robotiques de sécurité). Le segment des drones a traditionnellement l'une des plus fortes croissances de la filière. Bien qu'en baisse tendancielle, cette croissance s'est maintenue à 3% en 2020 et à plus de 5% les autres années. Enfin, le segment des avions de sécurité est en stagnation depuis de nombreuses années. Sur la période 2023-2030, la commande publique de 14 Falcon pour la Marine Nationale devrait faire renouer ce segment avec la croissance.
- **Produits électroniques.** Certains segments électroniques ont été particulièrement affectés par la crise du COVID en 2020. Le segment le plus touché étant celui des détection et alarme (y compris incendie) : ce segment a un marché majoritairement grand public et le télétravail a diminué temporairement la demande. Les segments dont le secteur du transport (aéroport, frontières) représente une grande partie du marché ont également été particulièrement touchés : contrôle d'accès, détection et inspection de produits ou de personnes, passeports... Parmi les segments les plus touchés, on trouve aussi les communications sécurisées et le suivi et traçage.

Au contraire, certains segments ont particulièrement bien résisté à la crise en 2020, en particulier les segments majoritairement exposés à des marchés régaliens dont la demande s'est maintenue sur l'année 2020 dans le cadre de programmes pluriannuels : observation large zone, commande-contrôle-aide à la décision, renseignement et collecte d'observation. Les besoins issus des services bancaires ont soutenu la demande dans le segment identification et authentification des personnes. Sur le segment d'identification et authentification des objets, le français Oberthur Fiduciaire a bénéficié d'une très belle croissance sur l'année 2020 malgré la crise. Enfin, le segment de l'observation et surveillance locale et le seul segment à forte composante « grand public » à avoir bien résisté à la crise du COVID avec une croissance de 2% en 2020.

- **Cybersécurité.** L'ensemble des segments de la cybersécurité ont maintenu une croissance supérieure à 5% en 2020 à l'exception de celui des formations en cybersécurité, particulièrement affecté par les restrictions. Les services de cybersécurité ont malgré tout été plus fortement affectés par les restrictions que les produits cyber avec une croissance qui a chuté de 10% en 2019 à moins de 6% en 2020.

Enfin, on observe une baisse tendancielle de la croissance de la cybersécurité sur la période 2019-2022. Cela tient simplement au fait que ce secteur commence à atteindre une taille conséquente avec plus de 10 Mds € réalisés depuis la France en 2021. La croissance se poursuit donc, mais les taux de croissance relatifs à la taille du secteur vont progressivement baisser en dessous de la barre des 10%, comme on l'observe déjà pour les services cyber. Signe de la très forte croissance de ce segment, le chiffre d'affaires généré en France par les produits cyber devrait doubler en 6-7 ans (entre 2016 et 2022-2023).

NOTE METHODOLOGIQUE

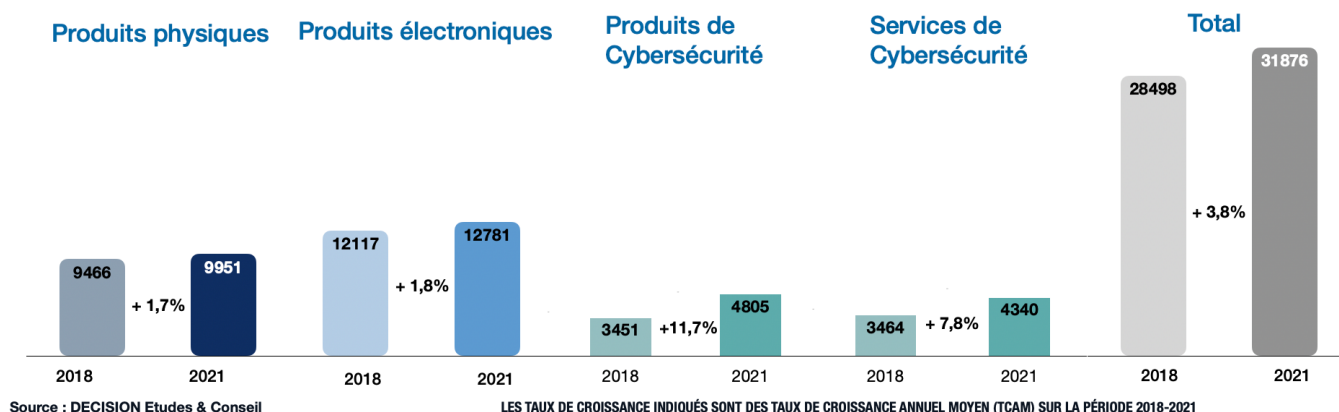
Depuis 2020, l'Observatoire de la filière de sécurité présente le détail des chiffres des 30 segments de la filière au niveau agrégé. En d'autres termes, ces chiffres ne sont pas seulement ceux de la base de données de DECISION, mais sont extrapolés pour être représentatifs de la filière française dans son ensemble.

Entre chaque édition de cet Observatoire, un travail d'analyse est 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, notamment à travers des interviews et des questionnaires en ligne. En conséquence de ces évolutions, les chiffres de l'Observatoire 2020 ne sont pas directement comparables avec ceux de l'Observatoire précédent.



III) Les chiffres clés de la filière

3.2.1 Taille et croissance 2018-2021



CHIFFRE D'AFFAIRES DE LA FILIÈRE INDUSTRIELLE DE SÉCURITÉ EN FRANCE PAR SEGMENT 2018-2021



PRODUITS PHYSIQUES
9 951 M€

PRODUITS ÉLECTRONIQUES
12 781 M€

PRODUITS DE CYBERSÉCURITÉ
4 805 M€

SERVICES DE CYBERSÉCURITÉ
4 340 M€

N° SEGMENT	CHIFFRE D'AFFAIRES SÉCURITÉ EN MILLIONS D'EUROS (2018-2021)	TCAM* 2018-2021
1.1.1.1 VÉHICULES TERRESTRES DE SÉCURITÉ	678 716	1,8 %
1.1.1.2 AVIONS, HÉLICOPTÈRES DE SÉCURITÉ	820 867	1,9 %
1.1.1.3 NAVIRES DE SÉCURITÉ	543 596	3,2 %
1.1.1.4 PLATEFORMES ROBOTIQUES	219 258	5,6 %
1.1.2 VÊTEMENTS DE PROTECTION	2 327 2 849	7,0 %
1.1.3 ÉQUIPEMENTS ET FOURNITURES	1 083 1 116	-1,0 %
1.1.4 INTERDICTION PHYSIQUE D'ACCÈS	1 906 2 043	-2,3 %
1.1.5 ÉQUIPEMENTS PHYSIQUES DE SÉCURITÉ INCENDIE	1 676 1 720	-0,9 %
1.2.1 SYSTÈMES ET CONTRÔLE D'ACCÈS ÉLECTRONIQUE	1 413 1 486	1,7 %
1.2.2 IDENTIFICATION DES PERSONNES	1 710 1 899	3,5 %
1.2.1.3 IDENTIFICATION ET AUTHENTIFICATION DES OBJETS	271 322	5,9 %
1.2.2 SYSTÈMES DE DÉTECTION	1 569 1 612	0,9 %
1.2.3 ALARME ET DÉTECTION INCENDIE	1 488 1 505	-0,4 %
1.2.4 DÉTECTION DE PRODUITS DANGEREUX	707 740	1,5 %
1.2.5 OBSERVATION ET SURVEILLANCE LOCALE	1 363 1 523	3,8 %
1.2.6 OBSERVATION ET SURVEILLANCE LARGE ZONE	491 531	2,6 %
1.2.7 SUIVI - TRAÇAGE - LOCALISATION	515 521	0,3 %
1.2.8 COMMUNICATIONS SÉCURISÉES	1 633 1 637	0,1 %
1.2.9 COMMANDE - CONTRÔLE - AIDE À LA DÉCISION	642 678	1,8 %
1.2.10 RENSEIGNEMENT - COLLECTE D'INFORMATION	297 344	5,1 %
2.0.1 GOUVERNANCE CYBER	538 748	11,6 %
2.0.2 GESTION DES IDENTITÉS ET DES ACCÈS	564 774	11,2 %
2.0.3 SÉCURITÉ DES DONNÉES	975 1 439	13,9 %
2.0.4 SÉCURITÉ DES APPLICATIONS	225 306	10,8 %
2.0.5 SÉCURITÉ DES INFRASTRUCTURES	827 1 158	11,8 %
2.0.6 SÉCURITÉ DES PRODUITS & ÉQUIPEMENTS	323 381	5,7 %
3.0.1 AUDIT - PLANNING - CONSEIL CYBER	1 490 1 857	7,6 %
3.0.2 MISE EN OEUVRE CYBERSÉCURITÉ	1 098 1 373	7,7 %
3.0.3 INFOGÉRANCE - EXPLOITATION	768 982	8,5 %
3.0.4 FORMATION EN CYBERSÉCURITÉ	108 127	5,5 %

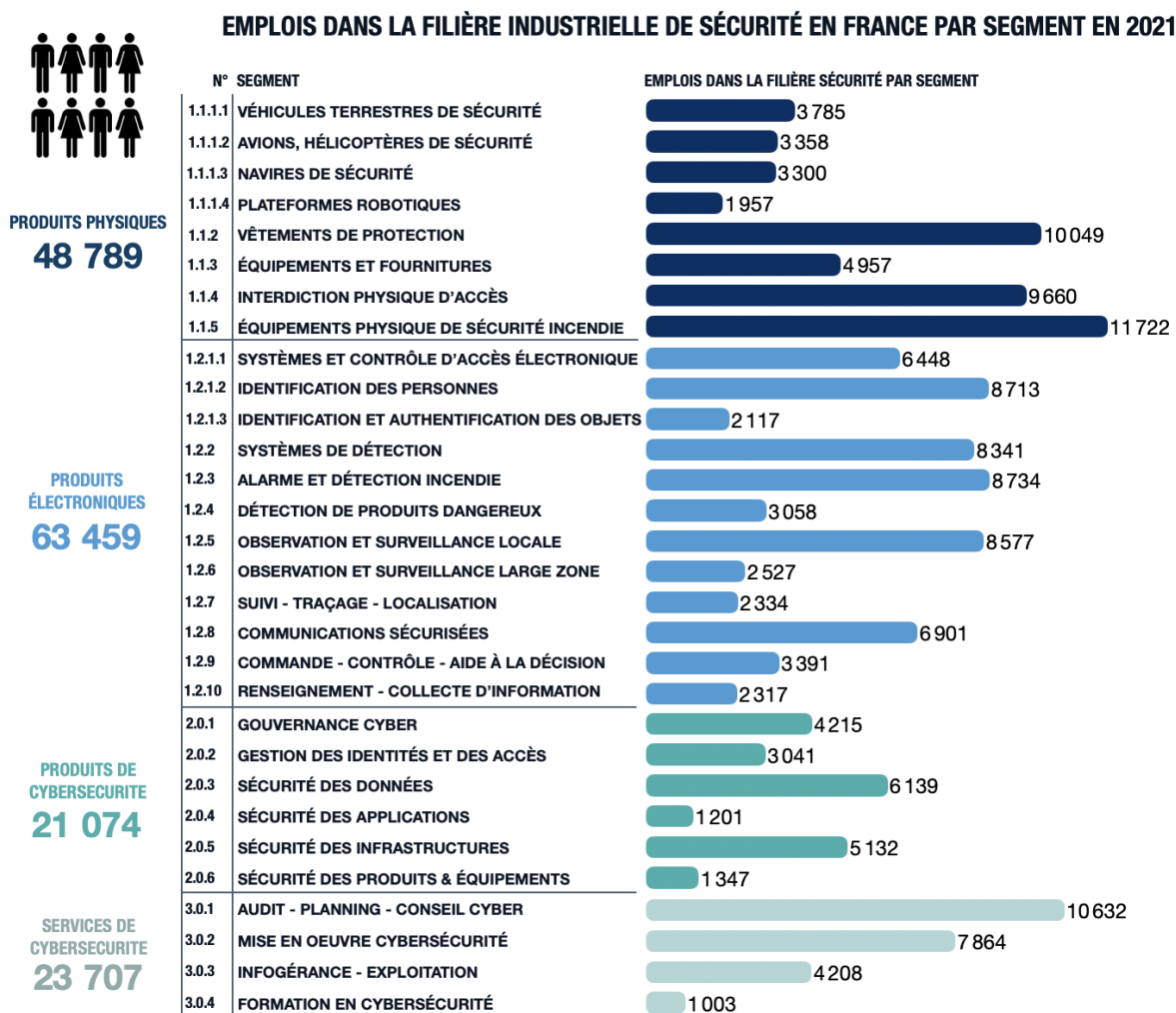
Source : DECISION Etudes & Conseil

*TCAM = TAUX DE CROISSANCE ANNUEL MOYEN

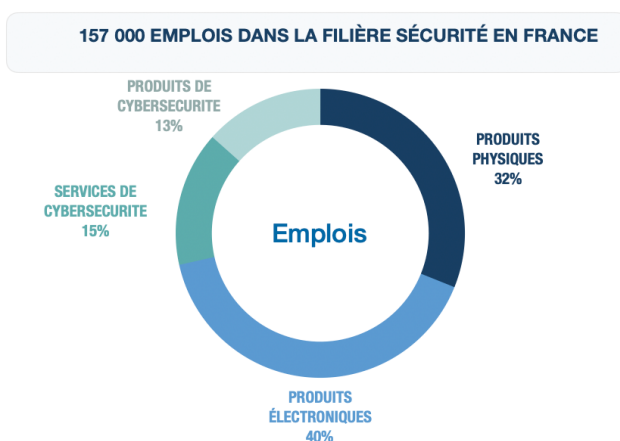


III) Les chiffres clés de la filière

3.2.2 Emplois 2021



Source : DECISION Etudes & Conseil



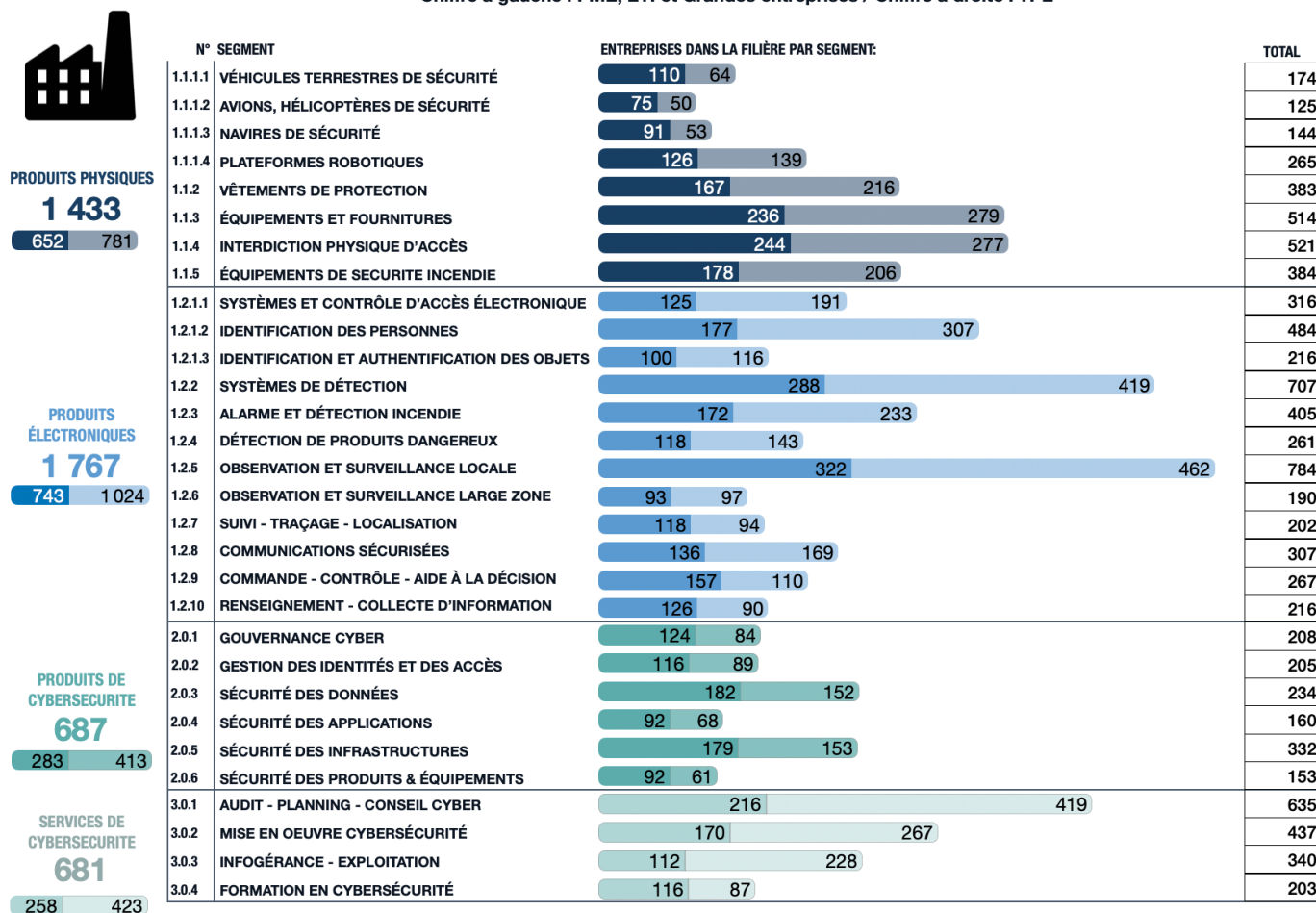


III) Les chiffres clés de la filière

3.2.3 Nombre d'entreprises 2021

NOMBRE D'ENTREPRISES DANS LA FILIÈRE INDUSTRIELLE DE SÉCURITÉ EN FRANCE PAR SEGMENT EN 2021

Chiffre à gauche : PME, ETI et Grandes entreprises / Chiffre à droite : TPE



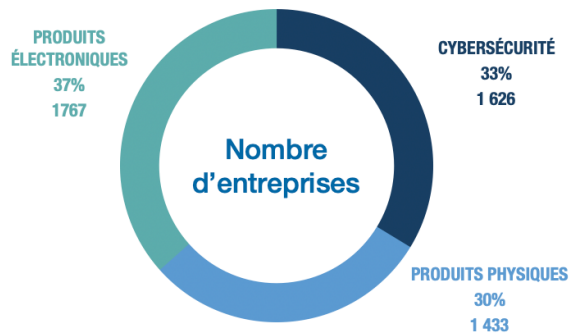
Source : DECISION Etudes & Conseil

4 402 ENTREPRISES DANS LA FILIÈRE EN FRANCE EN 2021

DONT

90 GRANDES ENTREPRISES
91 ENTREPRISES DE TAILLE INTERMÉDIAIRE
1 723 PETITES ET MOYENNES ENTREPRISES
2 498 TRÈS PETITES ENTREPRISES

Source : DECISION Etudes & Conseil



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



III) Les chiffres clés de la filière

3.4 Tendances de marché sur la période 2020-2022

3.4.1 De nombreux mouvements de fusions-acquisitions

Au sein de la filière industrielle de sécurité, 106 rachats d'entreprises concernant des sièges d'entreprises localisés en France ont été recensés sur la période 2020-2022 (soit en moyenne 35 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 :

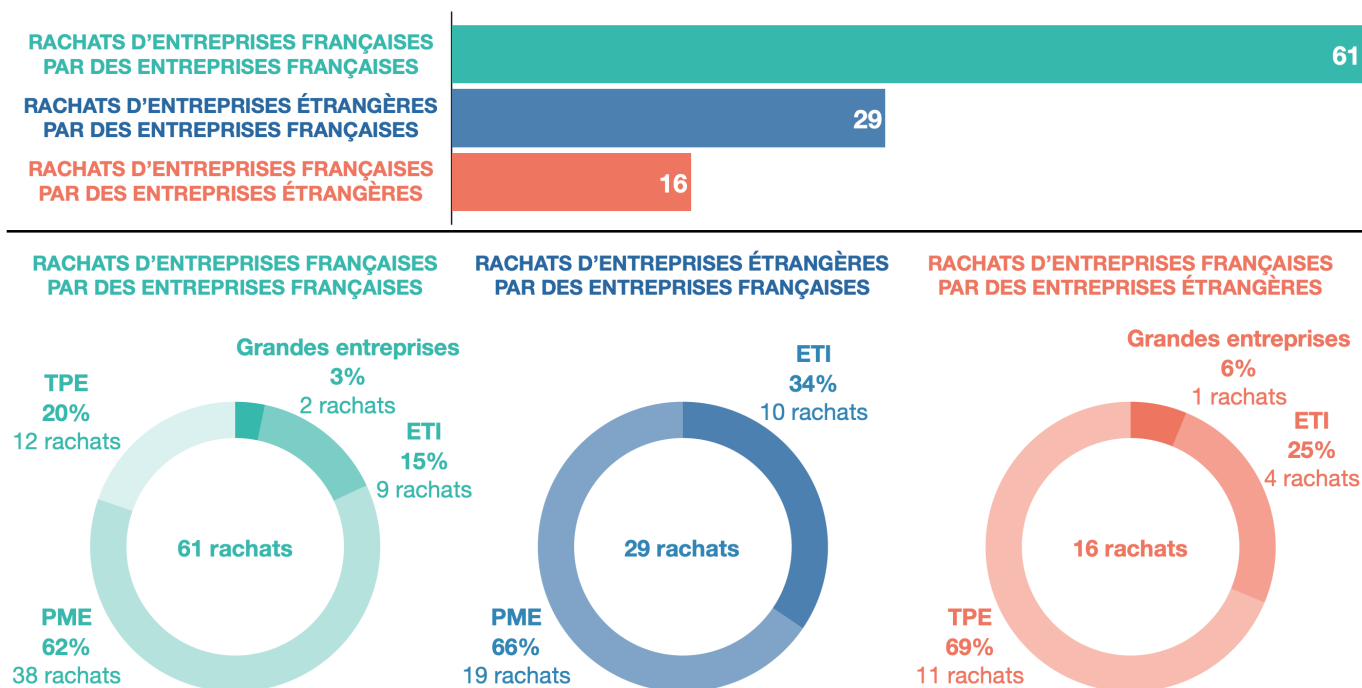
- 61 rachats d'entreprises françaises par d'autres entreprises françaises (58%)
- 29 rachats d'entreprises étrangères par des entreprises françaises (27%)
- 16 rachats d'entreprises françaises par des entreprises étrangères (15%)

La grande majorité des entreprises rachetées sont des PME (63%) et des ETI (21%), en croissance.

Le nombre de rachats d'entreprises étrangères par des capitaux français est supérieur de 81% sur la période au nombre de rachats d'entreprises françaises par des entreprises de capitaux étrangers. Cette situation sur la période 2020-2022 contraste avec celle de 2017-2020 durant laquelle les firmes étrangères rachetaient plus de firmes françaises que l'inverse. En moyenne, la taille des entreprises rachetées sur la période 2020-2022 est cependant plus modeste.

Les rachats les plus significatifs d'entreprises françaises par des entreprises étrangères sur la période 2020-2022 sont ceux d'Akka Technologies par Adecco (Suisse), de Finsecur par Jade Bird Fire (Chine), d'AFD.TECH par Accenture (Etats-Unis) et de Cover Guard par CSW Industries (Etats-Unis).

BILAN : RACHATS D'ENTREPRISES SUR LA PÉRIODE 2020-2022



Source : DECISION Etudes & Conseil



III) Les chiffres clés de la filière

72% des rachats effectués par des capitaux français sur la période 2020-2022 ont concerné des entreprises européennes: Nexus (Suède), BTN Henry van Ommeren (Pays-Bas), SEC Consult (Autriche), BU Digital Security d'Econocom (Belge), etc.

On remarque enfin que le nombre global d'acquisitions par an sur la période est très important historiquement: le nombre moyen de rachats annuels a progressé de +67% par rapport à la période 2017-2020. En moyenne, la taille des entreprises rachetées sur la période 2020-2022 est cependant plus modeste.

Les principaux mouvements d'acquisitions sur la période 2020-2022 sont présentés ci-dessous. Il n'y a pas de fusion sur la période.

Principaux rachats entre entreprises de capitaux français sur la période 2020-2022

Année	Entreprise acheteuse		Entreprise rachetée		
	Nom	Taille de l'entreprise	Nom	Taille de l'entreprise	Activité
2020	Groupe RG	ETI	EPI Center	ETI	Vêtements protecteurs spéciaux pour les agents publics et privés de sécurité (police, pompiers, gardiennage, etc.)
2020	Atos Worldline	GG	Ingenico	GG	Sécurisation des paiements
2020	Sopra Steria	GG	Sodifrance	ETI	Cabinet de conseil en tranformaton 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	Fonds d'investissement Capza (Axa)	Fond financier	Eurofeu	ETI	Équipements de sécurité incendie (portes coupe-feu, désenfumage, échelles, robinetterie, tuyaux, autres.), équipements électroniques de sécurité incendie
2021	HLD	Fond financier	Photonis	ETI	Observation et surveillance (local)
2021	Faye	GG	NXO (Butler Industries)	ETI	Services de cybersécurité
2021	Ardian	Fond financier	Groupe RG (LBO France)	ETI	Vêtements protecteurs spéciaux pour les agents publics et privés de sécurité (police, pompiers, gardiennage, etc.)
2021	Bouygues	GG	Equans	GG	Tous les segments sécurité d'Engie sont concernés par ce rachat : Cofely, Ineo et Axima. Les segments couverts sont la sécurité incendie, l'installation d'alarmes anti-intrusion, de caméras et d'outils de contrôle d'accès
2021	Fonds de consolidation et de développement des entreprises (FCDE)	Fond financier	Bertin Technologies (CNIM Groupe)	ETI	Détection et inspection des produits ou des personnes, observation et surveillance locale, suivi-traçage et localisation.
2021	Sopra Steria	GG	EVA Group	PME (grande)	Services de cybersécurité
2021	Safran / MBDA	GG	CILAS	ETI	Observation et surveillance (local)
2022	Sopra Steria	GG	CS Groupe	ETI	Produits et Solutions de cybersécurité : en particulier gouvernance cyber (systèmes de gestion, SIEM).

Sont reportées ici uniquement les firmes rachetées pendant 2020-2022 de type Grands Groupes (GG), ETI et grandes PME (minimum environ 30 millions de chiffre d'affaire). Elles sont classées par date de rachat.



III) Les chiffres clés de la filière

Principaux rachats d'entreprises de capitaux étrangers par des entreprises de capitaux français sur la période 2020-2022

Année	Entreprise acheteuse		Entreprise rachetée		
	Nom	Taille de l'entreprise	Nom	Taille de l'entreprise	Activité
2020	IN Groupe	ETI	Nexus	ETI	Identification des personnes et des objets. Plateforme PKI, Card Management System, etc.
2020	Descours & Cabaud	GG	BTN-Henny van Ommeren	PME (grande)	Vêtements de protection.
2020	Atos	GG	SEC consult	PME (grande)	Services d'audit, planning, conseil en sécurité informatique
2020	Atos	GG	Digital Security (Econocom)	ETI	Produits et solutions de cybersécurité.
2020	Atos	GG	Paladion	ETI	Produits et solutions de cybersécurité.
2021	Atos	GG	In Fidem	PME (grande)	Services d'audit, planning, conseil en sécurité informatique
2021	Bureau Veritas	GG	Secura BV	PME (grande)	Services d'audit, planning, conseil en sécurité informatique
2021	Coverguard	ETI	Safety-INXS	ETI	Vêtements de protection.
2021	Atos	GG	Motiv ICT Security	PME (grande)	Infogérance et exploitation
2021	Airbus Helicopters	GG	ZF Luftfahrttechnik	ETI	Hélicoptères pour les services de sécurité, etc.
2021	Thales	GG	Moog (activités aides à la navigation uniquement)	ETI	Suivi et traçage, positionnement et localisation
2022	Thales	GG	Advanced acoustic concept	ETI	Équipements et fournitures pour les services de sécurité (note : ne contient pas que du physique mais aussi de l'électronique). Systèmes et dispositifs de suivi, de localisation et de positionnement pour conteneurs, véhicules terrestres, avions, bateaux (comme AIS, LRIT, etc.)
2022	Fiducial	GG	Prosegur	ETI	Services de gardiennage et de surveillance
2022	Vinci Energies	GG	Kontron - la plupart des activités services IT	ETI	Services de cybersécurité.
2022	Thales	GG	S21sec	ETI	Audit, test de vulnérabilité et d'intrusion, évaluation de risque en sécurité, analyse et gestion des risques et menaces
2022	CS Group	ETI	HE Space	ETI	Observation et surveillance (large zone)

Sont reportées ici uniquement les firmes rachetées pendant 2020-2022 de type Grands Groupes, ETI et grandes PME (minimum environ 30 millions de chiffre d'affaire). Elles sont classées par date de rachat.



III) Les chiffres clés de la filière

Principaux rachats d'entreprises de capitaux français par des entreprises de capitaux étrangers sur la période 2020-2022

Année	Entreprise acheteuse		Entreprise rachetée		
	Nom	Taille de l'entreprise	Nom	Taille de l'entreprise	Activité
2020	Jade Bird Fire	ETI	Finsecur	ETI	Équipements de sécurité incendie (portes coupe-feu, désenfumage, échelles, robinetterie, tuyaux, autres). Équipements électroniques de sécurité incendie.
2020	FAAC	GG	Groupe français Agta Record (Assa Abloy)	ETI	Interdiction physique d'accès et contrôle d'accès, notamment portes de sécurité automatiques.
2021	Accenture	GG	AFD.TECH	ETI	Cloud computing, y compris certaines compétences autour de la sécurisation du cloud.
2022	Adecco	GG	Akka Technologies	GG	Akka technologies est l'un des leaders français du conseil en ingénierie. A ce titre, il intervient auprès de nombreux leaders de la filière de sécurité, pour des prestations de support en ingénierie, notamment en matière d'électronique mais aussi de services d'audit, planning, conseil en sécurité informatique.
2022	CSW Industries	GG	Cover Guard	ETI	Vêtements de protection

Sont reportées ici uniquement les firmes rachetées pendant 2020-2022 de type Grands Groupes, ETI et grandes PME (minimum environ 30 millions de chiffre d'affaire). Elles sont classées par date de rachat.

Autres mouvements intéressants pour la filière française

Sur le segment de la sécurité incendie, le rachat de Chubb Fire & Security par l'américain API Group début 2022 pour 3,1 milliards de dollars n'a pas encore été mentionné. Et pour cause, ni Chubb, ni API group ne sont des groupes français. Mais ces deux sociétés ont toutes les deux une activité importante en France. Chubb appartenait jusqu'alors à l'américain Carrier. Suite à ce rachat, API Group devient l'un des trois leaders français de la sécurité incendie avec les français Descours & Cabaud et Desautel. Carrier est rétrogradé à la 37ème place de la filière en France avec un CA de seulement 130M€ en 2021.



III) Les chiffres clés de la filière

3.4.2 Les levées de fond des start-ups

DECISION estime que respectivement en 2020, 2021 et 2022, les startups françaises de la cybersécurité ont levé respectivement 165M€, 546M€ et 59M€ auprès des investisseurs français. Le tableau ci-dessous regroupe les levées de fonds identifiées entre 2020 et 2022.

Année	Startup	Montant levé	Fonds impliqués	Activité de l'entreprise
2021	Ledger	321	Tekne Capital, Uphold Ventures, Felix Capital, Inherent, etc.	Sécurité crypto-actifs
2021	GuitGuardian	39	Eurazeo, Sapphire, Balderton Capital, Fly Ventures	Détection des risques cyber
2020	CybelAngel	36	PrimeVenture, Large Ventures - BPI France, TempoCap, etc.	Détection des risques cyber
2021	Datadome	30	Elephant, ISAI	Protection contre bots
2021	Yousign	30	Lead Edge Capital	Signature électronique
2021	Didomi	29	Elephant, Breega	Gestion consentements clients
2022	Gatewatcher	25	Move Capital Fund I,	Cybersécurité
2020	Odaseva	21	Eight Roads Ventures, F-Prime Capital, Partech, Serena, etc.	Gestion des données
2022	Secure-IC	20	Alliance entreprendre, GO capital, BNP Paribas Développement	Sécurité des données

3.4.3 Les principales entreprises en faillite

Année	Taille de l'entreprise	Entreprise	Activité
2020	ETI	SAB / SAB INGENIERIE INFORMATIQUE	Services de cybersécurité
2020	ETI	SOC PROMAT	Équipements physiques et électroniques de sécurité incendie
2021	PME	NOKIA BELL LABS FRANCE	Sécurité des communications et des équipements
2021	PME	EOLANE VAILHAUQUES	L'un des principaux EMS français : sous-traitant de fabrication d'équipements électroniques. Eolane fabrique des équipements pour de nombreux acteurs de la filière. Ce groupe est en difficulté depuis plusieurs années et son siège social de Vailhauques a fermé en 2021
2021	PME	MUZELLE DULAC HASSON	Vêtements de protection
2021	PME	CLOTURES PLACE	Interdiction physique d'accès, clôtures et enceintes
2020	PME	TRAQUEUR	Suivi et traçage, positionnement et localisation
2022	PME	COLT FRANCE	Équipements physiques et électroniques de sécurité incendie
2022	PME	E BIZNEXT	Services de cybersécurité

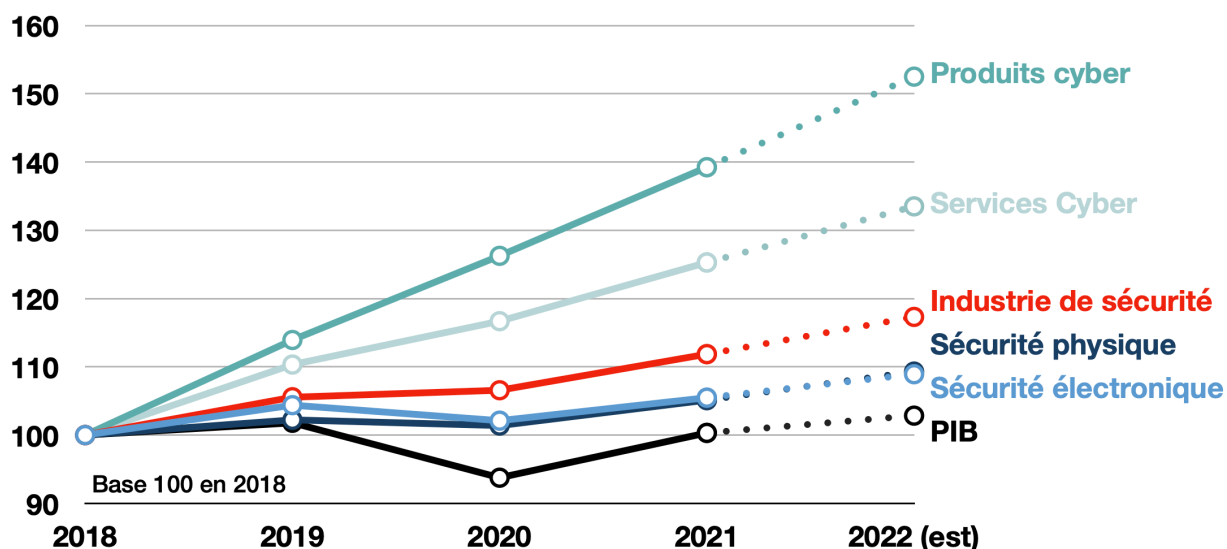
Sont reportées ici les firmes ayant fait faillite en 2020-2022 classées par année de fermeture, puis par chiffre d'affaire avant de fermer.



IV) Les tendances

4.1 Une filière résiliente face à la COVID

CROISSANCE FRANCE COMPARÉE 2018-2022



Segments	Croissance			
	2019	2020	2021	2022 (est)
Industrie de sécurité	5,5 %	1,0 %	5,0 %	4,9 %
Physique	2,2 %	-0,8 %	3,7 %	4,0 %
Electronique	4,4 %	-2,2 %	3,3 %	3,3 %
Produits cyber	13,9 %	10,8 %	10,3 %	9,5 %
Services cyber	10,3 %	5,8 %	7,4 %	6,6 %
PIB*	1,8 %	-7,9 %	7,0 %	2,5 %

Source : DECISION Etudes & Conseil

4.1.1 2020: La filière face à la crise

La filière a subi fortement l'impact de la crise sanitaire mondiale du COVID, avec des Taux d'Activité (TA¹) descendus à 50% et des Taux d'Emploi (TE) descendus à 65% en moyenne en avril 2020 (soit au cœur du premier confinement). Les segments physique et électronique, plus dépendants de l'export, ont été encore plus fortement touchés (TA de 30% et TE de 50%).

Deux tiers des entreprises de la filière jugent l'impact de la crise du COVID sur leur chiffre d'affaires de l'année 2020 comme fortement négatif (dont un tiers très négatif), selon une enquête réalisée par le GICAT². Selon cette même enquête, près de 50% des contrats étaient suspendus fin 2020 dont près de 20% définitivement annulés. Enfin, 80% des acteurs ont indiqué subir une baisse de leurs exportations en 2020. Cette baisse était supérieure à 50% pour 20% des acteurs.

Malgré ces difficultés au début de l'année 2020, **l'industrie de sécurité est la seule filière industrielle française qui n'a pas subi de récession cette année (1%)**, tandis que le PIB français chutait de -8% et que l'industrie française dans son ensemble subissait une récession de -12%.

¹ Correspondant à la production / chiffre d'affaires

² Enquête réalisée de décembre 2020 à janvier 2021 auprès de 123 entreprises de la filière.



IV) Les tendances

Cette bonne performance en 2020 a deux causes principales :

- L'augmentation toujours plus importante de la demande de produits et services de cybersécurité, qui n'a été que très peu impactée par les différentes restrictions mises en place. La cybersécurité a ainsi maintenu une croissance de 8,3% en 2020 contre 12,1% en 2019.
- Plus de la moitié du marché de la sécurité est constitué de segments répondant à des besoins vitaux qui ont continué à fonctionner sur l'ensemble de l'année : secteur public au sens large (y compris santé et transports), énergie et banque / finance / assurance.

La sécurité électronique a été le segment le plus fortement affecté par la crise avec une récession de -2,2% en 2020 pour trois raisons :

1. D'une part, ce segment comprend des produits électroniques fabriqués dans des usines qui ont subi des fermetures en début d'année 2020.
2. D'autre part, les segments de la sécurité électronique sont ceux qui ont été les plus fortement affectés par les mesures gouvernementales associées aux transports et aux voyages, en particulier aériens (contrôle d'accès, détection de produits ou de personnes, passeports, etc.).
3. Enfin, le segment électronique est le plus exposé aux marchés « grand public », particulièrement affectés par la crise.

Cette crise du COVID a démontré le caractère essentiel de la filière 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 retour à la mise en œuvre d'une politique industrielle planifiée visant à garantir la souveraineté et la résilience de l'industrie française. 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.

4.1.2 Depuis 2021, la filière renoue avec une forte croissance portée par des tendances structurelles solides et durables

En 2021 et 2022, la filière renoue avec une croissance forte de 5,0% portée par des tendances structurelles qui ont émergé il y a plus de dix ans et vont en s'accroissant d'année en année*.

- **Accélération de la croissance « digitale »** portée par la crise sanitaire et les besoins accrus de connectivité. Le télétravail a notamment accru l'attention des entreprises autour des problématiques de cybersécurité (plateformes sécurisées de télétravail, etc.), de même que l'importance des paiements numériques devant être sécurisés.
- **Accélération du déploiement de clouds** d'entreprises mais aussi de clouds applicatifs (Continuum Cloud-to-Edge), soutenant la demande d'un ensemble d'offres de confiance numérique autour des clouds de confiance, de la sécurité du cloud et de la sécurité at-the-edge. Ces tendances bénéficient particulièrement à des offres de produits cyber : gestion des identités et des accès (IAM), sécurité des données, sécurité des infrastructures et sécurité des produits et équipements (éléments sécurisés...).
- **Augmentation continue des cyberattaques** (particulièrement les ransomware depuis plusieurs années). En outre, 75% des victimes de ransomware sont désormais des petites et moyennes entreprises qui manquent de ressources dédiées (Orange Cyber Security Report 2022). Le marché de protection des PME et TPE françaises est à ce titre très prometteur.



IV) Les tendances

4.1.3 6 nouvelles opportunités de croissance pour les années à venir

Six tendances nouvelles génèrent des perspectives de croissance dans des segments qui étaient peu porteurs depuis une dizaine d'années, en particulier en matière de sécurité physique :

1. **Accélération de la croissance des segments ayant des applications sanitaires.** La crise du COVID a généré une croissance exponentielle des segments de la filière sécurité ayant des applications en santé : EPI (masques de protection), Détection de produits dangereux (tenues de protection NRBC, outils d'analyse de la qualité de l'air).
2. **Augmentation de la commande publique dans les véhicules et plateformes.** La période 2018-2021 a été particulièrement favorable à l'ensemble des fabricants de véhicules et plateformes de sécurité du fait de nouveaux contrats publics de renouvellement ou d'extension de flottes dans tous les sous-segments (à l'exception des avions de sécurité). Des commandes publiques importantes sont également prévues à horizon 2030 sur l'ensemble des segments et les perspectives à l'exportation sont favorables pour les leaders de ce secteur (Airbus, Dassault et Naval Group).

L'unique exception est le segment des véhicules terrestres de sécurité. Si ce segment a bénéficié sur la période 2017-2021 des efforts dédiés au renouvellement des parcs de la Police nationale mais surtout de la Gendarmerie Nationale (dont 50 % du parc aura été renouvelé en 5 ans), cette tendance devrait ne pas se poursuivre à partir de 2021-2022, à moins que n'apparaissent de nouvelles perspectives dans le cadre de la LOPMI ou bien à l'export, comme la commande ukrainienne de 370 camions échelles pour 300 M€ auprès de Desautel en 2021.

3. **Augmentation de la demande sécuritaire des états européens en lien notamment avec la guerre en Ukraine.** On observe une demande en forte croissance de la part de nombreux états (Suède, Finlande qui abandonne sa posture de neutralité entraînant une réflexion stratégique...). Principalement axés sur la Défense, les efforts budgétaires de ces états se portent également sur plusieurs segments de la filière de sécurité : moyens de lutte antiterroriste, contrôle aux frontières, etc. Cette conjoncture se combine au déploiement de nombreux projets européens d'envergure ayant trait à la sécurité : IRIS 2 (communications satellites sécurisées), EuroQCI / OpenQKD (communications quantiques sécurisées), etc. Ce tableau peut être nuancé par la tendance de nombreux états européens à réserver leurs achats pour l'industrie américaine (Allemagne, Pologne...) et/ou israélienne.
4. **Le changement climatique entraîne un besoin accru en matière de sécurité civile.** Les crises engendrées par le réchauffement climatique, à l'image des incendies qui ont ravagé près de 800 000 hectares en Europe en 2022 (un record historique), génèrent un besoin accru de moyens en matière de sécurité civile à l'échelle mondiale.
5. **Importance croissante de l'enjeu du contrôle aux frontières.** L'accumulation des crises aux frontières de l'Europe depuis plusieurs années (Libye, Mali, Syrie, Ukraine...) fait du contrôle aux frontières un enjeu d'une importance croissante pour les états européens : lutte contre l'immigration clandestine et les passeurs, les stupéfiants, la prolifération d'armes.

Les projets d'envergure se multiplient : la France bénéficie de nouveaux crédits de la part du Royaume-Uni pour sécuriser la frontière sur l'ensemble de la Manche (72,2M€ pour la période 2022-2023), le Royaume-Uni renégocie le contrôle de sa frontière avec l'Irlande, la coopération Franco-Belge est appelée à s'intensifier, de grands ports européens fournissent des efforts pour améliorer leur sécurité (Anvers...), etc. En la matière, les atouts de la filière française sont nombreux : Ballons captifs, drones, écoutes radars / sonars, etc.

6. Enfin, **la sécurisation des grands événements à venir en France** : Coupe du monde de Rugby et Jeux Olympiques. Le prochain paragraphe (4.2) est dédié à ce sujet.

Ces nouvelles tendances particulièrement bénéfiques au segment des produits physiques expliquent que la croissance de ce segment dépasse celle des produits électroniques en 2021, un phénomène qui devrait se poursuivre à minima en 2022.

La sécurité demeure cependant une industrie fortement concurrentielle et la présence d'acteurs étrangers sur le marché français se fait de plus en plus ressentir, en particulier en provenance de la Chine et des Etats-Unis.

Sur la période 2018-2021, DECISION observe en particulier la continuation de la forte progression des acteurs américains, souvent issus du monde digital (cloud, produits et services informatiques) qui se développent en France à travers des sièges sociaux dédiés : Microsoft, Dell, Palantir, Docusign, AWS, Google, Splunk, Check Point Systems, McAfee, CrowdStrike International, Juniper Networks, Nutanix, F5 Networks, Palo Alto Networks, Rubrik, Okta, Netskope, Forescout technologies, Aruba, Imperva, Tufin Software, Quest software, Proofpoint...

Enfin, la crise énergétique qui débute en 2022 aura probablement des répercussions négatives sur la croissance de l'industrie de sécurité sur la période 2023-2030, en particulier pour les segments les plus dépendants sur le plan énergétique (produits électroniques et en second lieu produits physiques).

*La quinzaine d'acteurs de la filière consultés au premier semestre 2022 indiquent une poursuite des tendances de l'année 2021



IV) Les tendances

4.2 Les enjeux des grands événements

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

Ces grands événements constituent des cibles de choix pour les actes malveillants et criminels et mais également pour des actes terroristes ou des cyberattaques ce qui engendre une menace forte et très évolutive.

L'excellence de la filière française dans ce domaine s'est par exemple illustrée dans le cadre de l'organisation de la Coupe du Monde au Qatar avec l'envoi de 600 gendarmes pour former la police qatarie ainsi que la sécurisation du métro et de l'aéroport de Doha.

En 2023 et 2024, la France va accueillir sur son sol deux grands événements : La coupe du monde de rugby puis les Jeux Olympiques.

L'opportunité des Jeux Olympiques de Paris 2024

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

Assurer la sécurité des JO de Paris 2024 est donc un enjeu essentiel avec trois objectifs majeurs : empêcher les attaques et les incidents, détecter les troubles fêtes, et réduire les perturbations au minimum pour les résidents. Mais cette mission combine de nombreuses contraintes : durée de la période à couvrir, sites très nombreux (également au-delà des sites olympiques : fan zones, transports, etc.), public et flux très importants, transparence pour laisser la place à la fête, etc.

Depuis plusieurs années déjà, la filière de sécurité mène une réflexion dans le but de déployer une offre française cohérente et structurée pour la sécurisation des Jeux Olympiques de 2024 à Paris, et plus largement déclinable à tous types de grands événements - notamment dans le cadre du CSF (Comité Stratégique de Filière) des Industries de Sécurité.

Le CSF a lancé 180 expérimentations visant à tester et valider en amont les solutions technologiques fournies par la filière de sécurité. La grande majorité de ces expérimentations portent sur des solutions émanant de sociétés françaises et proposées par des startups, PME ou Entreprises de Taille Intermédiaires (ETI). Les principaux domaines d'application de ces expérimentations sont :

- Commandement et hypervision
- Vidéoprotection / agrégation
- Cybersécurité
- Bulle 3D
- Sécurité nautique
- Gestion des foules
- NRBCE

Les JO sont aussi l'occasion d'approfondir les collaborations de la filière sécurité avec certaines collectivités locales (Paris, Marseille, Région IDF, etc.) ainsi que certains OIV/OSE en particulier dans le domaine des transports. Les synergies sont ainsi nombreuses avec le projet « Territoires de Confiance » du CSF sécurité.

La filière de la confiance numérique dispose de fortes compétences, d'une excellence reconnue et de solutions innovantes pour apporter, aujourd'hui et à l'avenir, une réponse évolutive et de très haut niveau aux besoins de sécurité et de confiance numérique des grands événements.

Les JO de Paris 2024 représentent donc une opportunité exceptionnelle pour les entreprises françaises de démontrer leur capacité à répondre à un tel défi et de se positionner sur des marchés durables tant sur le plan national qu'à l'export pour les années à venir.



IV) Les tendances

4.3 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.

4.3.1 Les innovations électroniques et numériques qui génèrent de nouveaux marchés

Les innovations issues des industries électronique et numérique impactent presque tous les secteurs des économies 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. 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 sept entreprises se maintiennent au niveau mondial : Samsung (Corée du Sud), TSMC (Taïwan) et Intel (États-Unis) dans les processeurs ; Samsung et SK Hynix (Corée du Sud), Micron et Western Digital (États-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.
- **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, en particulier à travers le déploiement du continuum Cloud-to-Edge et ses débouchés en matière d'IoT industriels.

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.)... Jusqu'à présent, la croissance issue des objets connectés a été encore faiblement ressentie par les acteurs de la filière française de sécurité, bien que nombre d'entre eux aient déjà travaillé à une offre dédiée. Les progrès dans la standardisation et l'interopérabilité des architectures IoT sont à même d'accélérer la croissance future.
 - **Automobile connectée.** Parmi les différents types d'objets connectés, la sécurisation des automobiles et de leurs communications a été le principal moteur de croissance sur les cinq dernières années : 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 bâtiments et dans les villes à des fins de sécurité a été le deuxième segment IoT le plus porteurs sur les cinq dernières années. Les acteurs qui ont le plus bénéficié de la thématique Safe City sont les grands intégrateurs (Thales, Accenture, Capgemini, etc.). La Safe City est globalement moins porteuse en France qu'à l'étranger (que ce soit en Chine, aux États-Unis ou dans de nombreux pays émergents) pour trois raisons principales : l'administration française qui s'est construite autour de processus non digitaux, la grande diversité des acteurs publics en France (état central, régions, départements, communes, communauté de communes, etc.), et l'austérité budgétaire.



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 États-Unis ou des BATX en Chine).

2. **Souveraineté de la donnée.** En parallèle du foisonnement technologique en matière d'électronique autour du stockage et du traitement des données (mémoires non-volatiles émergentes, puces neuromorphiques, calcul quantique, calcul photonique, photonique intégrée, réseaux d'interconnexion photonique, calcul de haute performance (HPC), etc.), le nombre et le volume des bases de données croît de manière exponentielle (big data). La problématique de sécurisation de ces jeux de données prend de plus en plus d'importance, que ce soit pour des raisons régaliennes (services publics, bases de données critiques), économiques (protection des données sensibles des entreprises), ou citoyennes (droits du citoyen, protection des données personnelles, droit à l'oubli...).
3. **Identités numériques.** Fortement corrélée à la thématique de souveraineté de la donnée, la nécessité de la re-définition des identités numériques provient également du développement des outils électroniques et de la transformation digitale (« citoyenneté à distance »). La norme actuelle en France demeure l'existence simultanée de nombreuses identités décorrélées, fortes (SIM, cartes bancaires, passeports, etc.), substantielles (identité numérique de La Poste), et faibles (identités numériques délivrées très majoritairement par les acteurs du numérique américains du type GAFA pour le e-commerce), sans garantie de protection souveraine des données. L'alternative est le déploiement d'une identité forte unique et souveraine pour des applications régaliennes et associée à l'utilisateur qui gère ensuite comme il le souhaite ses autres identités qu'il dérive de la première. La filière industrielle française dispose de tous les acteurs et de toutes les compétences nécessaires à cette alternative (éléments sécurisés, Identity & Access Management (IAM), intégration des solutions, cryptographie, biométrie, PVID, etc.). Le projet prend forme au niveau français autour du déploiement de la Carte Nationale d'Identité Electronique (CNIE), et au niveau européen autour du projet de portefeuille (wallet) d'identités numériques (eIDAS2).

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

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



IV) Les tendances

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

- **Cryptographie légère (Lightweight cryptography).** Le développement rapide de l'IoT a un impact énorme sur tous les aspects liés à la cybersécurité. De récentes attaques massives contre des configurations IoT ont montré que de solides techniques cryptographiques doivent être utilisées pour assurer une sécurité globale du système. Malheureusement, dans le cas de l'IoT, où le coût est un paramètre important, l'utilisation de la cryptographie peut être limitée par la taille, la puissance et les performances informatiques locales des objets. Cela a donné naissance à un domaine de recherche très actif autour de la cryptographie dite légère. En bref, la cryptographie légère recherche de nouveaux algorithmes ou protocoles cryptographiques adaptés à la mise en œuvre dans des environnements restreints, y compris les étiquettes RFID, les capteurs, les appareils de santé et de soins. La cryptographie légère devrait être progressivement utilisée dans tous les domaines IoT où le concept SWAP (taille, poids et puissance) tend à devenir critique. Les premières applications industrielles sont en train d'être développées et mises en place.
- **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 contre les attaques. Cependant, l'ordinateur quantique et sa puissance de calcul potentielle constitue une menace pour les données chiffrées avec ces méthodes qu'il pourrait décrypter en un temps record. Pour répondre à cette menace, la cryptographie post-quantique se base sur de nouveaux concepts mathématiques afin de chiffrer les messages et donc sécuriser le transport de l'information. La France se maintient dans le top trois mondial dans ce domaine et joue notamment un rôle clef dans l'élaboration de l'infrastructure européenne de communication quantique (EuroQCI).
- **Chiffrement homomorphique.** L'énorme développement du cloud computing a généré un champ de recherche très actif autour du chiffrement dit fonctionnel et du chiffrement homomorphique : le chiffrement fonctionnel est un nouveau paradigme pour le chiffrement à clé publique qui permet à la fois un contrôle d'accès à granularité fine et un calcul sélectif sur les données chiffrées. Dans sa version la plus complète, le chiffrement entièrement homomorphe (FHE) permet le calcul sur des données chiffrées sans divulguer aucune information sur les données sous-jacentes. En bref, une partie peut chiffrer certaines données d'entrée, tandis qu'une autre partie, qui n'a pas accès à la clé de déchiffrement, peut effectuer aveuglément des calculs sur cette entrée chiffrée. Le résultat final est également chiffré, et il ne peut être récupéré que par la partie qui possède la clé secrète. Ce champ est très prometteur et les premières applications industrielles émergent.
- **Cryptographie utilisant l'ADN.** Il s'agit d'une nouvelle branche de la cryptographie. Elle utilise l'ADN comme vecteur d'information et de calcul à l'aide de techniques moléculaires. Il s'agit d'un domaine relativement nouveau qui a émergé suite aux découvertes sur la grande capacité de stockage de l'ADN -qui est l'outil de calcul de base de ce domaine. Un gramme d'ADN stocke environ 108 To de données, ce qui dépasse la capacité de stockage de tout support de stockage électrique, optique ou magnétique. Les premières applications industrielles devraient émerger d'ici à 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 d'ici à 2030.



IV) Les tendances

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

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

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

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



IV) Les tendances

4. **Plateformes robotiques (dont drones).** Bien que sa croissance soit moins soutenue, le segment des plateformes robotiques a cru en moyenne de près de 6% sur la période 2018-2021, 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), entraînant d'ailleurs une guerre des prix et des faillites nombreuses -en particulier pour un segment bénéficiant d'une telle croissance.
5. **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 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.
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 du design de composants électroniques (Open Hardware). Les logiciels et les matériels en mode Open Source accélèrent l'innovation en permettant aux développeurs et aux concepteurs de partager et de réutiliser les développements réalisés par d'autres. La republication 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 la France dans 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. **Blockchain.** D'abord associée aux cryptomonnaies et au Bitcoin en particulier, la blockchain s'impose comme un nouvel outil au centre de nombreuses applications de 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 confiance numérique sont multiples : gestion des prestations sociales, protection des infrastructures des opérateurs d'importance vitale, mais aussi missions de sécurité civile ou intérieure et gestion du secret entre institutions.

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

8. D'autres développements technologiques existent, mais qui n'ont pas la même intensité d'impact sur la filière de sécurité mondiale. Les développements autour de l'identité numérique forment un exemple illustratif : **captcha et challenges pour logiciels, QR codes, reconnaissance d'iris, de la forme des veines, mot de passe dynamique...**



IV) Les tendances

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

4.4.1 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 chaîne de valeur en développant des compétences dans le logiciel. Ces derniers – à l'image de Thales, Idemia ou encore Naval Group – se positionnent de plus en plus fortement sur le développement de logiciels dédiés à des applications de sécurité.

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

Cette tendance touche même les services privés de sécurité. Alors que la sécurité physique des locaux n'était jusqu'à récemment composée que de moyens humains, son contenu technologique et électronique s'accroît continuellement (SOC, caméras de vidéosurveillance, etc.). Dans la surveillance humaine, la rentabilité nette est très faible (1-2% et dopée artificiellement par le CICE). Dans la sécurité électronique, elle est plus élevée, bien qu'avec des niveaux variables selon les entreprises. La volonté d'un grand nombre d'acteurs privés des services est donc de diversifier leurs services en y intégrant des produits électroniques et cyber et en montant en gamme. A titre illustratif, Prosegur, l'un des leaders européens du gardiennage, a récemment créé un fond d'investissement doté de 30 M€ pour investir dans la sécurité électronique et cyber. Depuis 2016, 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. Securitas, autre leader européen de la sécurité privée, a racheté l'activité sécurité électronique de l'américain Stanley Security en Janvier 2022 et se développe sur ce segment.

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

4.4.2 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.

4.4.3 ...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

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

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

4.5 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 événements 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 maîtrise 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.



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 presque tous les secteurs • Des structures fédératrices : CSF Industries de Sécurité, GICAT, 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. 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, biométrie - Imagerie, radars - Cryptographie, technologies post-quantiques - Intelligence artificielle (en particulier inférence) - Sécurisation des IoT - 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'Hexatruster 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 qui demeure faible dans de nombreux segments et qui manque de structuration • 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 développeurs spécialisés dans un domaine spécifique de la cybersécurité (PKI, cryptographie, etc.) demeure très difficiles à trouver en première embauche. Les entreprises sont contraintes le plus souvent d'embaucher des développeurs formés à la cybersécurité dans son ensemble, voir des ingénieurs généralistes qui seront formés en interne. Attitudes • Chasse en meute encore trop 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	Menaces
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. Le schéma de standardisation-certification-prescription est en place dans la plupart des segments de la filière (sécurité incendie, cybersécurité avec l'ANSSI et l'ENISA). Cependant, le volet commande publique manque dans la plupart des segments. A cet égard, la création d'un équivalent de la DGA et de la BITD en matière de sécurité permettrait de structurer une commande publique forte et d'assurer un suivi la base industrielle française permettant de répondre à la demande • Croissance du marché associé au besoin de sécurisation informatique des PME/TPE dont la majorité ne dispose par exemple d'aucune solution de sauvegarde de leurs données en cas d'attaque • Mise en oeuvre des réglementations en matière de protection des données • Certification sécuritaire des objets IoT (EU Cyber Resilience Act) • Structuration croissante de l'offre dédiée « sécurité » des entreprises et des équipes dédiées « sécurité » chez les clients Attitudes • La crise du COVID et en particulier les pénuries de matériels médicaux et de semi-conducteurs ont généré une prise de conscience, y compris dans l'administration, de la nécessité de préserver une souveraineté industrielle française. Les entreprises de la filière ne constatent cependant pour le moment pas d'évolution notable dans les pratiques Nouvelles technologies / offres en croissance • Développements cryptographiques: cryptographie légère, cryptographie quantique et post-quantique, chiffrement homomorphe, 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 d'open hardware/software pour l'edge computing et les IoTs • Analyse en temps réel des données d'observation locale et large zone Nouveaux marchés / marchés en croissance • Sécurisation des objets connectés: automobile, safe city... • Thématique de la souveraineté des données • Vêtements de protection sanitaire • La plupart des marchés de la cybersécurité...	Structures • Hausse des coûts énergétiques • Développement de standards américains ou autres sur les nouveaux marchés Compétences • Fuite des talents, en particulier en matière de deep learning. Les entreprises françaises 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, des politiques publiques volontaristes et des pratiques commerciales agressives consistant à casser les prix pour générer des situations de quasi-monopole afin dans un second temps de se garantir des marges particulièrement importantes • Avec une intensité bien moindre, concurrence en provenance, d'Israël, du Japon, de Suède, d'Allemagne, de Grande Bretagne, de Corée du Sud et du Canada • Entreprises US puissantes, tout particulièrement dans la partie Cybersécurité ou les généralistes de l'IT continuent à se renforcer : - 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 d'entreprises françaises par des capitaux étrangers, le plus souvent américains • 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- venant concurrencer les entreprises françaises y compris sur le haut de gamme. 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



A propos du CSF Sécurité

Le Conseil Stratégique de Filière (CSF) des Industries de sécurité, créée en 2019, coordonne l'ensemble de la filière industrielle française. La filière regroupe les fédérations et groupements actifs dans le domaine de la sécurité : le GICAT, l'AN2V, le GICAN, la FIEEC, l'ACN et HEXATRUST.

Ces groupements d'entreprises représentent plus de 1000 entreprises actives en sécurité. Ces entreprises réalisent plus de 25 milliards d'euros de CA en France soit plus de 80% du CA de la filière et plus de 100 000 emplois de haute technologie.



Pouvoirs publics



MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER



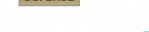
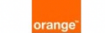
Membres



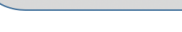
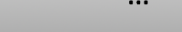
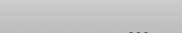
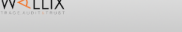
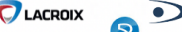
Associations représentées et principaux partenaires



Grands groupes représentés



Plus de 500 ETI et PME représentées, par exemple :



GICAT :

Groupement des industries de défense et de sécurité terrestres et aéroterrestres

AN2V :

Association nationale de vidéoprotection

GICAN :

Groupement des industries de constructions et activités navales

FIEEC :

Fédération des industries électriques, électroniques et de communication

ACN :

Alliance pour la confiance numérique

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 futur.

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 2020 et en 2022. Depuis 2017, DECISION conduit également chaque année l'Observatoire français de l'Alliance pour la Confiance Numérique (ACN).

Pour plus d'informations :

www.decision.eu



DECISION
ETUDES & CONSEIL

Etude commanditée par le **GICAT**, l'**ACN**, le **Ministère de l'Intérieur**,
le **SGDSN** et la **DGE**

en appui aux travaux du Conseil Stratégique de la Filière des Industries de Sécurité.



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