2024

Alliance pour la Confiance Numérique

confiance-numerique.fr

Observatoire de la Filière de la Confiance Numérique

ACN

Alliance pour la confiance numérique

SOMMAIRE

LE MOT DE L'ACN - ALLIANCE POUR LA CONFIANCE NUMÉRIQUE 4

LE MOT DE LA MINISTRE 6

ÉLÉMENTS CLEFS 8

I. CONFIANCE NUMÉRIQUE : CYBERSÉCURITÉ ET SÉCURITÉ NUMÉRIQUE 16
1.1 Cybersécurité et Sécurité Numérique : deux domaines complémentaires 16
1.2 Le Périmètre de la Confiance Numérique - Segmentation 17
1.3 Méthodologie 18

II. CONFIANCE NUMÉRIQUE : UNE FILIÈRE IMPORTANTE ET DYNAMIQUE 20
2.1 La Confiance Numérique est l'une des industries françaises qui bénéficient de la croissance la plus forte sur la période 2016-2022 20
2.2 La Confiance Numérique est une filière industrielle française à part entière 21
2.3 La Confiance Numérique est la filière industrielle dont l'activité est la plus créatrice de richesse en France 22
2.4 Les acteurs français sont au meilleur niveau en matière de compétences et de R&D 24
2.5 La croissance de la Confiance Numérique s'inscrit dans une dynamique mondiale 24
2.6 Une concurrence croissante de la part des acteurs étrangers 25
2.7 Conclusion - Une filière à très fort potentiel si les bons choix stratégiques sont réalisés 26

III. LES CHIFFRES CLÉS DE LA FILIÈRE 28
3.1 Taille et croissance 28
3.2 Valeur ajoutée 29
3.3 Emplois 30
3.4 Nombre d'entreprises 31
3.5 Les mouvements de fusion - acquisition 32
3.6 Une année dynamique pour les levées de fonds 36
3.7 L'émergence d'un fort écosystème de PME de Confiance Numérique 38

IV. POINT SUR LA MENACE INFORMATIQUE 40
4.1 La menace vue par l'ANSSI 40
4.2 Regards croisés des experts du secteur 44
Focus - SPAC - Tendance marché : Augmentation des attaques hybrides 50

V. LES TENDANCES DE MARCHÉ 53
5.1 Les tendances générales 53
5.1.a. La croissance de la filière française 54
5.1.b. Les marchés de la filière en 2023 55
5.1.c Un manque de main d'œuvre important qui peut être pallié 57
Focus - Ecole 2600 - L'approche « skills first » pour monter en compétences et répondre à la pénurie de main d'oeuvre dans la filière 58
Zoom - Transition écologique dans la filière - Eclairage sur la transition écologique dans la filière 62
Focus - AN2V - Territoires de confiance... numérique : 34 935 communes à soutenir ! 64
5.2 Les tendances réglementaires 68
Focus - Comités Stratégiques de Filière (CSF) 72

VI. LES TENDANCES TECHNOLOGIQUES 74
6.1 Les innovations électroniques et numériques qui génèrent de nouveaux marchés 74
6.2 Les innovations propres à la filière qui génèrent de nouveaux produits 77
6.3 Transformation numérique & miniaturisation : Vers des offres globales de *Security as a Service* *81*
Focus – CNRS, CEA, INRIA - Programme de Recherche (PEPR) de la stratégie nationale pour la cybersécurité 82

A PROPOS DE L'ACN 86

A PROPOS DE DECISION 88

LE MOT DE L'ACN - ALLIANCE POUR LA CONFIANCE NUMÉRIQUE

Daniel Le Coguic
Président de l'ACN

L'Observatoire de la filière de la confiance numérique, que l'ACN a l'honneur de présenter pour la 10ème année consécutive, apporte une analyse toujours plus fine des mutations à l'œuvre dans notre filière. Il constitue un apport significatif dans notre compréhension et notre capacité à anticiper les évolutions du secteur de la confiance numérique et à en déduire les stratégies à mettre en œuvre afin que nos entreprises de l'identité numérique, de la cybersécurité et de l'Intelligence Artificielle de confiance puissent contribuer à la souveraineté numérique de notre pays et à la préservation de nos valeurs fondamentales.

En cette année 2024, une vision stratégique claire est plus que jamais nécessaire pour répondre aux défis qui nous font face. La conflictualité géopolitique atteint des sommets que nous n'avions plus connus depuis des décennies et le numérique constitue un terrain d'affrontement chaque jour plus débridé où les agissements malveillants se multiplient mus par des motivations et des objectifs différents qui s'entremêlent, parfois se confondent et s'amplifient.

Compte-tenu du rôle incontournable du numérique dans l'ensemble de nos activités, il est désormais impératif de sortir de la relative naïveté qui a caractérisé notre développement numérique. Cette naïveté nous a poussés à utiliser massivement des outils, notamment extra-européens, dont on n'a que très peu questionné le niveau de confiance qu'on pouvait leur accorder. Or les risques sont nombreux, depuis le dysfonctionnement de nos systèmes, jusqu'à la captation de nos données personnelles ou stratégiques, en passant par la déstabilisation de nos sociétés démocratiques, l'exposition des citoyens, en particulier, les plus vulnérables, ou encore la perte de notre autonomie stratégique du fait de notre trop grande dépendance technologique dans certains domaines numériques clefs.

Gageons que ce retour de tensions nous permette d'ouvrir les yeux : il est urgent de placer la confiance numérique au centre de notre société. Ce basculement de paradigme majeur est en réalité déjà en train de s'opérer et nous nous réjouissons que nos gouvernants, tant au niveau national qu'européen, aient amorcé ce virage avec un volontarisme réel. Il faut désormais accélérer et amplifier les initiatives déjà initiées, principalement dans trois directions.

Tout d'abord, il s'agit de rattraper nos errements passés, non seulement en augmentant fortement l'équipement en outils de confiance numérique et la résilience de tous les acteurs de nos sociétés mais aussi en poursuivant l'effort de réglementation et de normalisation à l'œuvre en Europe et en France. Des textes législatifs bienvenus (projet de création d'un portefeuille d'identité numériques européen – EUID, projet d'AI Act, Résilience des Entités Critiques – REC, des entités financières – DORA – et des Entités Essentielles/ Importantes – NIS2) sont en cours de délibération : leur mise en œuvre rapide permettra d'élever substantiellement notre niveau de protection. Ces cadres réglementaires vont façonner le terrain de jeu de la confiance numérique et il est impératif pour l'ACN de jouer un rôle proactif dans ces débats pour défendre les intérêts de l'industrie française avec comme objectifs de concevoir et développer des technologies compatibles avec les libertés publiques et individuelles, et acceptables par les citoyens.

Ensuite, nous devons consolider nos acquis et capitaliser sur une filière de la confiance numérique dynamique et performante. L'année 2023 se caractérise par une croissance robuste (9,6%) pour notre secteur, avec un chiffre d'affaires atteignant 19 milliards d'euros en France et 31 milliards d'euros générés à l'échelle mondiale. L'emploi dans le secteur a également connu une augmentation significative, avec 89 000 personnes désormais employées en France et 145 000 dans le monde. Ces chiffres illustrent non seulement la vitalité de notre secteur mais soulignent également l'importance cruciale de la confiance numérique dans le tissu économique et social. Nos entreprises, qu'elles soient des leaders mondiaux ou des PME/start up innovantes, contribuent activement à la sécurisation et la structuration du nouvel espace numérique, tout en favorisant l'innovation et la compétitivité. Il est primordial pour cet écosystème foisonnant de trouver des débouchés marchés, susceptibles de lui permettre d'affronter la concurrence internationale dans des conditions comparables à celle des compétiteurs issus d'autres zones géographiques. La notion de marché domestique est, à cet égard, cruciale : c'est pourquoi, l'Union européenne doit évoluer le plus vite possible vers un marché unique du numérique de confiance. La mise en place rapide d'un « *Buy European Trust Act* », que porte l'ACN dans ses propositions pour les élections européennes de 2024, serait un accélérateur important vers cette ambition.

Enfin, préparer le futur est également une condition afin que nos sociétés puissent continuer à vivre selon les valeurs qui nous sont communes, mais qui ne font pas consensus dans d'autres régions du monde. Cela passe par notre effort de recherche et notre capacité à innover, sans cesse, afin d'être en capacité de maitriser les technologies essentielles à notre souveraineté. L'IA de confiance, le chiffrement post-quantique, l'informatique quantique sont autant de sujets qui questionnent intrinsèquement notre modèle actuel de société. Notre pays et notre continent doivent être à la pointe de l'innovation, tant dans les domaines techniques, qu'intellectuel ou encore réglementaire. Nous disposons d'atouts considérables, d'expertises humaines et techniques reconnues mondialement : ne nous laissons pas distancer.

La France accueille les Jeux olympiques, à Paris, cet été : la filière industrielle française de la confiance numérique et l'ACN se sont mobilisées pour faire de cet évènement majeur une vitrine de notre savoir-faire. « Plus haut, plus vite, plus fort, ensemble » : les messages olympiques entrent en résonnance avec l'horizon de notre industrie.

En conclusion, 2024 doit être une année de consolidation, d'action et d'anticipation. Nous devons continuer à bâtir sur les succès de 2023 tout en adaptant notre approche pour répondre aux défis de demain. L'ACN, en tant que porte-drapeau de la filière de la confiance numérique, a pour mission d'assurer que notre secteur joue, dans ce paysage en mutation rapide, son rôle fondamental au service de la souveraineté numérique nationale et de l'autonomie stratégique européenne.

Relever ces défis sera une œuvre collective. Tous les acteurs de la filière, des start up jusqu'aux aux grandes entreprises doivent renforcer leur collaboration, entre eux, mais aussi avec nos partenaires publics et privés au service de nos enjeux communs : défendre et promouvoir nos valeurs fondamentales pour maîtriser notre avenir numérique et notre avenir tout court.

LE MOT DE LA MINISTRE

Crédit : Ministère de l'Economie, des Finances et de la Souveraineté industrielle et numérique

Marina Ferrari

Secrétaire d'Etat chargée du Numérique

Dans un contexte de tensions géopolitiques renouvelées, la France et l'Union européenne sont confrontées à des défis majeurs pour sécuriser les espaces numériques face à la croissance de la menace cyber, contrer les tentatives de déstabilisation visant nos démocraties par le biais de campagnes massives de désinformation, et mieux protéger les données personnelles de nos concitoyens.

La transformation numérique de notre économie et de notre société est une réalité incontournable, porteuse de promesses fortes. Mais elle s'accompagne d'un besoin accru de sécurité, de transparence et de fiabilité dans l'utilisation des technologies numériques ; en un mot, de confiance numérique. C'est pourquoi cette filière joue un rôle essentiel pour accompagner ces mutations. L'identité numérique, la cybersécurité, et l'intelligence artificielle de confiance sont ainsi au cœur des préoccupations du Gouvernement et mon action, en tant que Secrétaire d'Etat en charge du Numérique, est fondée sur deux priorités fortes que sont la résilience et la souveraineté.

En matière de résilience, cette année sera résolument celle de la mise en place de mesures concrètes qui nous permettront collectivement de mieux faire face au risque cyber. La transposition dans notre droit national des directives REC, DORA et NIS2 vise à élever le niveau général de sécurité numérique en France en permettant aux entités concernées, désormais beaucoup plus nombreuses, de mieux se protéger sur tous les maillons de la chaîne de valeur. Afin de donner toute leur force à ces dispositions, il est essentiel de veiller à ce qu'elles soient ambitieuses, mais également proportionnées, adaptées et raisonnables pour toutes les parties prenantes, notamment les petites et moyennes entreprises qui sont au cœur de notre économie numérique. C'est pourquoi les travaux préparatoires de ces textes ont été menés en co-construction avec les entités régulées pour parvenir à une mise en œuvre équilibrée, favorisant ainsi un environnement numérique robuste, sans entraver l'innovation ni la compétitivité.

Le rôle de la filière de la confiance numérique est crucial dans la consolidation de ce cadre. Je sais pouvoir compter sur l'écosystème français, qui compte à la fois des grands acteurs structurants

et de très nombreuses start-up et PME qui sont autant de pépites technologiques. L'enjeu pour la filière sera de collaborer de manière efficace, entre les différents fournisseurs de services et de technologies, pour développer et mettre à disposition de tous les utilisateurs des solutions intégrées, cohérentes et conformes à leurs enjeux. En tant que syndicat professionnel, l'Alliance pour la Confiance Numérique (ACN) a un rôle déterminant à jouer pour dynamiser l'action collective des entreprises de la filière. C'est également la raison d'être de l'initiative « Je choisis la French Tech », qui vise à encourager tous les acheteurs publics et privés à mieux intégrer les solutions disponibles dans notre vivier national d'entreprises numériques.

Le renforcement de notre niveau de résilience, mais également de notre filière de la confiance numérique, sont la condition sine qua non de notre souveraineté numérique, dans un environnement où les acteurs étatiques comme non étatiques exploitent les vulnérabilités informatiques de nos entreprises et nos administrations pour perturber le bon fonctionnement de notre société. Au-delà de l'enjeu sécuritaire, c'est de la défense de notre démocratie dont il s'agit.

Pour ce faire, nous devons nous doter des capacités qui permettront à la France et à l'Europe de maîtriser, avec le plus grand degré d'autonomie possible, l'avenir numérique de nos concitoyens. Cela passe par une attention particulière pour la formation et la sensibilisation, mais aussi par un effort accru pour développer et structurer notre écosystème dans des domaines stratégiques tels que le quantique et l'intelligence artificielle. La confiance, fondée sur le triptyque de critères juridiques, techniques et éthiques que pose, à juste titre, l'ACN dans son Livre blanc sur l'intelligence artificielle de confiance, doit être notre boussole dans la construction de notre futur numérique. Le Gouvernement est fortement mobilisé dans cette perspective et conduit des initiatives structurantes, notamment à travers le plan France 2030, pour renforcer notre tissu économique. L'effort de soutien à la recherche et l'innovation que nous déployons, tant au niveau national qu'européen, doit servir à créer un effet de levier et renforcer in fine les compétences de notre pays et de l'Europe dans ces domaines.

Renforcer notre souveraineté numérique, c'est enfin assurer à chaque citoyen une identification et une authentification avec le plus haut niveau de sécurité lorsque l'usage le requiert, mais également la plus grande facilité d'usage. Sous l'impulsion de l'Union européenne, la création de portefeuilles d'identités numériques est résolument engagée. Ces nouveaux outils permettront à la fois de sécuriser les échanges mais aussi de renforcer la protection des données personnelles de chacun et de mieux protéger les mineurs face à des contenus sensibles et choquants. C'est, là aussi, un enjeu crucial de confiance dans le numérique pour lequel la loi visant à sécuriser et réguler l'espace numérique, adoptée par le Parlement le 10 avril dernier, apporte des réponses ambitieuses.

Protéger nos concitoyens, nos entreprises, nos administrations et nos valeurs dans l'espace numérique est plus que jamais indispensable. Ce faisant, nous devons impérativement conserver notre souveraineté numérique comme ligne d'horizon. A bien des égards, nous vivons des moments décisifs et je suis convaincue que c'est par le collectif que nous parviendrons à défendre et à promouvoir nos valeurs dans le numérique. Soyons acteurs de notre avenir, nous en avons les moyens.

ÉLÉMENTS CLEFS

La filière de la **Confiance Numérique** qui regroupe la **sécurité numérique** (identité numérique, systèmes et sous-systèmes électroniques de confiance, IA de confiance, OSINT), ainsi que la **cybersécurité** (produits / logiciels et services) est cruciale dans notre économie et dans notre société en pleine mutation numérique.

L'**Alliance pour la Confiance Numérique (ACN)** est le syndicat professionnel qui a pour mission de regrouper et soutenir les acteurs de cette filière en France et en assurer la représentation institutionnelle.

L'ACN a mis en place un **Observatoire de la Confiance Numérique** pour recueillir et mettre en commun des données sur les grandes caractéristiques et les tendances de cette filière ; c'est dans ce cadre que cette étude a été réalisée en 2024, couvrant le champ de la cybersécurité et de la sécurité numérique.

La Confiance Numérique en France en 2023 c'est :

19 milliards d'euros de chiffre d'affaires en France

- **19 milliards d'euros de chiffre d'affaires,** soit 9,6% de croissance entre 2022 et 2023 ;
- **9 milliards d'euros de valeur ajoutée ;**
- **89 000 personnes employées** dans le secteur **;**
- Un **chiffre d'affaires** réparti à **55% pour la Cybersécurité et à 45% pour la Sécurité Numérique.**

Les entreprises françaises de la Confiance Numérique dans le monde en 2023 c'est :

31,3 milliards d'euros de chiffre d'affaires à l'international

- **31,3 milliards d'euros de chiffre d'affaires** générés dans le Monde par la filière française de la Confiance Numérique (CA France, CA exporté depuis la France et CA réalisé à l'étranger par des entreprises détenues par des capitaux français) ;
- Des **leaders mondiaux** sur les segments de la sécurité numérique (Thales, Airbus D&S, Atos Eviden, ST Microelectronics), de la gestion des identités et des accès (Thales, Idemia, IN Groupe, Docaposte), des services de cybersécurité (Thales, Atos Eviden, Orange Cyberdefense, Sopra Steria, Capgemini), et de la sécurisation des paiements (Worldline) ;
- **18 milliards d'euros de chiffre d'affaires à l'international,** soit 57% du CA total (CA exporté depuis la France et CA réalisé à l'étranger par des entreprises détenues par des capitaux français) ;
- **5,7 milliards d'euros de chiffre d'affaires à l'exportation depuis la France,** soit un taux d'export moyen de 30%.

La Confiance Numérique est une filière à part entière :

9.6% de croissance en France en 2023

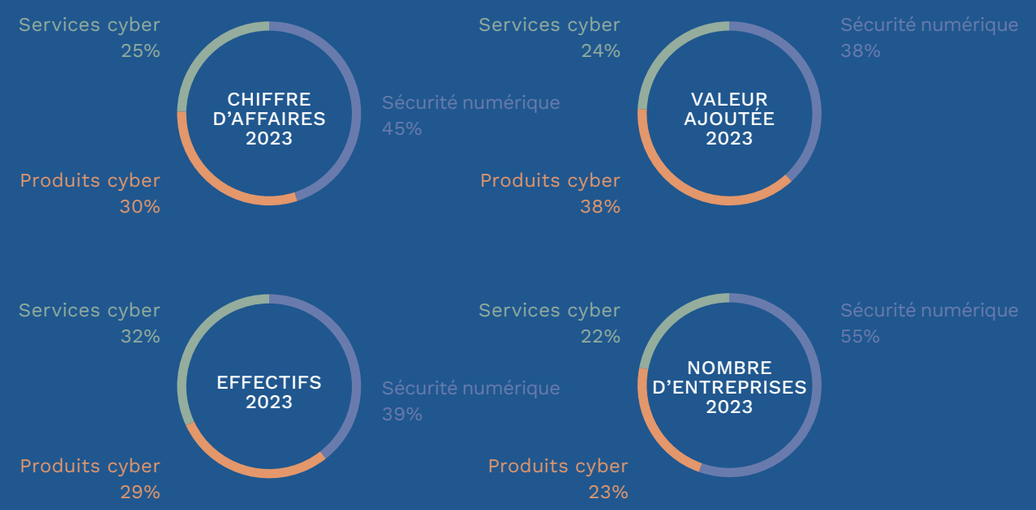
- **8%** de croissance moyenne annuelle en France sur la période 2018-2023, contre **0,7%** pour le PIB français* (*Croissance du PIB mesurée par l'INSEE en volumes chainés).
- La Confiance Numérique est la filière industrielle française qui bénéficie de la croissance **la plus forte**, et ce depuis 10 ans.
- **La Confiance Numérique s'est montrée particulièrement résiliente face à la crise de la COVID en 2020**, avec 3,6% de croissance en 2020 contre -7,8% pour le PIB français.
- La Confiance Numérique est la filière **la plus productive**, c'est-à-dire avec le plus fort ratio Valeur Ajoutée / Chiffre d'affaires.

La Confiance Numérique est un écosystème d'entreprises de toutes tailles :

2 178 entreprises dans la filière en France

- **2 178 entreprises** dans la filière en France ;
- Dont **75 grandes entreprises ;**
- Dont **68 ETI** (Entreprises de Taille Intermédiaire) ;
- Dont **635 PME** (Petites et Moyennes Entreprises) ;
- Dont **1 399 micro-entreprises**, générant moins de 2 millions de CA en 2023.

Les principaux segments de la Confiance Numérique



Sources : DECISION études et conseils

FONDAMENTAUX 2023

Chiffre d'affaires

31.3 MDS € de CA monde

- 12.3 MDS € de CA hors de France
- 19 MDS € de CA France
  - dont 5,7 MDS € de CA Export

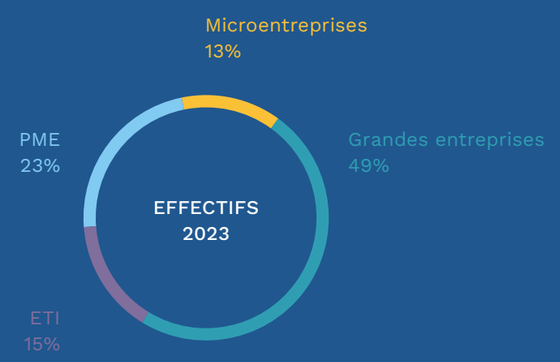
9 MDS € VA* France

*(valeur ajoutée)

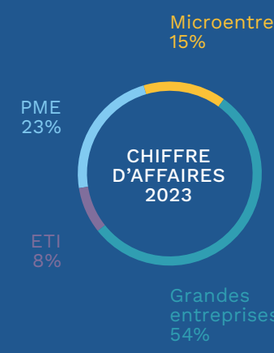
Emplois

89 000
Emplois en France en 2023

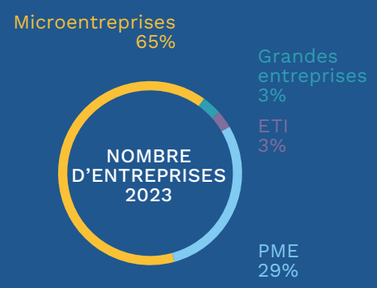
144 700
Emplois dans le monde en 2023



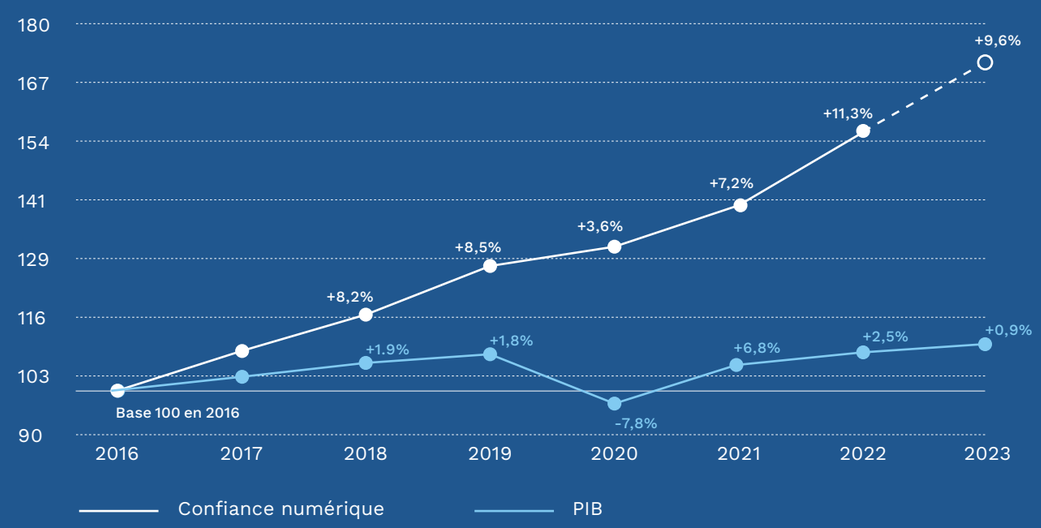
Croissance



9.6%
de croissance en 2023



Croissance France comparée 2017-2023



Croissance du PIB mesurée par l'INSEE et par le FMI pour l'année 2023

Source : DECISION Etudes & Conseils

Top 15 acteurs France

N°	Entreprises	CA Confiance Numérique France
1	**THALÈS**	2 304 M€
2	**AIRBUS D&S**	1 155 M€
3	**IDEMIA**	471 M€
4	**DOCAPOSTE**	446 M€
5	**EVIDEN**	436 M€
6	**ORANGE CYBERDEFENSE**	434 M€
7	**SOPRA STERIA**	355 M€
8	**IN GROUPE**	337 M€
9	**IBM**	310 M€
10	**ACCENTURE**	283 M€
11	**FORTINET**	186 M€
12	**EQUANS**	176 M€
13	**NOMIOS**	174 M€
14	**WORDLINE**	160 M€
15	**ASSA ABLOY**	147 M€

- Thales comprend Gemalto et Ercom.
- Atos comprend Idnomic, Ipsotek, Motiv ICT Security, Sec consult, In fidem, Paladion...
- Orange Cyberdéfense comprend Securelink, Securedata, Lexsi...
- Sopra Steria comprend CS Group, Tobania, Ordina, Sodifrance, Bluecarat, Kentor, Eva Group...
- Capgemini comprend Altran et Leidos Cyber.
- Docaposte comprend AR24, CDC Arkhineo, Open Value...
- Accenture comprend Arismore, Link by net, Openminded...
- Chapvision / Flandrin technologies comprend Deveryware, Bertin IT, Vecsys, Elektron, Owlint et Geotrend.
- Idemia comprend Otono Networks.
- IN Groupe comprend Surys et Nexus.
- Econocom comprend Exaprobe.
- Wordline comprend Ingenico.
- GFI Informatique comprend SIS.
- Cisco comprend Sentryo.
- Sogetel comprend Eryma.

Emergence d'un écosystème de distributeurs de produits et services de cybersécurité

Top 1-10 acteurs France

Top 10-20 acteurs France

CA Confiance Numérique France compris entre 115M€ et 230M€

Top 20-50 acteurs France

CA Confiance Numérique France compris entre 55M€ et 115M€

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

Top 15 acteurs Monde

N°	Entreprises	CA Confiance Numérique Monde
1	**ASSA ABLOY**	5 789 M€
2	**THALÈS**	5 677 M€
3	**FORTINET**	4 970 M€
4	**ACCENTURE**	4 602 M€
5	**IBM**	3 217 M€
6	**IDEMIA**	2 850 M€
7	**AIRBUS D&S**	1 924 M€
8	**EVIDEN**	1 499 M€
9	**ORANGE CYBERDEFENSE**	1 083 M€
10	**SOPRA STERIA**	600 M€
11	**IN GROUPE**	553 M€
12	**DOCAPOSTE**	496 M€
13	**NOMIOS**	400 M€
14	**EQUANS**	264 M€
15	**WORLDLINE**	180 M€

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

■ **Thales** a créé un leader mondial de la sécurité digitale avec le rachat de Gemalto en 2019

■ **Thales, Idemia, Docaposte** et **IN Groupe** sont des leaders mondiaux de l'identité numérique, de l'identification et de l'authentification

■ **Airbus Defence & Space** est l'un des leaders européens en sécurité numérique et mondial en observation large zone et communications sécurisées

■ **Atos (Eviden), Orange, Sopra Steria** et **Capgemini** sont les 4 leaders français parmi les entreprises de services du numérique (classement SITSI), et sont également les leaders français en matière de cybersécurité (avec **Thales** et **Airbus Defence & Space**)

■ **Docaposte** est un leader français présent sur de nombreux segments de la sécurité numérique et des produits cyber. Docaposte est à l'initiative d'une offre de cloud souverain « Numspot », annoncée à l'automne 2022. En collaboration avec Dassault Systèmes, Bouygues Télécom et la Banque des Territoires, cette offre de cloud souverain permettra d'opérer des services de confiance bénéficiant de la qualification SecNumCloud

■ L'américain **Accenture** maintient son positionnement dans le top 10 grâce aux précédents rachats rachats (Arismore, etc.)

ACN
Alliance pour la confiance numérique

L'ACN EST AU COEUR DE LA FILIÈRE

Parmi les adhérents de l'ACN, on trouve :

■ **14 grandes entreprises ou ETI, parmi lesquelles les 9 leaders français de la Confiance Numérique.**
■ Mais aussi **plus de 100 PME, TPE et startups innovantes adhérents directs et plus de 200 PME du secteur** via les écosystèmes de ses membres partenaires (Bretagne Développement Innovation, Pôle SCS, SPAC,
etc).

Les membres de l'ACN représentent :

64%
du CA des entreprises francaises dans le monde
16,1 mds € en 2023

83%
du CA des entreprises francaises dans le monde en sécurité numérique

61%
du CA des entreprises francaises dans le monde en cybersécurité

80%
du CA réalisé à l'internationnal par les entreprises francaises
12,2 mds € en 2023

I. CONFIANCE NUMÉRIQUE : CYBERSÉCURITÉ ET SÉCURITÉ NUMÉRIQUE

Parmi les acteurs situés entre la 10ème et la 20ème position et réalisant en CA Confiance Numérique supérieur à 115M€ depuis la France en 2023, on trouve des acteurs français tels que Cap Gemini et Nomios (services cyber), Worldline (sécurité des paiements), Safran, Equans (sécurité numérique) et Selp (identification et documents sécurisés), mais aussi des acteurs étrangers: Assa Abloy (contrôle d'accès et authentification) , Linxens (cartes à puces), Fortinet (produits cyber), et Econocom (services cyber).

Les entreprises situées aux environs de la cinquantième position dans la filière ont des CA France de confiance numérique qui avoisinent tous les 55 M€ : Somfy, Securitas (Stanley Security), Serma Safety & security, Schneider, Honeywell, Palantir, Devoteam, SAP, Oracle, Bechtle, Inetum, Claranet, Computacenter, Scalian... Enfin, si les acteurs français dominent largement le top 10 de la filière, on trouve parmi les acteurs du top 10-50 une plus forte présence d'entreprises étrangères implantées en France, en particulier américaines.

1.1 Cybersécurité et Sécurité Numérique : deux domaines complémentaires

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

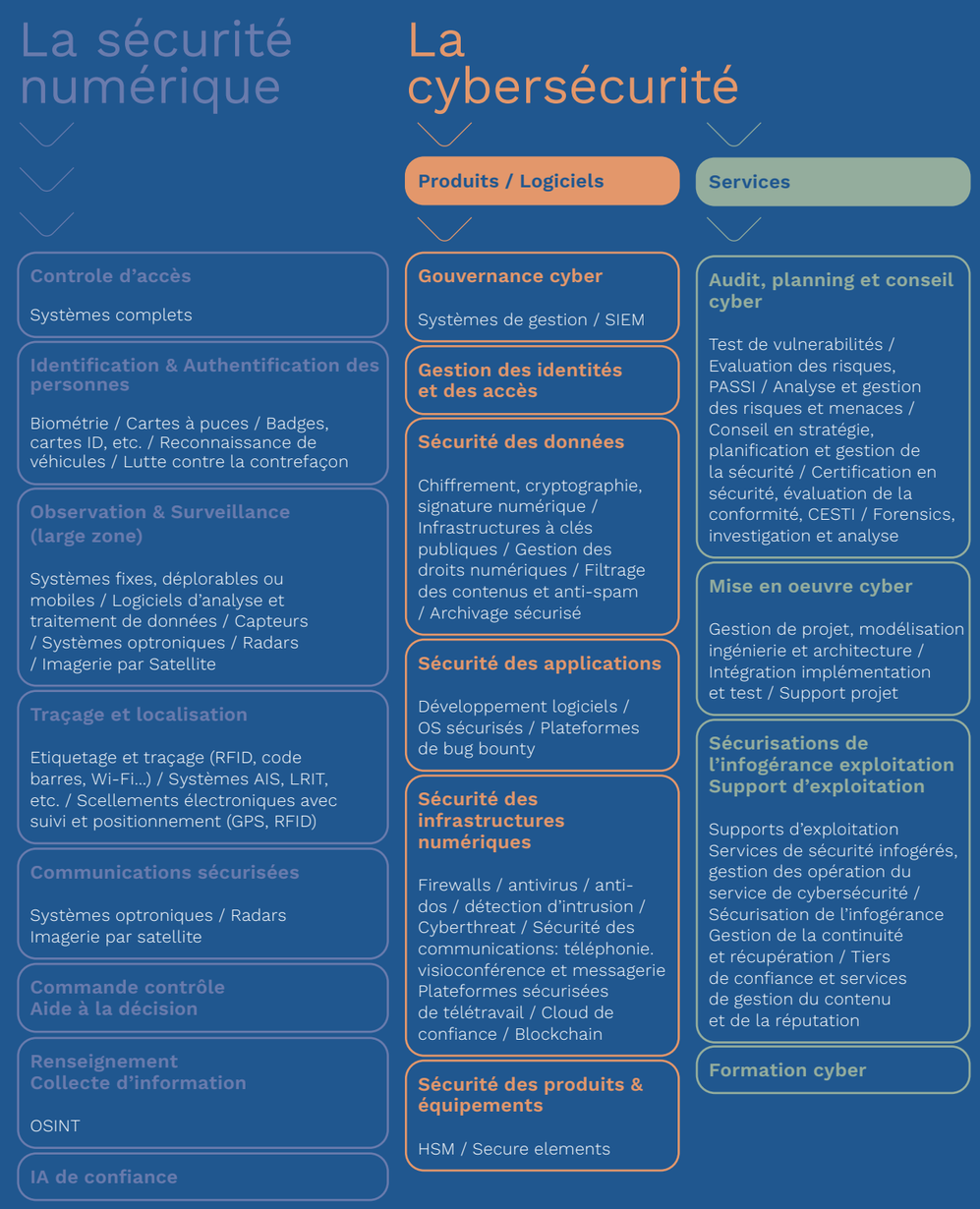
L'Observatoire de la Confiance Numérique couvre deux industries :

1. La Cybersécurité proprement dite, qui correspond à la sécurisation «interne» des systèmes numériques. La cybersécurité regroupe deux types d'activités souvent associées dans la pratique, les services (conseil, conception, mise en place, exploitation, formation), et les logiciels et solutions, destinés aux marchés professionnels (Etat et secteur public, installations critiques, entreprises, PME) et grand public (ordinateurs, smartphones, maison, véhicules et objets connectés, etc).

2. La Sécurité Numérique, c'est-à-dire les produits et solutions électroniques de mise en œuvre de systèmes numériques pour instaurer la confiance dans le monde extérieur. Ces systèmes mettent en œuvre des moyens numériques sécurisés pour instaurer la confiance dans l'environnement citoyen, en particulier par la gestion des identités, la gestion des accès, la biométrie, les transactions, les objets et les véhicules connectés, les processus industriels et la logistique, les transports, les réseaux, les villes intelligentes, IA de confiance et OSINT, etc. Les produits de sécurité numérique sont des produits matériels (cartes à puce, documents, lecteurs, etc.) ou des équipements (gestion des accès, biométrie, détection, localisation, etc.).

1.2 Le Périmètre de la Confiance Numérique - Segmentation

Le diagramme ci-dessous présente les différents segments de la Confiance Numérique, répartis en trois domaines :



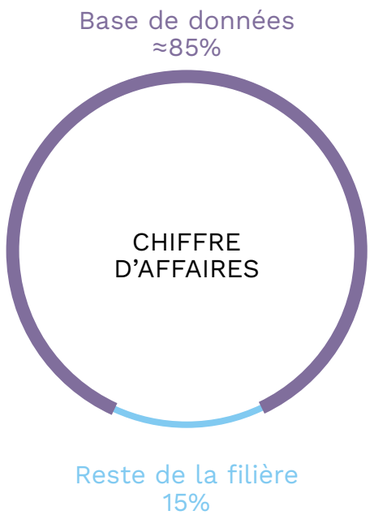
1.3 Méthodologie

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

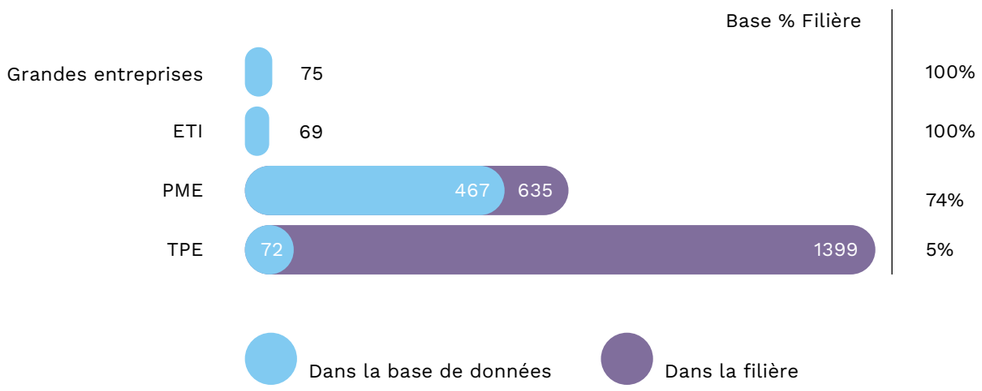
Le cabinet d'études DECISION Etudes & Conseil conduit cet Observatoire depuis 2017. Les données présentées dans ce rapport sont issues d'une base de données de DECISION recensant 683 entreprises parmi les 2 178 que compte la filière de la Confiance Numérique. Cette base de données prend en compte :

■ La totalité des grandes entreprises de la filière (75/75) ;
■ La totalité des entreprises de tailles intermédiaires (ETI) de la filière (68/68) ;
■ La majorité des petites et moyennes entreprises (PME) de la filière (467/635) ;
■ Les très petites entreprises (TPE) et startups les plus remarquables et innovantes (72/1399).

Ainsi, bien que seul 31% des entreprises de la filière soient prises en compte dans la base de données, celle-ci est représentative de 85% du chiffre d'affaires total de la filière de Confiance Numérique France.



Nombre d'entreprises



Collecte d'information pour la base de données

Pour chaque entreprise de la base de données sont collectées chaque année les données suivantes pour la France :

■ Les données administratives : SIREN, SIRET, adresse, code NAF, nom de l'actionnaire principal du groupe, date de création, nom et fonction du dirigeant, contacts (mail, numéro de téléphone), etc.
■ Les données économiques sur la période 2015-2023 : Chiffre d'affaires, effectifs, chiffre d'affaires à l'exportation, valeur ajoutée, résultat net.

Analyse des acteurs et segmentation

DECISION effectue ensuite une analyse spécifique à chaque entreprise afin d'estimer la part de l'activité dédiée à la confiance numérique et la répartition du chiffre d'affaires selon les 17 segments de l'ACN (la segmentation ACN est désormais pleinement intégrée dans la segmentation plus large du Comité Stratégique de la Filière des industries de sécurité). Cette analyse des entreprises est réalisée grâce à l'expertise de DECISION sur le secteur de la sécurité depuis 10 ans, et notamment grâce aux entretiens directs conduits avec les acteurs clefs de la filière. Enfin, un questionnaire en ligne est envoyé chaque année aux membres de la filière et permet d'affiner les analyses.

A partir des informations de la base de données, une méthode d'extrapolation a été mise en place afin de construire des chiffres pour l'ensemble de la filière en France.

Calcul de la croissance

La **croissance** en France est estimée chaque année sur chacun des segments à travers un arbitrage entre trois composantes :

■ **Base de données** : Une analyse en sous-échantillon est effectuée afin de mesurer la croissance totale en France des acteurs représentatifs de chaque segment, c'est-à-dire des entreprises réalisant plus de 10% de leurs chiffres d'affaires grâce à leurs activités sur le segment concerné.

■ **Documents issus des entreprises** : L'analyse des rapports annuels, des documents financiers et des communications des entreprises de la filière.

■ **Questionnaire en ligne** : Le questionnaire en ligne renseigné chaque année par les membres de la filière fournit notamment des données sur la croissance de l'année passée. Pour l'édition 2024, les membres ayant répondu au questionnaire représentent 9% du CA de la filière en France.

Enfin, une analyse spécifique de l'évolution de l'activité mondiale (globale et sécurité), des principaux acteurs de la Confiance Numérique est effectuée chaque année pour estimer le chiffre d'affaires réalisé par la filière à l'étranger ainsi que son évolution.

COMPARAISONS PAR RAPPORT AUX PRÉCÉDENTS OBSERVATOIRE

Chaque année, en plus de l'estimation de la croissance, DECISION affine la segmentation des différents acteurs de la filière, notamment grâce aux informations issues du questionnaire en ligne.

En conséquence, **les chiffres en valeur absolue de chaque édition de l'observatoire ne sont pas directement comparables entre eux.** Les chiffres de cet Observatoire sont présentés pour l'année 2023 et en fonction de la nouvelle segmentation des acteurs. Les chiffres 2022 actualisés sont présentés page 13 de ce rapport.

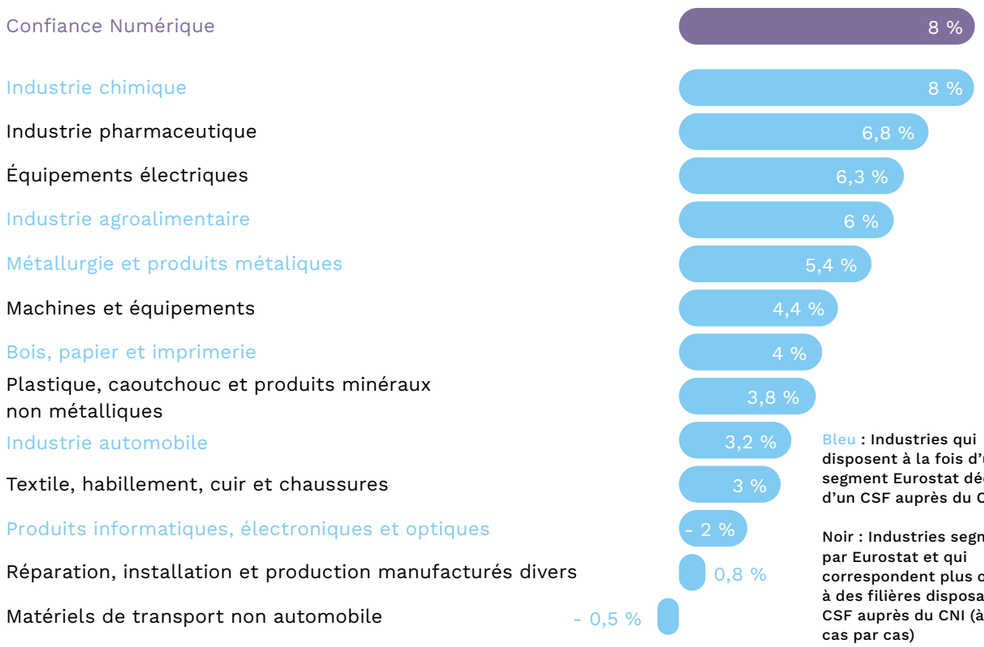
II. CONFIANCE NUMÉRIQUE : UNE FILIÈRE IMPORTANTE ET DYNAMIQUE

2.1 La Confiance Numérique est l'une des industries françaises qui bénéficient de la croissance la plus forte sur la période 2016-2022

Sur la période 2016-2022, la Confiance Numérique est l'une des filières industrielles françaises qui bénéficie du plus fort taux de croissance, avec 8%/an en moyenne. Bien que mesurées selon une méthode qui n'est pas directement comparable, les seules autres filières industrielles françaises qui bénéficient d'une croissance similaire sont l'industrie chimique, l'industrie pharmaceutique, l'industrie des équipements électriques, l'industrie agroalimentaire ainsi que l'industrie de la métallurgie et produits métalliques. Les autres industries bénéficient d'une croissance annuelle moyenne entre 0% et 5% sur la même période, voir négatif comme le cas des Matériels de transports hors automobile.

La Confiance Numérique est l'une des quatre filières (sur un total de quinze) à ne pas avoir souffert d'une récession en 2020. Avec une croissance de 3,6% cette année là, il s'agit de la filière qui a le mieux résisté à la crise du COVID et ses conséquences. Cette résilience traduit des besoins pérennes en biens et services de Confiance Numérique. Si bien qu'à horizon 2030, la Confiance Numérique pourrait devenir la 11ème filière industrielle française sur 15 en valeur ajoutée en dépassant à la fois la filière de l'équipement électrique et la filière réparation, installation et production manufacturés divers.

Croissance annuelle moyenne des filières Françaises sur la période 2016-2022



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

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

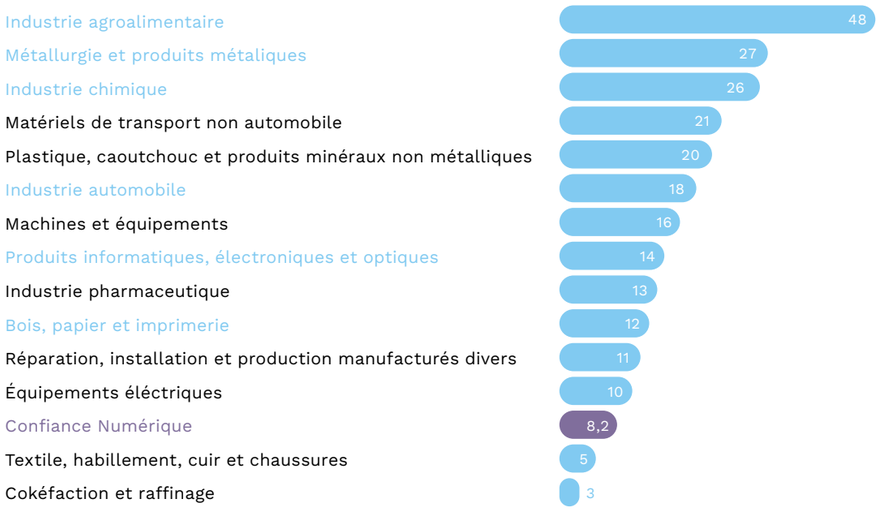
Source : DECISION, basé sur des données Eurostat de 2016 à 2020

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

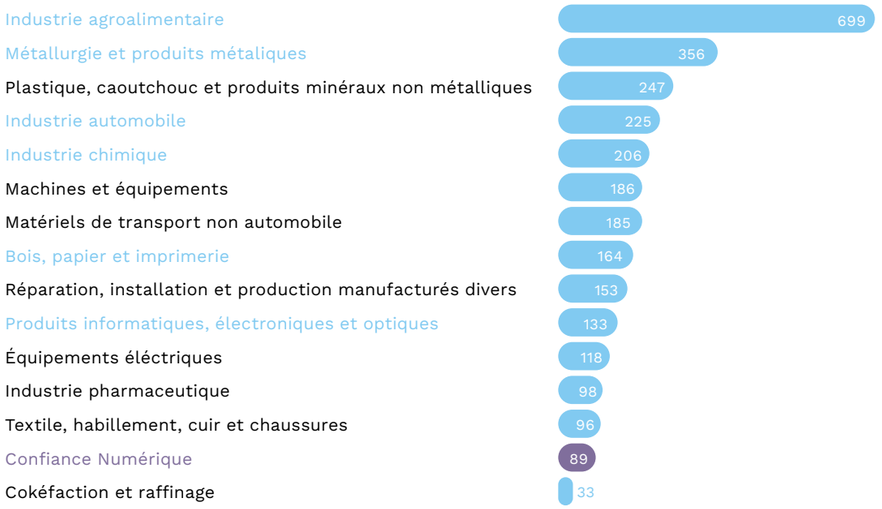
La Confiance Numérique est une filière industrielle à part entière. En termes de valeur ajoutée, elle avoisine la filière du textile et de l'habillement et se rapproche de la filière des équipements électriques ou encore du bois, papier et imprimerie.

En termes d'emploi, elle dépasse largement la filière de cokéfaction et se rapproche de la filière du textile et de l'habillement.

Valeurs ajoutées des filières françaises en 2021 (MDS €)



Emplois des filières françaises 2020 (en millier)



Bleu : Industries qui disposent à la fois d'un segment Eurostat dédié et d'un CSF auprès du CNI.
Noir : Industries segmentées par Eurostat et qui correspondent plus ou moins à des filières disposant d'un CSF auprès du CNI (à voir au cas par cas)

Source : Decision, Eurostat, OCDE

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

La Confiance Numérique est la filière la plus productive avec un taux de valeur ajoutée de 47% (Valeur Ajoutée / Chiffre d'affaires). En d'autres termes, la Confiance Numérique est la filière industrielle dont le degré de création de richesse, c'est-à-dire de transformation des produits au cours de l'activité est le plus élevé. Ainsi, l'augmentation du chiffre d'affaires de cette filière se traduit en moyenne par un plus fort taux d'activité transformatrice sur le sol français en comparaison des autres filières industrielles françaises.

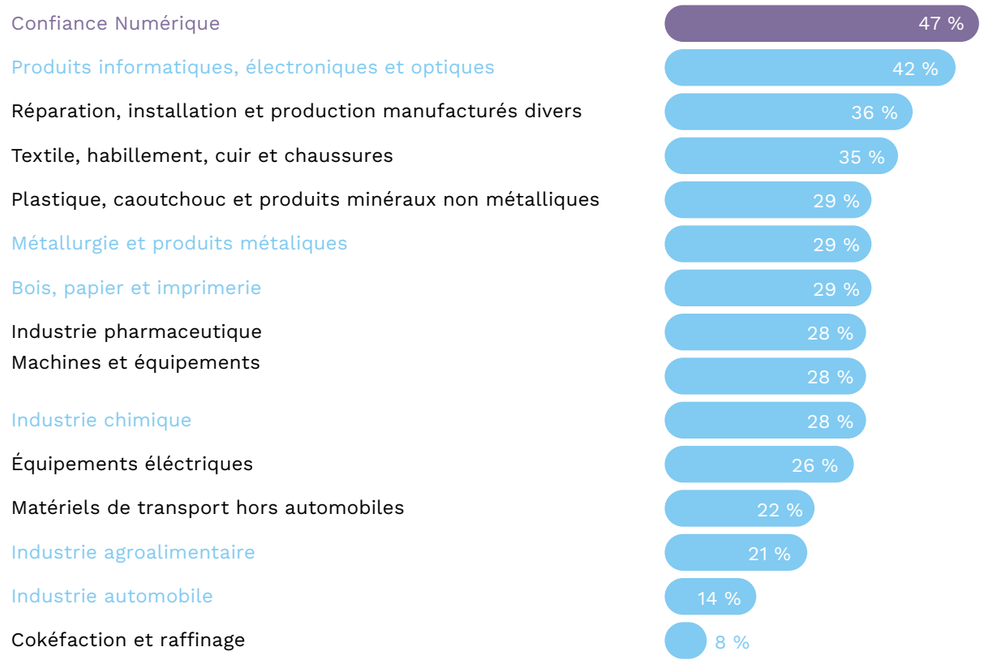
Ce phénomène s'explique principalement par trois facteurs :

1. **Le pourcentage de l'activité dédiée aux services est relativement élevé dans la filière française de Confiance Numérique** (25% en 2023), à travers les services de cybersécurité (conseil, audit, formation, etc.). Les activités de services ont par définition un taux de valeur ajoutée très fort car ils utilisent très peu de consommations intermédiaires et correspondent presque exclusivement à de la transformation des produits au cours de l'activité. Cependant, ce phénomène ne justifie pas à lui seul que l'industrie de sécurité française soit la première en matière de taux de valeur ajoutée car la plupart des filières industrielles françaises comprennent également une partie conséquente de services.

2. Les produits électroniques dédiés à la Confiance Numérique (sécurité numérique) représentent 45% du chiffre d'affaires total de la filière de la Confiance Numérique. Or, alors même qu'en ce qui concerne l'industrie électronique française dans son ensemble, une grande partie des étapes de production en amont de la chaine de valeur est réalisée en Asie, **ce phénomène ne s'applique que peu au segment de la Confiance Numérique qui maintient autant que faire se peut toutes les étapes de la production en France en raison de sa proximité avec les secteurs régaliens**. D'autres filières françaises se concentrent plus fortement sur des activités d'intégration en amont de la chaîne de valeur et sur des activités d'ingénierie pure (design, développement, etc.). Etant donné qu'une grande partie de la chaîne de valeur de l'industrie de sécurité numérique est réalisée depuis la France, le taux de valeur ajoutée augmente.

3. Enfin, les produits de cybersécurité correspondent à 30% du CA total de la filière de sécurité et impliquent **une très grande partie de travail humain hautement qualifié** (développement de logiciels, etc.), associé à un taux de valeur ajoutée très élevé (à des niveaux avoisinants ceux des services de cybersécurité).

Taux de valeur ajoutée (VA/CA des filières francaise en 2021)



Bleu : Industries qui disposent à la fois d'un segment Eurostat dédié et d'un CSF auprès du CNI.
Noir : Industries segmentées par Eurostat et qui correspondent plus ou moins à des filières disposant d'un CSF auprès du CNI (à voir au cas par cas)

Source : Decision, Eurostat, OCDE

2.4 Les acteurs français sont au meilleur niveau en matière de compétences et de R&D

Grâce notamment à l'excellence française en matière de recherche et développement, **la grande majorité des entreprises françaises de la Confiance Numérique est positionnée 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 GAFAM ont installé depuis plusieurs années des centres de recherche dédiés à cette thématique et débauchent de nombreux talents français. Du côté de la R&D publique, l'INRIA dispose notamment d'équipes dédiées aux stratégies de défense et d'attaque via le *deep learning*.

Technologies post-quantique (dont cryptographie) :
La France se maintient dans le top trois mondial. D'ici quelques années, 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.

Cryptographie :
La France fait historiquement partie des leaders mondiaux et maintient sa position.

La France est également en bonne position en **blockchain** et en **sécurisation des objets connectés.** La recherche publique souffre cependant du peu d'effectifs dédiés au Big data. La France dispose notamment de près de 1 000 chercheurs académiques affectés à temps plein à des thématiques de cybersécurité, notamment dans les campus de Rennes, Paris-Saclay, Brest, Grenoble et Lyon.

2.5 La croissance de la Confiance Numérique s'inscrit dans une dynamique mondiale

Au niveau mondial, la croissance de la Confiance Numérique est portée par quatre facteurs, dont les trois premiers ne sont pas propres 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. Il s'agit d'un phénomène de long terme. A court terme, la croissance des composants électroniques est cyclique et la période 2020-2022 a au contraire vu les prix des semi-conducteurs s'envoler. Depuis le début de l'année 2023, la baisse des prix de semi-conducteurs a repris son cours.

2. **La transformation numérique**. Accélérée par la crise du COVID en 2020, les entreprises et administrations du monde entier numérisent leurs processus, déploient des *clouds* et interconnectent les réseaux de données.

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 la Confiance Numérique et sur lesquelles la France est souvent très bien positionnée aussi bien en termes d'acteurs industriels que de savoir-faire scientifique : biométrie comportementale, innovations associées aux éléments sécurisés, développements cryptographiques, analyse en temps réel des données d'observations large zone, *blockchain*, etc.

La France bénéficie historiquement d'une filière de défense et de sécurité puissante et fortement exportatrice au regard de la moyenne internationale et a su mettre à profit son excellence en matière de recherche et développement pour tirer profit de ces quatre tendances mondiales et ainsi construire une solide filière de Confiance Numérique. La croissance est cependant encore plus forte dans les industries de Confiance Numérique américaine et surtout chinoise.

2.6 Une concurrence croissante de la part des acteurs étrangers

Les acteurs de nationalité française génèrent 74% du chiffre d'affaires de la Confiance Numérique en France, soit 14,1 milliards d'euros en 2023. Autrement dit, **les acteurs étrangers de la filière réalisent 26% du chiffre d'affaires de la filière en France**, soit environ 5 milliards d'euros en 2023. Ce chiffre correspond uniquement au chiffre d'affaires généré par les filiales d'acteurs étrangers en France et n'inclut pas les exportations des acteurs étrangers vers la France (qui n'a pas pu être mesuré dans cet observatoire).

Si la part de la richesse produite en France par des acteurs français est encore assez élevée, elle baisse régulièrement depuis 2013 jusqu'en 2023 et cette tendance devrait se poursuivre. On assiste en particulier depuis plusieurs années au développement d'acteurs américains en France, notamment à travers l'installation de nouveaux sièges sociaux : Microsoft, Dell, Palantir, Docusign, AWS, Google, Cisco, Check Point Systems, Crowdstrike International, Juniper Networks, Nutanix, F5 Networks, Palo Alto Networks, Rubrik, Okta, Netskope, Forescout technologies, Aruba, Tufin Software, Quest software, Proofpoint, etc. Les acteurs chinois se développent également, avec depuis peu des offres de haut niveau capables de concurrencer sur le plan technique les offres françaises.

De même que pour la production en France, le poids des acteurs étrangers sur le marché français est important : il avoisinerait les 40%. Autrement dit, le marché national reste largement influencé par des solutions étrangères et non européennes, alors que la filière française dispose d'offres dans tous les segments et compte dans ses rangs des fleurons technologiques et de nombreux acteurs déjà de taille à couvrir à minima l'ensemble du marché national.

Des rachats significatifs d'entreprises françaises par des acteurs étrangers ont eu lieu dans la plupart des segments de la Confiance Numérique sur la période 2013-2021. Parmi ces rachats figure celui d'Arismore par Accenture (Etats-Unis), de DenyAll par Rohde & Schwarz Cybersecurity (Allemagne), ou encore d'Oberthur Technologies (racheté par le fond américain Advent en 2011) puis Safran Morpho (racheté par Advent en 2018) et fusionné avec Oberthur Technologies sous la marque Idemia en 2018. **Depuis 2021, le nombre et la taille de ces rachats tend cependant à baisser**, si bien que le seul rachat d'entreprise française de taille significative par une entreprise étrangère identifié est celui d'Akka Technologies par le suisse Adecco en 2022.

Enfin et surtout, de nombreux acteurs de la filière de la Confiance Numérique relèvent une absence dommageable de culture d'achat de produits français, aussi bien de la part des entreprises que des administrations. Cette absence de culture d'achats de produits français a naturellement conduit les entreprises et les administrations françaises à se tourner vers des offres étrangères. En effet, dans un contexte général de stagnation de la croissance (0,7%/an de croissance du PIB français sur la période 2018-2023), d'inflation, et d'austérité budgétaire du côté des services publics, le premier critère d'achat s'avère souvent être le prix. Or, les acteurs américains et chinois sont souvent plus compétitifs que les français sur le seul critère du prix (notamment en raison d'économies d'échelles plus importantes et d'une sous-traitance plus forte dans des pays à faibles coûts salariaux). **En plus de pénaliser les acteurs français de la filière, l'achat de solutions étrangères non maîtrisées est susceptible de menacer la souveraineté de la France lorsque les acheteurs sont des organismes publics, des OIV (Opérateurs d'Importance Vitale), et/ou des OSE (Opérateurs de Services Essentiels).** Malgré la récente prise de conscience des enjeux de souveraineté et d'autonomie stratégique, le manque de culture d'achat de produits français se fait particulièrement ressentir au niveau du secteur public et des grandes entreprises françaises.

Le triptyque standardisation, certification et prescription, notamment porté par l'ANSSI, permet de garantir l'utilisation de solutions fiables et sécurisées tout en déplaçant la compétition non plus uniquement sur le terrain du prix mais également sur celui de l'excellence technique, favorisant ainsi naturellement les acteurs français.

2.7 Conclusion - Une filière à très fort potentiel si les bons choix stratégiques sont réalisés

La Confiance Numérique est une filière stratégique car :

- **Le potentiel de croissance** est durablement supérieur à celui de toutes les autres industries françaises ;
- La Confiance Numérique est déjà de **taille significative** ;
- Les acteurs français sont à la pointe en matière de **compétences et de R&D** ;
- Ce secteur est essentiel à la **souveraineté numérique nationale** et à **l'autonomie stratégique européenne ;**
- Le potentiel de croissance risque d'être sous-exploité en raison de la **forte concurrence internationale**, en particulier en provenance de la Chine et des États-Unis.

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

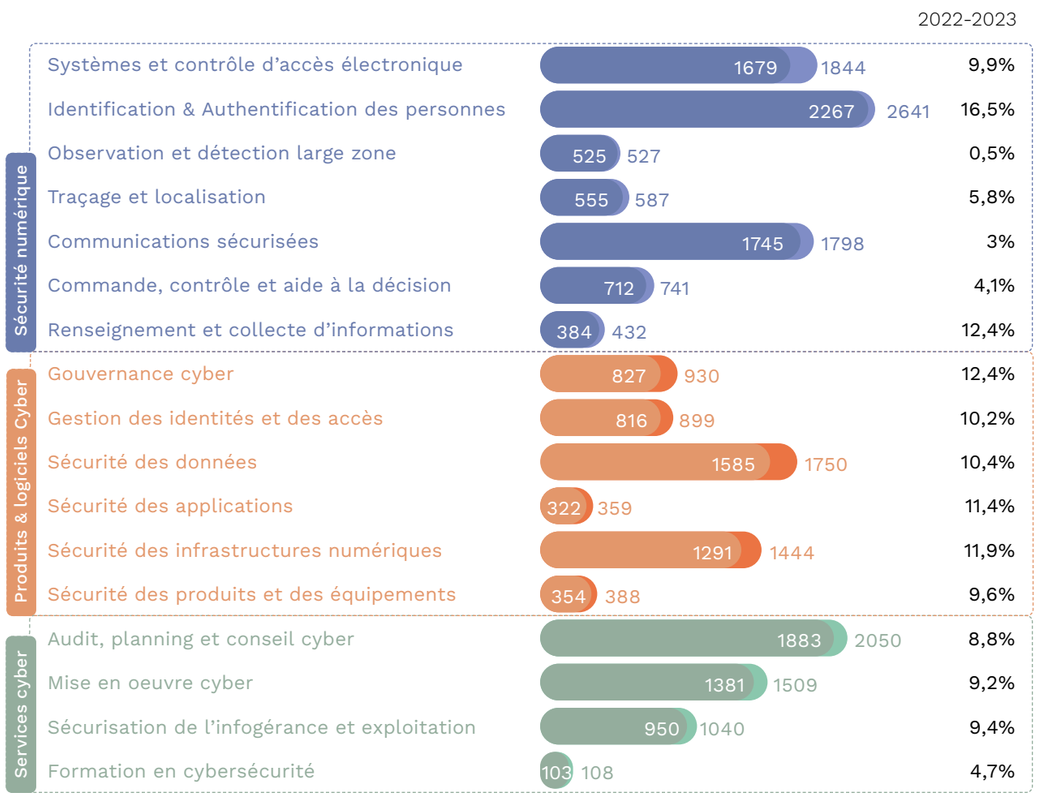
III

LES CHIFFRES CLÉS DE LA FILIÈRE

III. LES CHIFFRES CLÉS DE LA FILIÈRE

3.1 Taille et croissance

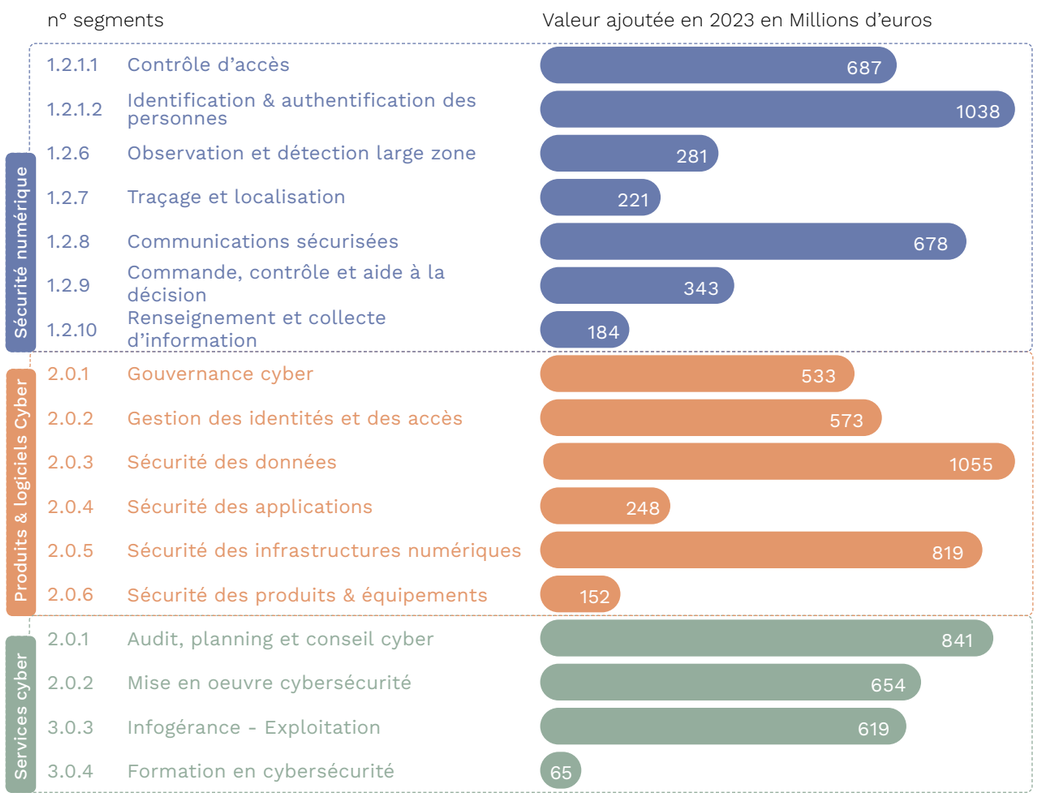
CA de la Confiance Numérique en France 19 Mds € en 2023



Sécurité Numérique	Poduits & logiciels Cyber	Services cyber	Total
+ 8,9%	+ 11,1%	+ 9%	+ 9,6%
8 570 Mds €	5 570 Mds €	4 706 Mds €	19 045 Mds €

3.2 Valeur ajoutée

Valeur ajoutée en France par segment

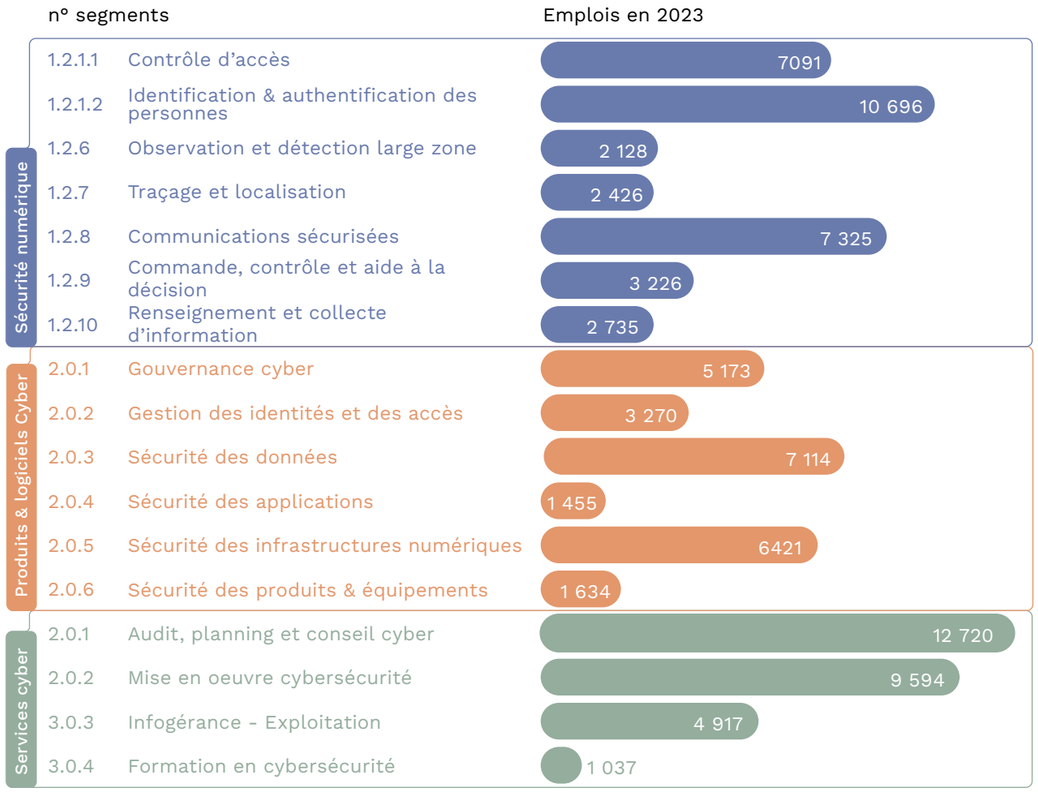


Sécurité Numérique	Poduits & logiciels Cyber	Services cyber	Total
3 432 M€	+ 3 380 M€	+ 2 178 M€	= 8 990 M€
			De VA de Confiance Numérique en France

Source : Decision Etudes & conseils

3.3 Emplois

Emplois en France en 2023 par segment

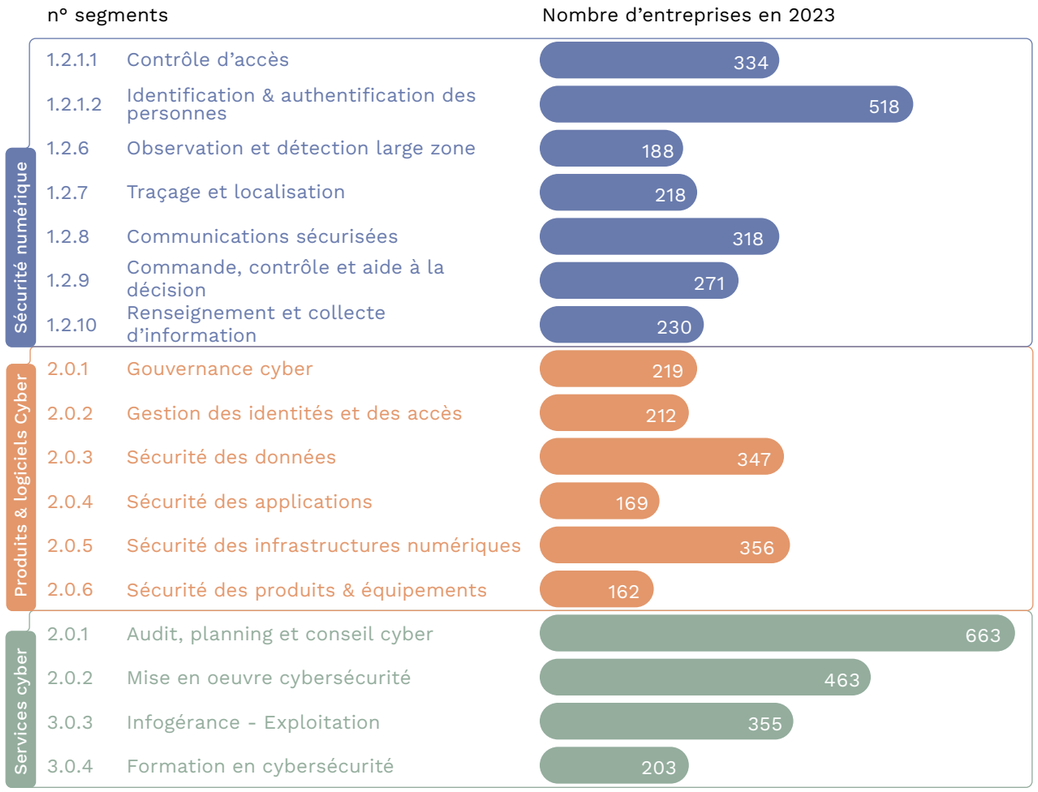


Sécurité Numérique	Poduits & logiciels Cyber	Services cyber	Total
35 627 emplois	+ 25 069 emplois	+ 28 268 emplois	= 88 964 Emplois de Confiance Numérique en France

Source : Decision Etudes & conseils

3.4 Nombre d'entreprises

Nombre d'entreprises en France en 2023 par segment



Sécurité Numérique	Poduits & logiciels Cyber	Services cyber	Total
1 775 entreprises	+ 726 entreprises	+ 704 entreprises	= 2 178 Entreprises de Confiance Numérique en France

Source : Decision Etudes & conseils

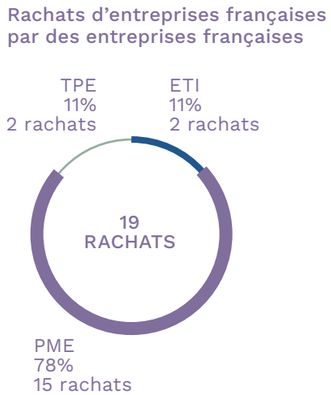
3.5 Les mouvements de fusion - acquisition

Bilan : Rachats d'entreprises sur la période 2022-2024

Au sein de la filière de la Confiance Numérique, 36 rachats d'entreprises concernant des sièges d'entreprises localisés en France ont été recensés de janvier 2022 à mars 2024 (soit en moyenne 16 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.

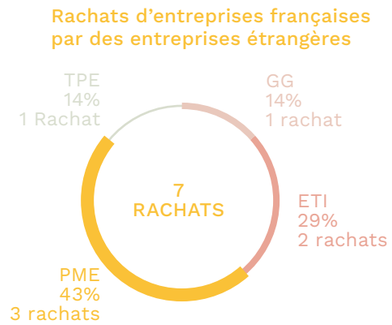
Parmi eux :

19 rachats d'entreprises françaises par d'autres entreprises françaises (53%)

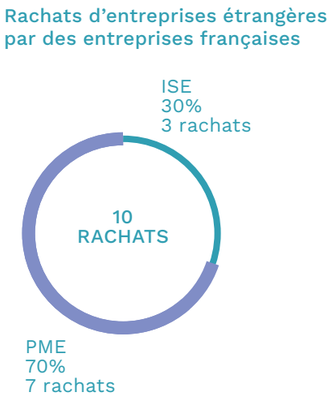


Source : Decision Etudes & conseils

7 rachats d'entreprises françaises par des entreprises étrangères (19%)



10 rachats d'entreprises étrangères par des entreprises françaises (28%)



La grande majorité des entreprises rachetées sont des PME (69%) en croissance.

Par rapport à la période 2017-2020, la fréquence de rachats est similaire, mais **la taille des entreprises rachetées est en moyenne relativement plus petite, avec un fort attrait pour les PME.**

En outre, sur la période 2017-2020, le nombre de rachats d'entreprises françaises par des capitaux étrangers était nettement supérieur au nombre de rachats d'entreprises étrangères par des entreprises de capitaux français, et pour des tailles d'entreprises achetées supérieures. **Cette tendance s'est estompée et même légèrement inversée depuis 2022, avec notamment le rachat de Imperva et Tesserent par Thales en 2023.**

En 2021, les deux-tiers des rachats d'entreprises françaises par des entreprises étrangères se sont opérés au profit de capitaux américains, dans la continuité de la période 2017-2020. Parmi ces rachats, on trouve notamment Link by net, Openminded et AFD.TECH, tous les trois rachetés par Accenture. Entre 2023 et mars 2024, les Etats-Unis restent les principaux acquéreurs étrangers d'entreprises françaises avec 3 rachats enregistrés: Brainwave GRC racheté par Radiant Logic, Proph3cy racheté par le fond Carlyle et enfin Vade racheté par Hornetsecurity (entreprise allemande à capitaux américains).

Enfin, les grands groupes français montrent leur intérêt pour le marché européen depuis 2022 en rachetant des entreprises dont le marché est généralement situé dans les pays frontaliers de la France.

A. Les principales acquisitions depuis 2023 par les leaders français

Thales étend ses activités dans le monde à travers deux acquisitions stratégiques

En 2023, Thales a renforcé sa position dans le domaine de la cybersécurité en réalisant plusieurs achats importants. L'entreprise a d'abord acquis Tesserent, une société australienne spécialisée dans la lutte contre les cyberattaques, pour 111 millions d'euros. Tesserent est reconnue pour son travail avec le secteur public et la défense en Australie et en Nouvelle-Zélande, et a rapporté environ 110 millions d'euros de revenus l'année dernière.

Le plus gros achat de Thales a été celui d'Imperva, une entreprise américaine experte en sécurité des données et des applications, pour 3,6 milliards de dollars. Cette acquisition est la cinquième en un peu plus d'un an pour Thales et suit les achats de S21sec, Excellium, et OneWelcome, signalant un effort majeur pour devenir un leader mondial en cybersécurité. Avec le rachat d'Imperva, Thales espère ajouter environ 500 millions d'euros à son chiffre d'affaires de cybersécurité en élargissant notamment ses activité sur le marché américain, visant un total de 2,4 milliards d'euros par an.

Airbus renforce ses activités cybersécurité avec l'acquisition de l'allemand Infodas

Fin mars 2024, Airbus fait l'acquisition d'Infodas, une entreprise allemande spécialisée en cybersécurité, marquant ainsi un renforcement significatif de son portefeuille cyber. Basée à Cologne, avec 250 employés et un chiffre d'affaires annuel de 50 millions d'euros, Infodas se distingue par ses solutions de sécurité avancées pour le secteur public, la défense et les infrastructures critiques. Cette acquisition, prévue pour être finalisée d'ici fin 2024, souligne l'engagement d'Airbus à se positionner comme leader dans la protection des systèmes critiques, surtout dans le contexte du développement du système de combat aérien du futur (SCAF).

Chapsvision continue sa stratégie de croissance externe agressive

ChapsVision poursuit activement sa stratégie de croissance externe pour devenir un leader européen dans le traitement souverain de la donnée massive et hétérogène. En s'appuyant sur des acquisitions clés, ChapsVision renforce son expertise et élargit son portefeuille de solutions. Après plusieurs acquisitions visant à développer son portefeuille cyber en 2022, le groupe développe ses compétences dans la cyber intelligence depuis 2023.

Parmi ces acquisitions, on note Geotrend, spécialiste de l'intelligence économique et stratégique, ACIC, expert belge du traitement vidéo par intelligence artificielle, renforçant les capacités de ChapsVision dans la vidéosurveillance intelligente, répondant aux besoins de sécurisation des entreprises et des administrations publiques, et enfin Owlint, une start-up spécialisée dans le renseignement d'origine sources ouvertes (OSINT). Ces acquisitions complètent l'offre de ChapsVision en intégrant des technologies avancées pour l'analyse de données du Web, renforçant la cybersécurité et l'intelligence économique. Ces acquisitions reflètent l'ambition de ChapsVision de créer un leader européen pour la cyber intelligence et la cybersécurité confirmant son engagement pour la souveraineté européenne de la donnée.

Docaposte consolide sa position de leader dans le marché de santé

Docaposte renforce sa position dans le secteur de la santé à travers des acquisitions stratégiques visant à compléter son offre de solutions et de services de confiance numérique. Docaposte fait notamment l'acquisition de Thiqa, spécialiste en services numériques de confiance et de sécurité, laquelle renforce l'offre de Docaposte en conseil, intégration et exploitation. En ajoutant Weliom, un cabinet de conseil expert en santé, Docaposte élargit ses compétences en stratégie numérique, sécurité des systèmes d'information et conformité. Enfin, Docaposte complémentent ces acquisitions liées à la sécurité avec les acquisitions de Maincare et Axonal-Biostatem, un éditeur de logiciels dans la santé et un leader en recherche et développement clinique. En combinant ces expertises avec les capacités de Docaposte en confiance numérique, cela permet de faire de Docaposte un leader technologique souverain pour la transformation digitale du secteur de la santé.

B. Les principaux rachat d'entreprises françaises par des capitaux étrangers

Les Etats-Unis restent les principaux acquéreurs d'entreprises françaises entre 2023 et aujourd'hui

Trois rachats par des capitaux américains ont été enregistrés sur cette période. Tout d'abord, Radiant Logic acquiert Brainwave GRC, un spécialiste français des données d'identité. Ce rachat leur permet de renforcer leurs capacités mutuelles en offrant une plateforme intégrée pour la gouvernance des données d'identité et l'analyse comportementale en temps quasi-réel, contribuant à une meilleure détection des cyberattaques et activités frauduleuses.

Ensuite, le fonds d'investissement américain Carlyle acquiert Pr0ph3cy, une start-up française de cybersécurité. L'investissement de près de 100 millions d'euros par Carlyle dans Pr0ph3cy vise à soutenir son expansion, notamment à travers des acquisitions. Proph3cy est renommé Neverhack après ce rachat.

Enfin, Hornetsecurity, une entreprise allemande avec une majorité de capitaux américains, a acquis Vade, un spécialiste français de la sécurisation des e-mails, portant un coup à la souveraineté française. Ce rachat permet à Hornetsecurity de renforcer son offre dans la protection des e-mails et d'étendre sa présence sur le marché français.

Cession des activités IoT de Thales auprès du tout nouveau Telit Cinterion

Au troisième trimestre 2022, Thales a conclu un accord pour céder son activité de produits IoT cellulaires, initialement acquise lors du rachat de Gemalto en 2019, à Telit, qui créera ainsi Telit Cinterion. Cette nouvelle entité a pour objectif de devenir un leader occidental des solutions IoT. Dans cette transaction, Thales reçoit une participation de 25% dans Telit Cinterion, désormais contrôlée par l'anglais DBAY Advisors. Cette cession permet à Thales de se concentrer davantage sur l'IoT industriel tout en conservant un intérêt stratégique dans Telit Cinterion.

Bechtle rachète Apixit et fait son entrée dans le marché français de la cybersécurité

Anciennement aux portes du top 50 des entreprises de la filière confiance numérique en France, Apixit, entreprise française de services de cybersécurité, se fait racheter par Bechtle, une importante société de services informatiques allemande. Ce rachat marque ainsi l'entrée de Bechtle dans le marché français de la cybersécurité et lui permet de renforcer son positionnement parmi les principaux acteurs IT en France.

3.6 Une année dynamique pour les levées de fonds

Signe de l'attractivité de la filière, les levées de fonds des startups de la Confiance Numérique ont continué de voir leur nombre et leur montant croître de manière exponentielle sur les six dernières années.

Comme l'illustre l'infographie ci-dessous, 41 levées de fonds ont été réalisées au sein de la filière en 2023, représentant un montant total de 456 millions d'euros. La période de janvier à mars 2024 témoigne d'une dynamique positive des levées de fonds, avec plus de 94 millions d'euros levés à travers 7 opérations, Zama se distinguant par une levée de 73 millions d'euros.

Pour la troisième année consécutive, la filière a bénéficié de deux levées de fonds aux montants exceptionnels en 2023 : 100 millions d'euros pour Ledger et 90 millions d'euros pour ChapsVision, deux entreprises ayant déjà reçu d'importants investissements les années précédentes.

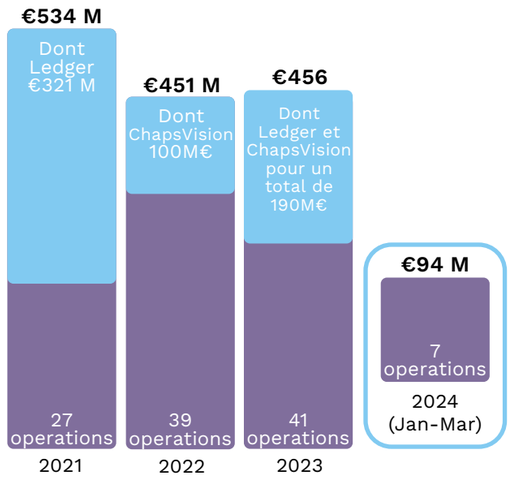
Sur un montant total de 456 millions d'euros, les membres de l'ACN ont représenté 36 % des investissements, soit 166 millions d'euros en 2023. Au premier trimestre 2024, sur un montant total de 94 millions d'euros investis, l'ACN a représenté 84 % des investissements, grâce aux opérations menées par Zama et Anozr Way.

En 2023, la grande majorité des entreprises ont été soutenues par des investisseurs français, parmi lesquels figurent des acteurs majeurs tels que Tikehau Ace Capital, Qualium Investissement, InfraVia Capital, la Banque des Territoires, Crédit Mutuel, 115K, etc.

Malgré un contexte économique difficile en 2023, moins propice aux investissements, la France a maintenu ses dynamiques antérieures, avec un nombre d'opérations toujours supérieur aux années précédentes et un montant total surpassant celui de 2022. La France conserve sa place sur le podium européen en matière de levées de fonds dans la filière de la Confiance Numérique : elle est en deuxième position en nombre de levées et en montants levés, et en troisième position en termes de montant moyen levé.

Cette position est d'autant plus significative pour la filière et pour la France, qui démontre une résilience remarquable. Selon le baromètre européen des investissements en cybersécurité de 2024 par Tikehau Ace Capital, les montants levés ont diminué en Europe, tous secteurs confondus, en raison d'un contexte économique et financier moins favorable. Bien que le nombre de levées de fonds ait augmenté, le montant total levé par le secteur européen de la cybersécurité a baissé de 42 % en 2023. Cette tendance à la baisse, à laquelle la France fait exception, est également observée aux États-Unis et en Israël.

Montant des levées de fonds des startups françaises de la Confiance Numérique



Liste des levées de fonds des startups françaises de la Confiance Numérique

En 2022

	Entreprise	Syndicat	Année	Montant (M€)
1	ChapsVision	ACN	2022	100
2	Mailinblack		2022	50
3	Tehtris	ACN	2022	44
4	Zama	ACN	2022	43
5	Vade		2022	28
6	Gatewatcher		2022	25
7	Trustpair		2022	20
8	Crowdsec	ACN	2022	14
9	DFNS		2022	12,3
10	Citalid	ACN	2022	12
11	Hackuity		2022	12
12	Stoïk	ACN	2022	11
13	Secure-IC		2022	10
14	Yogosha	ACN	2022	10
15	Bodyguard		2022	9
16	Dattak		2022	7
17	Cosmian		2022	4,2
18	Bfore.ai		2022	4
19	Stoïk	ACN	2022	3,8
20	Ocode		2022	3
21	Meelo		2022	3
22	Augmented Ciso		2022	2,5
23	ncScale		2022	2,5
24	C-risk		2022	2,5
25	Arsen		2022	2,5
26	Buster.ai		2022	2
27	Patrowl		2022	2
28	Snowpack		2022	2
29	Tenacy		2022	1,6
30	Equisign		2022	1,6
31	RFence		2022	1,3
32	Cryptr		2022	1,2
33	Kubo Labs		2022	1
34	Dastra		2022	1
35	Legapass		2022	1
36	Cyberjobs		2022	0,9
37	dappy		2022	0,5
38	Ravel		2022	
39	Eyst		2022	
	Total ACN			238

En 2023

	Entreprise	Syndicat	Année	Montant (M€)
1	Ledger		2023	100
2	ChapsVision	ACN	2023	90
3	DataDome		2023	38,6
4	sekoia.io	ACN	2023	35
5	Egerie		2023	30
6	HarfangLab		2023	25
7	Provenrun		2023	15
8	Dattak		2023	11
9	CryptoNext		2023	11
10	Sesame IT	ACN	2023	10
11	Stoïk	ACN	2023	10
12	Cybervadis		2023	7
13	Ecole 2600	ACN	2023	6
14	Filigran		2023	5
15	MiTrust		2023	5
16	Astran	ACN	2023	4,7
17	Qeviar AI		2023	4,5
18	NANOCORP	ACN	2023	4,2
19	CSB school		2023	4
20	VSORA		2023	4
21	OverSOC		2023	3,8
22	Escape		2023	3,6
23	Narval		2023	3,6
24	Zygon		2023	2,8
25	Dotfile		2023	2,5
26	Bastion Technologies	ACN	2023	2,5
27	elba		2023	2,5
28	ShareID	ACN	2023	2
29	Defants		2023	2
30	Alcyconie		2023	2
31	VeriQloud		2023	1,9
32	Qontrol	ACN	2023	1,5
33	Naaia		2023	1,3
34	Mithril Security		2023	1,2
35	BonjourCyber	ACN	2023	1
36	Legapass		2023	0,6
	Inspeere		2023	0,6
37	Escape		2023	0,5
38	OneWave		2023	0,4
39	Bastion Technologies	ACN	2023	
40	Kubo Labs		2023	
	Total ACN			167

3.7 L'émergence d'un fort écosystème de PME de Confiance Numérique

Comme le montre l'infographie ci-dessous, l'écosystème français de la Confiance Numérique s'est construit autour de **grands acteurs historiques,** souvent issus de la sécurité numérique et/ou des services numériques, et souvent liés aux écosystèmes régaliens et de défense. Ces grands acteurs historiques, fortement exportateurs, ont des offres orientées vers les états, les Opérateurs d'Importance Vitale (OIV), et les grandes entreprises internationales. Ils représentent 15,7 Mds € de chiffre d'affaires en 2023.

Cependant, **un écosystème de PME spécialisées dans la Confiance Numérique** a commencé à émerger à partir des années 1990. Au cours de la décennie des années 2010, cet écosystème a progressivement pris de l'importance et recense désormais de nombreuses grandes PME dont certaines ont déjà dépassé la barre des 50 M € de CA et sont devenues des Entreprises de Taille Intermédiaires (ETI), tournées vers l'international.

Cet écosystème est composé très majoritairement de startups de la cybersécurité dont beaucoup ont des offres visant à adresser de nouveaux marchés comme les PME/TPE ou encore les petites collectivités territoriales. La forte croissance de cet écosystème est portée par des levées de fonds pour des montants toujours plus importants d'années en années. Cet écosystème représente un chiffre d'affaires estimé entre 2,5 et 3 Mds € en 2023 (en additionnant les PME

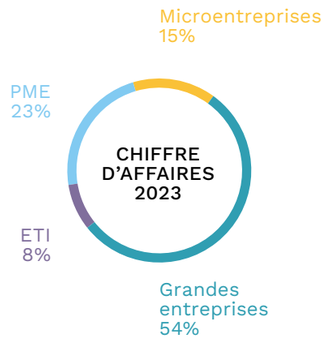
Emergence d'un fort écosystème de PME

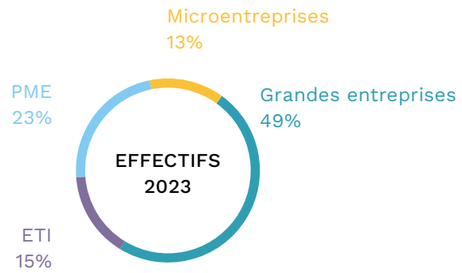
2,5 à 3Mds € en 2023

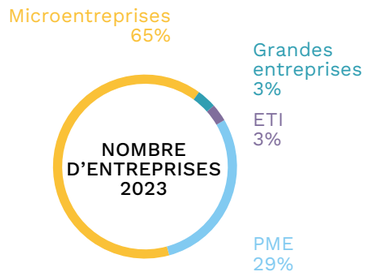
Grands Acteurs Historiques

15,7 Mds € en 2023

Analyse par taille d'entreprise







IV. POINT SUR LA MENACE INFORMATIQUE

4.1 La menace vue par l'ANSSI

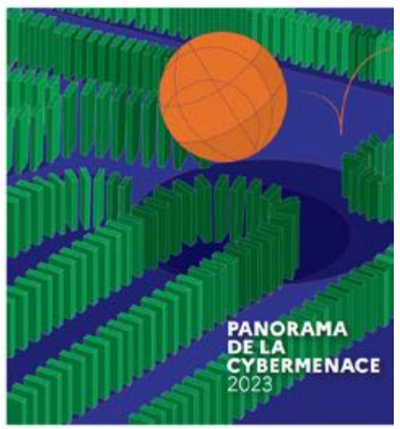
Dans son Panorama de la cybermenace 2023, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) revient sur les grandes tendances observées sur l'année 2022-2023 et en propose des perspectives d'évolution à court terme.

L'ANSSI a constaté une nouvelle fois une augmentation de la menace informatique, supérieure à l'année 2022, notamment l'espionnage informatique et les attaques par rançongiciels. L'une des raisons de cette évolution est le contexte géopolitique marqué par de fortes tensions et la tenue d'événements sur le sol français, tels que les Jeux Olympiques et Paralympiques 2024.

Evolution :
30% d'attaques par rançonlogiciels en 2023

2022 :
832 incidents avérés

2023 :
1112 incidents avérés



Document de Référence :
Panorama de la Cybermenace 2023
ANSSI – 27 février 2024

Document disponible ci-dessous :
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-001.pdf

1. Une augmentation notable de la menace cyber

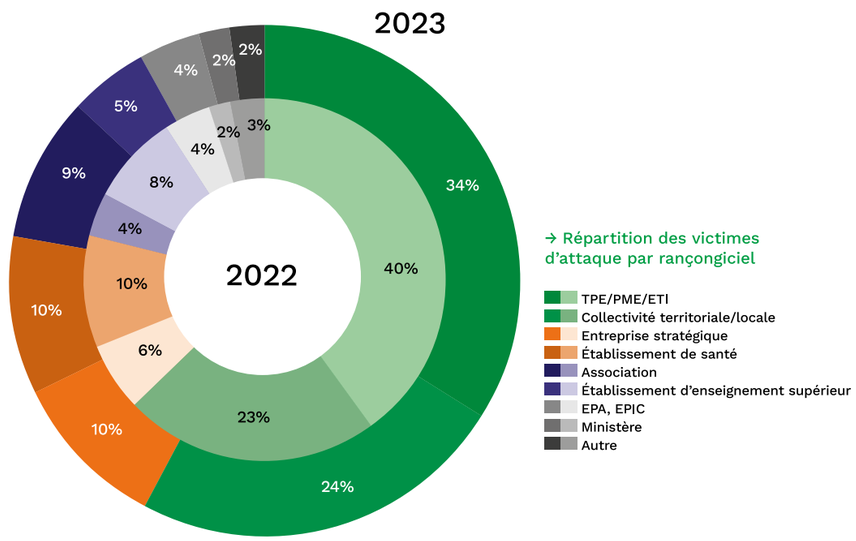
La cybermenace a connu un regain net en France par rapport à l'année 2022. L'espionnage informatique s'est maintenu à un niveau élevé au cours de l'année 2023 et les attaques touchent principalement des individus ainsi que des structures non-gouvernementales pouvant créer ou héberger des données sensibles.

L'ANSSI a relevé que l'espionnage via les téléphones portables professionnels et personnels, visant des individus ciblés, s'était accru. Il en va de même pour les attaques destinées à promouvoir un discours politique, à entraver l'accès à des contenus en ligne ou à porter atteinte à l'image d'une organisation.

L'espionnage stratégique et industriel est la menace qui demeure la plus préoccupante et qui a fortement mobilisé les équipes de l'agence. Le ciblage s'est focalisé sur des entités travaillant dans des domaines stratégiques, tels que des groupes de réflexion, des instituts de recherche ou qui assurent la transmission de données sensibles, comme la base industrielle et technologique de défense (BITD).

Les attaques par rançongiciels sur des organisations françaises ont représenté 30 % des attaques informatiques de l'année 2023. Dans le secteur de la santé et de l'énergie, dont les entités sont particulièrement sensibles aux interruptions de service, la cybercriminalité représente encore une menace importante. L'ANSSI a notamment apporté son soutien à une opération internationale visant à démanteler l'infrastructure du réseau cybercriminel QaKBot.

Le graphique ci-dessous montre l'évolution des cibles visées par rançongiciel dans le cadre des incidents traités par l'ANSSI en 2022 et en 2023, une hausse des attaques affectant le secteur associatif, les collectivités territoriales et locales a été constatée par l'ANSSI :



Source : ANSSI, 27 février 2024, «Panorama de la cybermenace 2023»

2. L'évolution constante des capacités offensives des acteurs malveillants

L'amélioration des techniques offensives des acteurs malveillants est constante. Leur objectif principal est de réduire le risque d'être détecté via des réseaux d'anonymisation toujours plus discrets et complexes. Les outils utilisés pour conduire une attaque sont toujours plus performants.

En parallèle, l'ANSSI constate que certains routeurs utilisés par des particuliers, des petites et moyennes entreprises (PME) ou de collectivités territoriales sont compromis puis intégrés à des réseaux d'anonymisation. Ces routeurs sont ensuite utilisés comme relais actifs de campagnes d'espionnage et plus largement de la cybercriminalité.

En outre, les équipements périphériques (routeurs, passerelles de messagerie, pare-feu…) sont toujours une vulnérabilité pour les systèmes informatiques en 2023. L'ANSSI a relevé que les techniques de *living-off-the-land* (exploitation d'applications et de fonctionnalités déjà présentes sur le réseau compromis) ont été particulièrement utilisées par les cybercriminels ce qui rend plus complexe la distinction entre les activités de l'attaquant et celles de la victime. L'ANSSI souligne que ces techniques ont été utilisées par des attaquants russes et chinois sur des infrastructures se trouvant aux Etats-Unis et en Ukraine.

Par ailleurs, le marché privé de la surveillance a connu un réel essor : certaines entreprises fournissent des codes malveillants à des acteurs publics, des entreprises ou encore des particuliers qui auraient l'intention de nuire. Afin de lutter contre la prolifération et l'utilisation abusive de logiciels espions commerciaux, la France a soutenu la Déclaration conjointe adoptée dans le cadre de la 2ème édition du Sommet pour la démocratie. De plus, lors du Forum de Paris pour la Paix en novembre 2023, le Royaume-Uni et la France ont réalisé des consultations pour combattre le développement de ces logiciels espions commerciaux.

3. Des opportunités d'attaque mieux sélectionnées

Les acteurs malveillants font désormais appel à des faiblesses plus précises afin de compromettre les systèmes informatiques visés. Les failles peuvent être à la fois techniques comme humaines : exposition d'équipements non sécurisés sur internet, mauvaises pratiques d'administration ou de gestion, vulnérabilités dans les systèmes, absence de durcissement… Ces failles constituent des brèches par lesquelles les attaquants s'engouffrent, les victimes de maitrisant difficilement leurs systèmes d'information.

L'ANSSI a traité de nombreux incidents de sécurité impliquant une exploitation de vulnérabilités au cours de l'année 2023, notamment avec l'utilisation de plusieurs vulnérabilités 0-day ou jour-un par des groupes cybercriminels. Les services de messagerie ont été particulièrement ciblés lors de cette année-là : elles permettent aux attaquants d'accéder à des données confidentielles d'entreprises ou de s'introduire dans le poste de travail de leurs cibles.

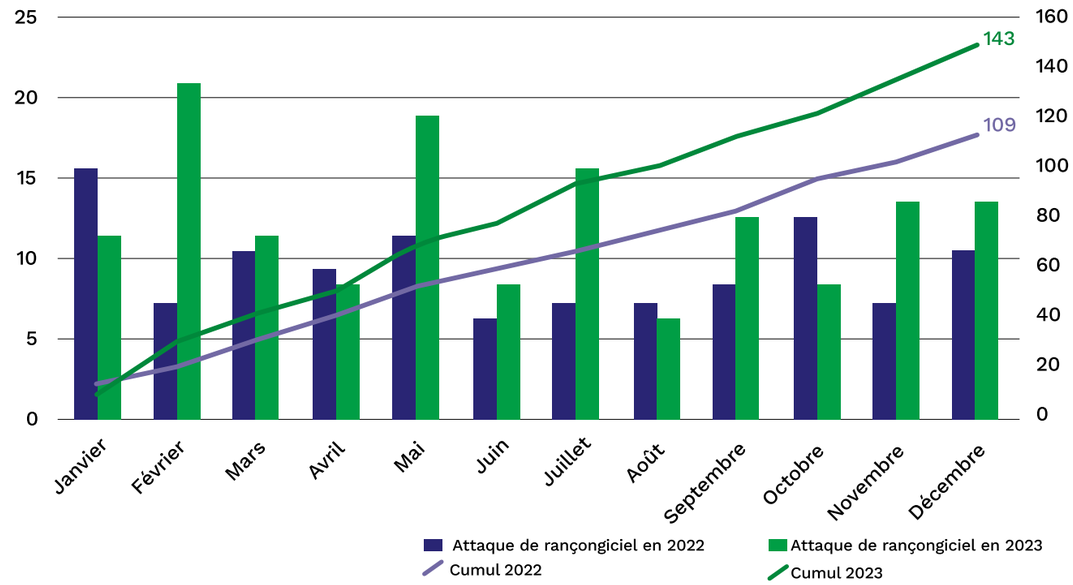
L'opportunité d'agir pour les attaquants se retrouve également dans l'organisation de grands événements. Dans leur mise en place, une multitude d'acteurs sont sollicités ce qui conduit à des niveaux de sécurité hétérogène. L'exploitation de la couverture médiatique de l'évènement, les organisateurs ou les participants peuvent représenter des cibles idéales. La coupe du monde de rugby organisée en France en 2023 a d'ailleurs, pu permettre au pays d'anticiper les potentielles attaques en vue des Jeux Olympiques et Paralympiques 2024.

Pour autant, une opération d'espionnage ou des attaques par déni de service distribués (DDoS) pourraient viser les Jeux Olympiques et Paralympiques 2024. Afin d'éviter cela, l'ANSSI sera fortement mobilisée concernant la cybersécurité de cet évènement. Un dispositif de détection, d'alerte et de traitement de sécurité informatique sera mis en place en coopération avec les différents services de l'Etat qui y sont impliqués.

Le climat international, toujours très tendu, est une occasion incitant les acteurs malveillants à s'introduire et à se maintenir sur des réseaux d'importance critique, tels que l'énergie, les transports ou la logistique. Les entités ukrainiennes demeurent l'une des cibles principales, mais des activités de pré-positionnement ont pu être détectées en Europe, en Amérique du Nord et en Asie.

Enfin, au cours de cette année, les évolutions dans la structure et les méthodes des attaquants, montre qu'on ne peut exclure la menace d'attaques à grande échelle. De ce fait, un suivi régulier des publications du CERT-FR sur les menaces et vulnérabilités, ainsi que l'entrée en vigueur de la directive NIS 2, permettront de renforcer et de garantir progressivement un bon niveau de cybersécurité.

Comparaison des signalements d'attaques par rançongiciels en 2022 et 2023 :



Source : ANSSI, 27 février 2024, «Panorama de la cybermenace 2023»

4.2 Regards croisés des experts du secteur

Le back-up est mort, vive la cyber résilience !

Yosra Jarraya
Co-Fondatrice et Directrice Générale

« Le ransomware, un fléau qui paralyse les entreprises, frappe désormais toutes les deux heures. La question n'est plus de savoir «si» une attaque surviendra, mais «quand» elle aboutira ! Face à cette menace, les Kits de Survie deviennent indispensables pour garantir la résilience de l'organisation. Ces kits complètent le plan de continuité d'activité classique (détection, le confinement, l'analyse, l'éradication et la restauration des backup) qui nécessite entre 22 et 90 jours pour être mené à bien. Durant cette période de crise, l'entreprise ne peut se permettre de simplement «attendre». Les données et services soigneusement sélectionnés de ces kits, continuellement disponibles, représentent le dernier rempart contre les impacts financiers destructeurs et la perte de confiance des clients. Le back-up est mort, vive la cyber résilience ! »

Contextualiser la menace pour anticiper et quantifier le risque cyber

Alexandre Dieulangard
Co-fondateur et Directeur général

« 2024 est le théâtre d'une conjonction d'évènements géopolitiques et d'activités cyberoffensives. Les hacktivistes exploitent les tensions internationales, comme en Ukraine et au Moyen-Orient, pour mener des actions peu sophistiquées mais médiatisées. Malgré le succès d'opérations internationales d'entrave, la cybercriminalité reste la principale menace pour les acteurs publics et privés. Discrètes, les actions étatiques demeurent une réalité, en attestent les récents rapports sur Sandworm, APT29 ou encore Volt Typhoon. Les JO seront un catalyseur pour des attaquants aux motivations variées. Dans ce contexte l'exploitation d'un outil de Cyber Risk Quantification (CRQ), alimenté en renseignement stratégique fiable, est indispensable pour faire face au risque cyber avec confiance et sérénité. »

Les rançongiciels se professionnalisent

Erwan Keraudy
CEO et Co-fondateur

« Les demandes de rançons sont en hausse de 40% à cause notamment du développement des RaaS. En 2023, grâce à sa capacité de détecter les menaces externes, CybelAngel a identifié 62 groupes de rançongiciels actifs impliqués dans plus de 5000 attaques connues et 132 pays. Les incidents liés aux rançongiciels ne sont pas suffisamment rapportés car de plus en plus d'entreprises choisissent de payer la rançon et d'assumer les risques associés plutôt que de s'attaquer au problème sous-jacent. Pourtant, identifier les vulnérabilités dès le départ peut réduire considérablement la menace. Les Ransomware-as-a-Service (RaaS) gagnent en popularité ; de plus en plus de données, de services du cloud et de bases de données sont exposés. Tout porte donc à croire que cette tendance va continuer de croître. »

La protection de tous, un enjeu fondamental

Gwenaëlle Martinet
Directrice de l'offre cyber

« Les plus grandes structures sont aujourd'hui pleinement conscientes des risques cyber et déploient des moyens pour s'en prémunir. Les plus petites d'entre elles, privées ou publiques, rencontrent de nombreuses difficultés : manque de ressources humaines et financières, complexité technique difficile à appréhender, foisonnement de solutions. Pourtant 20% des organisations ont déjà été victimes de cyberattaques. L'enjeu est donc de démocratiser l'accès à la cybersécurité. Docaposte, leader de la confiance numérique en France, accompagne les petites et moyennes entités, en intégrant dans un seul contrat tous les produits de cybersécurité nécessaires pour se préparer, se protéger et réagir. Docaposte permet ainsi à tous de faire face à la menace, simplement et efficacement. »

Renforcement des menaces sur les mobiles

Romain Waller
Directeur Général

« Nous faisons face à une augmentation des incidents de compromission de téléphone portables. De nouvelles techniques ciblent les mobiles avec une précision accrue, à des fins d'espionnage, de cybercriminalité ou de déstabilisation. En effet, un téléphone mobile contient en interne des informations, donne accès à un micro proche de l'utilisateur mais est aussi un vecteur d'attaque possible contre le SI d'une organisation, comme mentionné dans le Panorama de la Cybermenace en 2023 de l'ANSSI. Après l'épisode Pegasus, encore très récemment il a été découvert dans des téléphones mobiles de membres du Parlement européen des traces de logiciels de surveillance. Face à ces défis, il est impératif de mettre en place des mesures efficaces de protection et de détection pour une sécurité renforcée. »

Cloud, vers une souveraineté pragmatique et sécurisée !

Fanch Francis
CEO

« En 2023, l'autonomie numérique de l'UE est menacée par la domination des géants du cloud, avec AWS, Azure et GCP contrôlant plus de 70% du marché. Cette prédominance étrangère expose les entreprises européennes à des risques de conformité et de sécurité, entravant ainsi la souveraineté des données. NANO Corp. répond à ce défi en proposant un système de contrôle déployable sur tous les clouds y compris les hyperscalers américains, aligné sur les certifications de sécurité de l'UE, pour garantir l'intégrité et l'autonomie opérationnelle au sein du cloud. Alors que l'UE vise à accroître son adoption du cloud d'ici 2030, notre mission devient cruciale : permettre une transition sécurisée vers le cloud, renforçant ainsi la position stratégique de l'Europe dans l'échiquier numérique mondial. »

Une adoption croissante de l'authentification forte

Bruno Bernard
Président

« La sécurité des données numériques est essentielle face à la multiplication des cybermenaces. En 2022, plus de 51 types ont été gérés par la plateforme cybermalveillance.gouv.fr avec en tête l'hameçonnage ou *phishing*. Pour faire face à ce type d'attaques de plus en plus sophistiquées, la double authentification par SMS n'est plus suffisante. Pour une sécurité maximale, il est recommandé d'utiliser des moyens d'authentification forte tels que les dispositifs matériels FIDO. Ce standard est adopté par Microsoft, Google, Apple et plus de 250 autres fournisseurs de services et notamment les fédérations d'identité telles qu'Evidian, Ilex, Systancia, Octka, Ping Identity, ...»

L'essor de l'identité numérique : avancée pour les citoyens, mais aussi terrain propice aux fraudes

Frédéric Cercle
Gérant

« Le développement de l'identité numérique simplifie les démarches en ligne des citoyens, mais ouvre également la voie à de nouveaux risques et défis. En effet, la création d'un moyen d'identification électronique (MIE) repose sur un titre officiel d'identité. La vérification à distance de l'identité pour établir un MIE doit donc être robuste face aux attaques telles que les deepfakes et les injections vidéo. L'enthousiasme actuel et la croissance des technologies basées sur l'IA rendent accessibles aux fraudeurs des outils sophistiqués pour la création de deepfakes et d'identités synthétiques. Ces tentatives de fraude constituent un enjeu majeur à bien négocier pour garantir la crédibilité du marché de l'identité numérique, en attendant les améliorations promises par le règlement eIDAS 2... »

La conformité est-elle la clé pour réduire les risques de cybersécurité ?

Roland Atoui
CEO

« En 2023, une étude de Cybersecurity Ventures révèle qu'une cyberattaque a lieu toutes les 39 secs, totalisant plus de 2K cas par jour. En 2022, Statista comptabilise 12 millions d'attaques IoT, les secteurs des fabricants et financiers étant les plus touchés. L'Europe a également souffert, avec 4K+ incidents. Dans cet effort global et européen, des standards et régulations tels que l'ETSI EN 303 645, CEN-CENELEC, s'efforcent à assurer une harmonisation à l'état de l'art de sécurité nécessaire. En attendant, la sécurité repose sur les initiatives personnelles des fabricants et acheteurs des produits IoT. C'est dans cet esprit que CyberPass a été conçu, afin de soutenir ces démarches et simplifier la conformité. Face à ces défis, que faites-vous pour sécuriser notre avenir numérique ? »

La menace cybernétique

Audrey Amedro
CEO

« En 2024, la menace cybernétique se fait de plus en plus insidieuse et silencieuse. Ces attaques, souvent indétectables jusqu'à ce qu'il soit trop tard, exploitent les failles sécuritaires pour s'ancrer profondément dans l'infrastructure réseau. Face à ce type de cybermenace, l'adoption d'un système de détection sur le réseau (NDR) devient essentielle. JIZÔ NDR de Sesame*it surveille en continu des dizaines de réseaux IT et OT. Grâce à la combinaison d'un double niveau d'IA et de moteurs de détection avancés, il identifie les activités suspectes qui échappent souvent aux solutions de sécurité traditionnelles. Alors que les cyberattaques évoluent, la surveillance proactive du trafic réseau via un NDR devient une nécessité vitale pour protéger les actifs numériques. »

Les techniques de fraude à l'identité évoluent rapidement

Sara Sebti
CEO & Cofondatrice

« En 2024, les cybercriminels s'attaquent de plus en plus à l'identité numérique. Nous constatons une montée en puissance de l'utilisation de "deep fakes" et de techniques propulsées par l'intelligence artificielle pour usurper des identités et contourner les systèmes de sécurité traditionnels. Si ces menaces représentent un danger important pour la confiance numérique, elles peuvent aussi avoir un fort impact sur l'économie en ligne. Il est donc indispensable de mettre en place des solutions d'authentification robustes et d'innover constamment pour combattre les nouvelles techniques de fraude utilisées, même les plus sophistiquées. L'intelligence artificielle et l'utilisation de la biométrie jouent un rôle crucial dans ce combat. »

Quand un QR code ouvre la boîte de Pandore aux attaques cyber

Nathalie Launay
Consultant Senior Expert Identité Numérique au sein de Galitt

« Le COVID a accéléré l'adoption des QR codes pour interagir en proximité sans contact (commande à une table de restaurant...). Avec les smartphones, son usage se répand rapidement y compris en ligne. Mais ce code visuel devient le cheval de Troie pour frauder un paiement (QR code pour payer sa recharge électrique...), usurper les données d'authentification (Avis de réception de la Poste dans sa boîte aux lettres ou « quishing » par email), voire permettre l'installation de malware espion. Au-delà d'une App de confiance pour le scan, les nouveaux standards et wallets de paiement instantané ou d'identité numérique (EUDIW) nécessitent l'adoption de codes sécurisés interopérables, tels que le Cachet Electronique Visible développé en France, adopté par l'ANTS, et normalisé (Afnor et ISO). »

Mickaël Wajnglas
Secrétaire Général

L'augmentation des attaques hybrides

« La tendance est clairement à l'augmentation des attaques hybrides. Il s'agit pour un attaquant de réaliser dans un premier temps une intrusion physique au sein d'un bâtiment, pour ensuite atteindre plus facilement le cœur du SI et effectuer une cyberattaque. Il existe un grand nombre d'attaques hybrides différentes, notamment les attaques ciblant les périphériques matériels de sûreté installés en périmétrie comme les lecteurs de contrôle d'accès ou les caméras de vidéoprotection. L'UE a d'ailleurs parfaitement pris en compte ce nouvel enjeu avec la Directive NIS 2 qui associe pour la première fois, la sécurité physique à la cybersécurité. SPAC Alliance est fier de se tenir au côté de l'ACN pour apporter son expertise sûreté, et sensibiliser l'ensemble du marché à ces nouvelles menaces. »

Vincent Nguyen
Directeur cybersécurité

Nos prévisions 2024 : encore un peu plus près de la cyber-fin du monde ?

« En 2024, les attaques exploitant des failles connues et les chaînes d'approvisionnement, notamment les services Cloud, prédomineront. Les avancées en IA et IoT, bien que non disruptives actuellement, exigent une surveillance accrue. La sécurité sera cruciale durant les Jeux de Paris 2024. NIS 2 révolutionne la conformité en imposant des normes de sécurité strictes à de nombreuses organisations. L'assurance cyber devient essentielle, offrant protection financière et conformité réglementaire. Les organisations doivent améliorer leurs défenses, affiner leur réponse aux incidents et vérifier la pertinence de leur couverture d'assurance. En 2024, anticiper les menaces et s'adapter rapidement sera vital pour naviguer dans un environnement cyber complexe et risqué. »

Yannick Ragonneau
Directeur associé

La résurgence des attaques cyber

« L'approche des JO2024 suscite une inquiétude grandissante quant à la résurgence des attaques cyber. Avec une augmentation exponentielle de la surface d'attaque et une multiplication des cibles, aucun secteur n'est épargné. Les attaques classiques sont revisitées grâce à l'IA, à l'image des arnaques au président qui profitent déjà de la sophistication des deepfakes. Face à cette menace, il devient urgent et stratégique de changer de paradigme et de passer d'une approche réactive à une approche proactive « résiliente ». L'organisation des JO2024 doit être vu comme une opportunité de transformation de nos services technologiques pour apprendre à réagir et à résister aux tensions géopolitiques, aux cyberattaques et aux changements induits par l'accélération digitale. »

Patrick Bas
Chercheur au CNRS

Teddy Furon
Chercheur à l'INRIA

Sur la nécessité de légiférer vis à vis de la conception de générateurs de contenus par IA

« Les générateurs par IA proposent des contenus de plus en plus réalistes. Les méthodes d'analyse forensique passives n'apportent qu'une solution temporaire compte tenu de la nécessité de mettre à jour les détecteurs et de la difficulté potentielle de la tâche. Une protection active consiste à utiliser un système de tatouage pour modifier les contenus de manière imperceptible tout en insérant une marque permettant de prouver que le contenu est généré. Le déploiement de ce type de méthode n'est possible que s'il existe une législation obligeant les fournisseurs de générateurs à intégrer une solution de tatouage. Il faut également que la solution soit robuste à des traitements usuels et à des attaques adverses. La communauté scientifique française est bien positionnée pour répondre à ce défi. »

Focus - SPAC

TENDANCE MARCHÉ : AUGMENTATION DES ATTAQUES HYBRIDES

Mickaël Wajnglas
Secrétaire Général SPAC Alliance

“L’augmentation des cyberattaques n’est pas une nouveauté. C’est une tendance observée depuis de nombreuses années.
Ce qui est assez nouveau, c’est la tendance à l’augmentation des attaques hybrides.

1. Qu’est-ce qu’une attaque hybride ?
L’objectif d’une cyberattaque et d’une attaque hybride est le même – s’attaquer ou s’introduire dans le système d’information (SI) à des fins malveillantes. Alors qu’une cyberattaque se réalise plutôt de manière déportée, à distance, en utilisant des failles du SI, une attaque hybride utilise des biais physiques. En clair, dans le cadre d’une attaque hybride, un attaquant va, dans un premier temps, réaliser une intrusion physique au sein d’un bâtiment, pour atteindre plus facilement, dans un second temps, le cœur du SI et finaliser sa cyberattaque.

Notons que le procédé inverse existe également. Il s’agit alors d’effectuer une cyberattaque en amont, afin de s’introduire dans le SI et en prendre le contrôle, pour faciliter ensuite une intrusion physique.

2. Les différents types d’attaques hybrides ?
Il existe deux familles principales d’attaques hybrides : celles qui exploitent le facteur humain, et celles qui exploitent les failles de sécurité et de cybersécurité de l’écosystème des périphériques connectés.

Dans une attaque exploitant le facteur humain, l’objectif de l’attaquant est de s’introduire par tous les moyens possibles au sein de l’infrastructure d’une organisation, en soudoyant ou en leurrant, par exemple le personnel de sécurité à l’entrée du bâtiment.

Dans le cas d’une attaque à la clé USB, l’attaquant ne va pas essayer de pénétrer lui-même dans le bâtiment, il va utiliser la curiosité et la crédulité potentielle d’un personnel peu sensibilisé aux enjeux de cybersécurité. Le procédé peut par exemple consister à laisser une ou plusieurs clés USB comportant un malware sur le parking d’une entreprise. Cette clé sera ensuite récupérée par un employé, qui se chargera d’introduire physiquement ce périphérique corrompu au sein du bâtiment et de le connecter sur son ordinateur, lui-même connecté au réseau.

Le ver Stuxnet qui a déstabilisé le programme nucléaire iranien est un parfait exemple de ce type d’attaque.

Il existe également bon nombre d’exemples d’attaques ciblant les équipements de sécurité périmétrique ou IoT, comme la connexion à une caméra sur réseau IP non sécurisé.

Concernant le contrôle d’accès, si le lecteur ou le protocole de communication ne propose pas les plus hauts niveaux de sécurité, il existe un risque qu’un attaquant effectue une substitution de lecteur afin de récupérer les secrets (clés de chiffrement). Des attaques par rejeu sont également possibles si le protocole de communication entre le lecteur d’accès et le SI ne propose pas les plus hauts niveaux de sécurité. Un attaquant pourrait écouter/intercepter les communications.

Il faut savoir aussi qu’environ 70% du parc de badges d’accès intègre encore aujourd’hui des technologies obsolètes. Un attaquant peut donc très facilement et très rapidement cloner un badge d’accès d’un employé pour pénétrer au sein du bâtiment et accéder ensuite au réseau.

3. Les conséquences d’une attaque hybride
« Quand vous perdez le contrôle d’un lieu, vous devez supposer que tout est compromis » : cette citation de l’agence fédérale américaine, NIST, prononcée à la suite de l’assaut du Capitole, résume parfaitement les impacts que peut avoir une attaque hybride sur une organisation.

Nous savons tous que des centaines de personnes ont investi le Capitole en 2021 dans un but à l’origine insurrectionnel. Cette attaque a donné lieu à de nombreux actes de vandalisme et de saccage. En revanche, ce que l’on sait un peu moins, c’est que de nombreux équipements informatiques, contenant des secrets, des informations critiques et des données d’accès, ont été dérobés.

Il est fort probable qu’il n’y ait pas eu que de simples partisans mécontents du résultat de l’élection présidentielle américaine qui aient participé à cet assaut. Il y a de fortes chances que de nombreux périphériques informatiques restés sur place aient également été infectés. Il est aisé d’imaginer les conséquences et l’impact que cet évènement a eu sur le pays en termes de cybersécurité et de sécurité nationale.

Nous savons aujourd’hui qu’à la suite de cet évènement, une augmentation des tentatives d’intrusion sur les réseaux des administrations américaines a été identifiée.
Etant donnée l’ampleur de cette attaque hybride, le processus de réponse à incident mis en place a été beaucoup plus complexe que si le Capitole avait été confronté à une cyberattaque dite « classique ».

Aujourd’hui encore, tout risque cyber lié à cette attaque hybride n’est pas à écarter à 100%...

4. Cybersécurité et sécurité physique, changement de paradigme européen
L’évolution des menaces, notamment l’augmentation des attaques hybrides, nous oblige désormais à considérer la cybersécurité comme intimement liée à la sécurité physique. Une organisation peut être dotée des plus hauts niveaux de protection cyber, si la porte d’entrée du bâtiment reste ouverte, le système d’information sera encore plus exposé.

L’Union Européenne a parfaitement intégré ce nouvel enjeu : la Directive NIS 2 qui rentrera en vigueur en octobre 2024, fait pour la première fois un lien clair et explicite entre la cybersécurité et la sûreté. La sécurité physique et logique vont désormais de pair.

5. Contre-mesures
L’enjeu pour protéger l’ensemble des solutions de sécurité physique est de taille.
D’une part, parce que la sécurité physique est aujourd’hui considérée comme le premier rempart contre l’accès non autorisé au SI d’une organisation.
D’autre part, parce que ces périphériques de sécurité sont en général, par leur application métier, installés en périmétrie des bâtiments, c’est-à-dire en zone non sécurisée.

En outre, le déploiement des périphériques IoT est en forte augmentation, grâce notamment à l’essor du Smart Building. Même si ces objets connectés sont généralement installés en zone sécurisée (à l’intérieur du bâtiment), ils sont en grande majorité très peu sécurisés. Ce qui augmente d’autant plus la surface d’attaque du bâtiment.
D’où l’intérêt d’intégrer des technologies et des protocoles européens souverains, standards et dotés des plus hauts niveaux de sécurité comme SSCP®.

Ce protocole de communication historiquement conçu pour le contrôle d’accès est le seul à avoir été certifié CSPN par l’ANSSI, et c’est aujourd’hui le protocole le plus intégré dans les solutions de contrôle d’accès certifiées du marché.
Ce protocole a été ouvert en 2020 à travers SPAC Alliance pour devenir le seul standard industriel européen permettant aux périphériques de contrôle d’accès de communiquer avec le SI.

Sa standardisation a également permis d’ouvrir ce protocole à d’autres écosystèmes de sécurité comme celui de l’intrusion ou de la vidéoprotection. L’objectif étant, encore une fois, de proposer les plus hauts niveaux de sécurité, mais également et surtout des niveaux de sécurité homogènes au sein de tout l’écosystème de sécurité physique.”

V

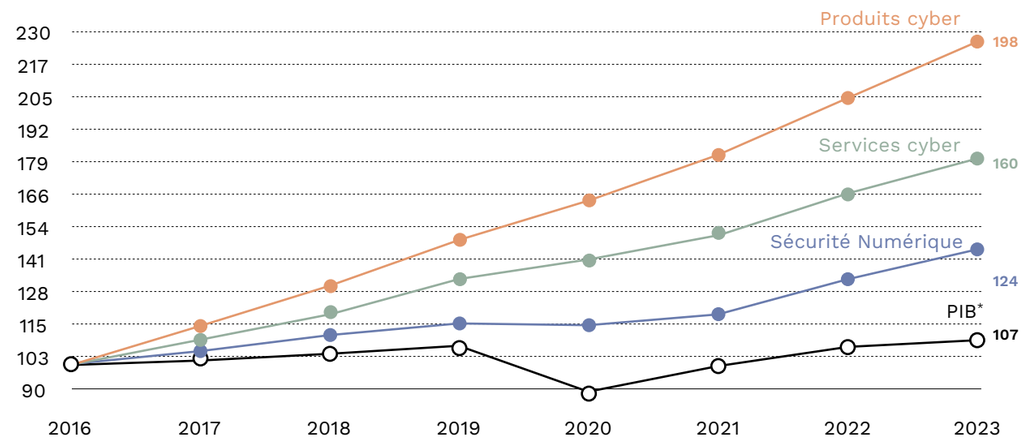
LES TENDANCES DE MARCHÉ

V. LES TENDANCES DE MARCHÉ

5.1 Les tendances générales

Le graphique ci-dessous montre l'évolution comparée de la croissance des trois principaux segments de la filière Confiance Numérique et du PIB sur la période 2017-2023.

Croissance France comparée 2017-2023



Croissance

Segments	2018	2019	2020	2021	2022	2023
Confiance numérique	**8,2 %**	**8,5 %**	**3,6 %**	**7,3 %**	**11,3 %**	**9,6 %**
Produits cyber	13,9 %	14,0 %	10,9 %	8,8 %	12,6 %	11,1 %
Services cyber	9,9 %	10,3 %	5,8 %	8,9 %	10,3 %	8,6 %
Sécurité Numérique	4,7 %	4,8 %	-1,7 %	5,2 %	11 %	8,9 %
PIB*	1,9 %	1,8 %	-7,8 %	6,8 %	2,5 %	0,9 %

Source : INSEE

5.1.a. La croissance de la filière française

Une croissance particulièrement forte en 2022 qui se poursuit en 2023

L'année 2022 a été marquée par une croissance particulièrement forte. La cybersécurité réalise une bonne année avec 11,5%, qui renoue avec la tendance des années 2014-2019. Cependant, la sécurité numérique réalise elle une année exceptionnelle avec une croissance de 11%. Cette croissance est notamment portée par les leaders Thales, Airbus (au niveau mondial), IN Groupe et IDEMIA à travers des projets liés aux contrôle d'accès et à l'identification. C'est le cas par exemple de IDEMIA à travers plusieurs partenariats lancés depuis 2021 (système central contrôle aux frontières en partenariat avec le ministère de l'Intérieur, renforcement de son système d'identification multi-biométrique avec INTERPOL, contribution au programme France Identité Numérique et au «service de garantie de l'identité numérique » avec l'Agence nationale des titres sécurisés). Mais cette croissance dans la sécurité numérique a également été soutenu par une hausse des exportations notamment à destination de l'Europe, mais aussi dans le monde.

En parallèle d'autres facteurs explicatifs subsistent:

■ Un effet rebond suite à la période de récession associée à la crise du COVID (près de -2% en 2020, certains grands acteurs ayant connu une récession jusqu'en 2021).

■ La répercussion de la hausse des prix des semi-conducteurs suite à la pénurie mondiale, induisant une croissance en valeur. Cela est particulièrement vrai pour le segment de l'identification et authentification des personnes (cartes à puces, etc.) et pour le segment cyber de la sécurité des équipements (éléments sécurisés, HSM), mais ce phénomène s'étend à l'ensemble de la sécurité numérique.

■ Enfin, une conjoncture favorable induisant une croissance en volume : importance croissante de l'enjeu du contrôle aux frontière avec des projets publics qui se multiplient, augmentation de la demande sécuritaire des états européens en lien avec la guerre en Ukraine, sécurisation des grands évènements (Coupe du monde de rugby en France en 2023, JO de Paris en 2024...).

Bien que moins exceptionnelle que 2022, **2023 reste une année synonyme de forte croissance pour la confiance numérique, avec un croissance à 9,6% globalement, soit 8,9% dans la sécurité numérique et 10.1% dans la cybersécurité.**

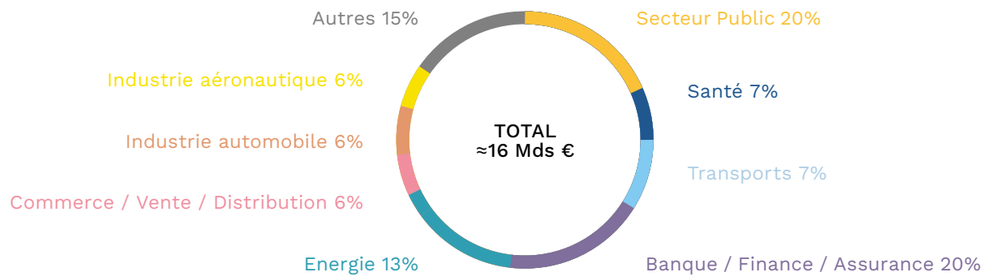
Les leaders de la filière continuent leur croissance: Thales et Airbus enregistrent des croissances moins élevées, entre 2 et 5% de variation organique dans leurs activités confiance numérique, tandis que Idemia et IN Groupe eux se maintiennent sur leur lancée avec des croissances à deux chiffres sur leurs activités confiance numérique. La cybersécurité poursuit également ses tendances passées avec les leaders tels que Docaposte et Sopra Steria (ce dernier étant par exemple impliqué avec IDEMIA dans le projet FAED V3 de modernisation du système de gestion des empreintes digitales) qui enregistrent des croissances entre 10 et 15% sur l'année 2023.

5.1.b. Les marchés de la filière en 2023

Comme le montre le diagramme, le **secteur public au sens large**, c'est-à-dire en incluant les transports et la santé **représente un tiers du marché français** (6 Mds € en 2023), les deux tiers restants provenant du secteur privé (11-12 Mds €).

Le poids du secteur privé est appelé à croitre d'année en année. La filière de la Confiance Numérique est en effet née autour de l'Etat et du besoin de sécurisation des Opérateurs d'Importance Vitale (OIV). Le besoin de confiance s'est ensuite étendu aux grandes entreprises en général, au-delà des OIV. La tendance actuelle est désormais au développement du marché des PME et TPE, qui sont pour la plupart démunies face au risque de cyberattaques qui les concerne désormais, en particulier le risque de subir un rançongiciel.

Principaux marchés de la filière en 2023



Source: DECISION Etudes & Conseil, questionnaire renseigné par les entreprises de la filière en de 2022 à 2024.

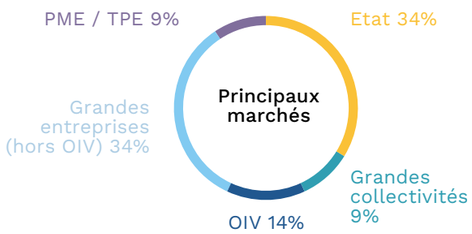
Pour l'année 2023, le secteur public continue cependant d'être indiqué comme l'un des premiers moteurs de la croissance par les entreprises de la filière ayant répondu à notre questionnaire, au côté du secteur Banque / Finance / Assurance et du secteur de l'énergie.

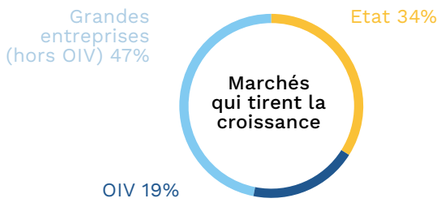
L'émergence d'un marché des PME/TPE et des petites collectivités territoriales

La série de diagrammes ci-contre, issue de l'édition 2024 du questionnaire en ligne auprès des acteurs de la filière, montre la segmentation du marché français de la filière selon le type d'entreprise fournisseur de solutions de confiance (grande entreprise versus TPE / PME).

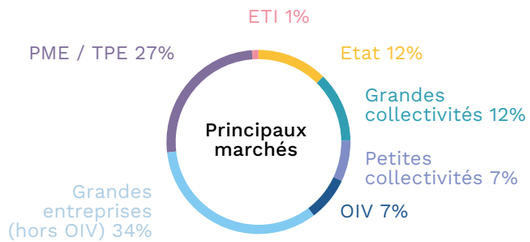
On observe que l'Etat, les Opérateurs d'Importance Vitale (OIV) et les grandes entreprises (hors OIV) représentent plus de 80% du marché des grandes entreprises de la filière, et près de 100% de leurs perspectives de croissance pour les années à venir. Ces grandes entreprises fournisseurs de solutions de confiance représentent 54% du chiffre d'affaires de la filière en France en 2023 (72% si l'on inclut les activités réalisées hors de France). On retrouve donc ici les grands marchés traditionnels autours desquels la filière s'est construite : Etat, OIV et grands comptes privés.

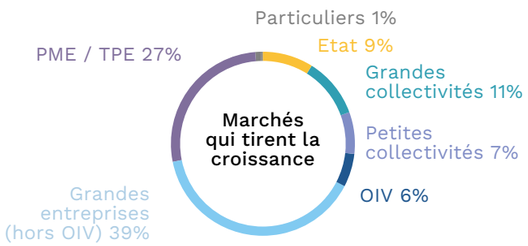
Grandes entreprises





TPE / PME





A contrario, l'Etat et les OIV ne représentent que 20% du marché des PME et TPE de la filière. Ce sont les grandes entreprises (33%), les PME / TPE (26%) et les collectivités locales (20%) qui représentent l'essentiel du marché et des perspectives de croissance pour les PME et TPE fournisseurs de solutions de confiance en France. Autrement dit, à travers cette vision des PME et TPE de la filière, on observe l'émergence de deux marchés :

- **Celui des collectivités locales,** y compris les petites collectivités locales. Par extrapolation, on peut estimer le marché des petites collectivités locales entre 1 et 1,5 milliard d'euros en 2023.

- Mais surtout, **le développement du marché associé au besoin de produits et services de confiance de la part des PME et TPE françaises.** Par extrapolation, on peut estimer ce marché entre 2,6 et 3,6 milliards d'euros en 2023. Ce marché se caractérise par des offres dédiées : offre standardisée, déploiement rapide, faible coût, souvent sans support *hardware*…

Le développement de ce marché des PME et TPE françaises a été ralenti en 2020 par la crise du COVID. En effet, les PME et TPE françaises ont été plus affectées par les restrictions associées au COVID que les grands clients traditionnels de la filière de la Confiance Numérique (Etat, OIV, grandes entreprises) qui sont quant à eux particulièrement centrés sur la fourniture de besoins essentiels (Banque / Finance / Assurance, Energie, Santé…).

Cependant, la tendance structurelle est bien au développement de ce marché des PME et TPE qui est voué à devenir l'un des grands marchés de la filière et va sous-tendre sa croissance pour les années à venir.

5.1.c Un manque de main d'œuvre important qui peut être pallié

L'écart entre les besoins en main-d'œuvre et le nombre de professionnels disponibles se creuse de plus en plus, et ce malgré une augmentation du nombre de personnes formées en cybersécurité. Face à une menace croissante et un paysage technologique en rapide évolution, le secteur a été confronté à des réductions de budget dues à la conjoncture économique. Or, la sécurité des systèmes d'information est de plus en plus menacée durant ces périodes d'incertitude économique.

Dans son enquête 2023 sur les métiers de la cybersécurité, l'ANSSI propose trois axes principaux pour combattre le manque de talents dans la cybersécurité:

- Travailler sur l'image du secteur de la cybersécurité pour la rendre plus attrayante. L'ANSSI pointe du doigt une méconnaissance des réalités du métier parmi les étudiants, et propose de démystifier le secteur tout en promouvant une éducation renforcée aux usages numériques dès le jeune âge. Cela inclut de diversifier les représentations du secteur pour attirer un plus large éventail de talents et de développer une culture de la cybersécurité dans la société.

- Démocratiser l'accès aux carrières en cybersécurité en diversifiant les profils et les parcours. Le rapport critique une image élitiste et très technique du secteur qui dissuade de nombreux potentiels candidats. Pour cela, il est suggéré d'élargir les profils recrutés, de valoriser les reconversions professionnelles et les compétences non traditionnelles, et de clarifier les parcours de formation et les possibilités d'évolution professionnelle.

- Améliorer les conditions de travail dans le secteur de la cybersécurité. Le rapport constate que seulement 63% des professionnels se sentent valorisés socialement dans leur métier, et que dans le secteur privé notamment, il faut développer une culture cyber pour faire de la cybersécurité un enjeu stratégique reconnu par tous. Cela passe aussi par une meilleure rémunération et des contrats plus attractifs pour retenir les talents dans un domaine où les compétences sont rares et précieuses.

L'ANSSI a publié en mars 2023 une enquête sur l'attractivité de la filière cybersécurité

Enquête 2023
« L'attractivité et la représentation des métiers de la cybersécurité »

Focus - Ecole 2600

L'APPROCHE « *SKILLS FIRST* » POUR MONTER EN COMPÉTENCES ET RÉPONDRE À LA PÉNURIE DE MAIN D'OEUVRE DANS LA FILIÈRE

Valérie Poulain de Saint-Père
Présidente et co-fondatrice de l'Ecole 2600

"2023 a été une année sombre en matière de cybersécurité : si le nombre de cyberattaques réussies reste stable, il n'en concerne pas moins, selon le baromètre du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) près de la moitié des entreprises françaises a été attaqué. Les chiffres récemment publiés par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) le confirment : les actes de cybercriminalité dans notre pays ont augmenté de 400% entre 2020 et 2023 ! Non seulement la menace reste omniprésente, mais elle se signale par une dangereuse capacité à se réinventer.

Dans ce contexte préoccupant de guerre numérique et de professionnalisation des cybercriminels, et alors que 68% des dirigeants d'entreprises font de la protection contre les cybermenaces leur priorité majeure pour 2024, selon un sondage du cabinet BDO, charge aux acteurs de la formation en cybersécurité eux-mêmes d'endosser cette capacité à se réinventer : tout en accélérant massivement la formation, pour former plus d'experts en cybercriminalité, il est impératif de changer de paradigme pour les former mieux.

Nous sommes convaincus que l'approche "skills first" facilitera l'émergence des "nouveaux cols", à l'image des initiatives d'IBM projet P-Tech). Cette nouvelle culture, axée sur les compétences, permettrait une meilleure mobilité interne, une réduction du taux d'attrition des collaborateurs mais surtout une culture qui privilégie la compétence au seul diplôme. Ceci permettrait de pourvoir les postes vacants, développer des talents souvent négligés et favoriser la diversité socio-économique.

Ce changement de paradigme a vocation à se concrétiser dans un nouveau modèle d'évaluation. Plus adapté aux besoins concrets des entreprises, il substituerait à l'hyper valorisation actuelle des diplômes génériques l'hy personnalisation d'une formation continue, à travers la certification de micro-compétences en cybersécurité. C'est toute la vocation de la plateforme de formation « tout au long de la vie » que nous avons déployée au sein de l'École 2600.

Nous sommes partis d'un postulat très simple : pour garantir le meilleur niveau de performance des

experts face aux évolutions technologiques dont bénéficient les cybercriminels (machine learning, intelligence artificielle générative, algorithmes quantiques...), leurs compétences doivent être très régulièrement réévaluées et mises à jour. Elles doivent aussi correspondre à des modules spécifiques, de manière à obtenir le niveau de granularité le plus fin possible.
Faire émerger ce nouveau modèle de formation continue axé sur la micro-certification, c'est ce qui nous permettra de constituer un vivier d'experts à l'agilité, à la capacité d'adaptation et à la rapidité maximales, au plus près des entreprises et des institutions. Nombre d'entre elles ne sont pas encore en mesure d'évaluer les compétences de leurs collaborateurs, et par là même les risques et les compétences à développer pour les anticiper. Alors que le marché français de la cybersécurité est pénurique, avec 15 000 postes vacants contre 37 000 emplois nécessaires d'ici à 2035, ce nouveau modèle de formation permettra également d'up-skiller et/ou re-skiller les collaborateurs d'une entreprise, afin de garantir la continuité de l'expertise cyber en son sein.
En ce sens, pour assurer toute l'efficacité de notre plateforme, il nous a paru essentiel de l'adosser à une approche pragmatique à deux entrées.

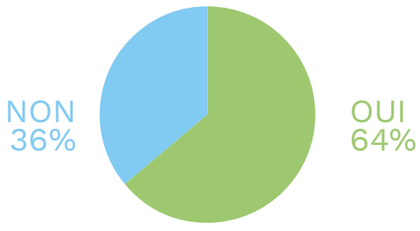
Tout d'abord, pour faire face à une menace globale, il faut avoir une approche globale. C'est pourquoi la plateforme s'aligne sur les orientations stratégiques de l'Union européenne concernant le développement d'un référentiel de compétences européen. Nous avons créé des fiches de poste par métiers avec des compétences qui regroupent les référentiels de l'ENISA mais aussi le NICE du NIST et celui de l'ANSSI, en complément de notre propre référentiel.
Enfin, afin d'assurer le lien le plus fin entre les formations proposées et les besoins réels des entreprises, il est impératif de cartographier ces derniers. C'est tout le sens de l'outil de collecte et d'extraction des compétences et de cartographie des stack techniques que nous avons mis en place, pour suivre en temps réel l'état des besoins en compétences dans le monde entier par rapport aux offres de poste publiées.
Face à tous ces enjeux majeurs et à la menace grandissante des cyberattaques, l'École 2600 continuera à défendre un modèle de formation en cybersécurité pertinent et puissant, apte à participer au besoin impérieux d'une cyberdéfense nationale souveraine et solide, dans l'intérêt de nos entreprises et de notre pays."

Zoom - Transition écologique dans la filière

A l'heure où la transition écologique est une priorité pour tous, chaque filière s'interroge sur la meilleure manière d'agir au regard de ses enjeux et de ses contraintes. L'ACN a initié une large réflexion dans ce domaine afin de permettre aux entreprises de la filière de partager leurs bonnes pratiques et de mutualiser leurs réflexions pour positionner notre secteur sur une trajectoire ambitieuse de transition écologique.

Dans le cadre de cette édition 2024 de l'Observatoire ACN de la confiance numérique, nous avons souhaité apporter des éléments d'éclairage quantitatifs et qualitatifs sur la réalité de cette transition dans notre secteur. A cet effet, nous avons interrogé les industriels de la confiance numérique sur leur implication et leurs motivations à mettre en œuvre des actions de réduction de leur empreinte environnementale.

La transition écologique est-elle une priorité pour votre entreprise ?



La transistion écologique un sujet majeur pour la filière

2% de leur chiffre d'affaires

c'est le montant estimé des investissements réalisés par les entreprises de la filière pour des actions en transition écologique.

Les actions mises en œuvre

Les entreprises de la filière sont majoritairement conscientes de la nécessité d'agir pour limiter l'empreinte carbone de leurs activités.

Pour réduire leur empreinte nous avons souhaité savoir si elles privilégient des actions visant à optimiser leur consommation de ressources dans leur processus (conception, déploiement, opération) ou si elles mettent en place des stratégies visant à compenser leur impact direct.

Aujourd'hui, vos actions pour limiter l'impact carbone de vos produits/services/technologies relèvent-elles davantage ?

41% D'actions visant à réduire leur consommation de ressources à la source (conception, déploiement, opération)

0% D'actions de remédiation visant à compenser leur impact direct

41% Un peu des deux

18% D'aucune, nous sommes encore trop loin de ces questions; les enjeux de développement ou d'amélioration de la sécurité restent des nos priorités premières

Deux types d'actions ont été mises en évidence : 41% des entreprises optimisent leur consommation de ressources et 41 % optimisent leur consommation de ressource et en même temps, compensent leur impact direct.

On observe que le levier de la compensation n'est jamais utilisé seul et qu'il y a seulement 18% des entreprises interrogées qui ont fait le choix de ne pas mettre en place d'actions.

Les motivations des entreprises pour entreprendre ces actions

Lorsque nous les interrogeons sur leurs motivations à entreprendre dans ce domaine, les entreprises de la filière classent les priorités dans l'ordre suivant :

En tant que chef d'entreprise, quelles sont/seraient vos motivations pour engager (ou pas) une démarche de transition écologique ?

1. **Améliorer votre performance technologique pour permettre de nouveaux usages**
2. **Se conformer aux exigences légales et normatives en vigueur**
3. **Réduire vos coûts opérationnels grâce à des pratiques plus durables**
4. Utiliser la transition écologique comme argument marketing pour attirer les clients
5. Renforcer votre activité en tant que marque employeur par votre engagement écologique
6. Assurer un leadershp technologique pour l'avenir
7. Rien de tout cela ; vous avez d'autres priorités plus urgentes liées à votre coeur de métier

A noter que la motivation liée à une utilisation marketing de ces actions n'arrive qu'en quatrième position, ce qui indique une compréhension profonde des enjeux écologiques de la part des entreprises.

Eclairage sur la transition écologique dans la filière
Interview de Chantal Droulez

Chantal Droulez

Présidente d'AwaCloud et Présidente du groupe de travail transition écologique du CSF Industries et Sécurité

Selon vous, quels sont les grands enjeux de la transition écologique dans le secteur de la confiance numérique ?

L'objectif de réduction des gaz à effets de serre est évalué à -30% à horizon 2030. Le consensus actuel est que les voies d'optimisations envisagées ne permettront pas d'atteindre l'objectif parce qu'immédiatement consommées par la croissance des usages. Des actions complémentaires seront donc nécessaires pour développer la sobriété. A cet égard, l'un des enjeux est de faire évoluer les pratiques de développement logiciel pour avoir des outils plus frugaux dans leur consommation de ressources et plus modulaires dans leur conception pour ne délivrer au client que les services qui lui sont utiles. Cela passera nécessairement par l'évolution des pratiques et des compétences des développeurs comme des architectes. Il est aussi important de comprendre qu'à l'instar de la sécurité by design, le green by design implique des choix plus radicaux et par voie de conséquence plus contraignants sur le plan technique avec pour effet des temps de développement plus longs. Cela pose la question des dispositifs d'accélération compte tenu de l'ampleur des évolutions à réaliser.

Quelles sont les actions en cours pour amener les entreprises vers la transition écologique ?

Les travaux réalisés sont trop nombreux pour être listé de façon exhaustive. Parmi les nombreuses initiatives, je relèverais l'initiative Planet Tech'Care du Numeum qui mobilise leur réseau de partenaires en vue de réduire l'impact environnemental du numérique. L'initiative Cyber4tomorrow du Campus Cyber vise à intégrer/diffuser les principes du développement durable dans la filière cybersécurité et bien sûr The Shift Project qui pilote plusieurs réflexions sur la sobriété numérique. Ces différentes initiatives sont à mettre en face de celles du Cigref sur la sensibilisation et la diffusion de bonnes pratiques côté DSI et RSSI clients.

A l'échelle de la filière de la confiance numérique, l'ACN a entrepris de mobiliser les entreprises du secteur, de mesurer leur activité en matière de transition écologique (notamment par le biais de leur Observatoire de la confiance numérique 2024) mais aussi, d'animer leurs réflexions dans les groupes de travail internes afin de favoriser la mutualisation et le partage de bonnes pratiques.

Enfin, les comités stratégiques de filière (CSF) incorporent tous, dans leurs contrats de filière un volet transition écologique. Un groupe de travail est dédié à cet effet dans le CSF Industries de Sécurité, auquel l'ACN participe activement.

Il y a beaucoup à faire et le secteur se met en ordre de bataille pour avancer.

Quelles sont les voies les plus prometteuses pour réduire les GES dans le numérique ?

La première (et la plus évidente) est la voie de l'optimisation logicielle. Les technologies développées ces dernières années l'ont été sans contrainte de ressources et sont globalement peu optimisées du point de vue du code.

Avantage : le gisement d'optimisation est là.

Difficulté : Dans un contexte de course aux fonctionnalités additionnelles et de pénurie de développeurs, dédier des ressources à l'optimisation du code est une décision difficile quand elle n'est pas rendue impossible du fait de l'entrelacement des dépendances logicielles. Paradoxalement, plus un logiciel est intégré plus le gisement d'optimisation est élevé et moins il est accessible. La portée de ce levier s'en voit diminuée. Les plus à même de le mobiliser avec des résultats significatifs sont ceux qui ont une parfaite maîtrise de leur supply chain technologique ou qui dispose d'un legacy faible.

Une autre voie est celle de l'économie de la fonctionnalité. Elle implique une analyse très fine des besoins que l'on souhaite adresser et des choix radicaux en termes d'architecture. Les résultats peuvent être impressionnants. Une entreprise américaine a, par exemple, fait récemment état de plus de 98% d'économie de ressources cloud. Pour mobiliser ce levier sur les produits existants, il faudrait accepter de les reconcevoir intégralement. Aussi, ce sont plutôt des startups qui investissent ce champ.

Il y a aussi la voie des architectures modulaires pensées pour délivrer au client uniquement les services dont il a besoin. C'est probablement à terme l'un des leviers les plus importants particulièrement si on l'associe au levier précédent avec à la clé l'émergence d'un numérique très différent de celui qu'on connait. Mais sur ces questions nous en sommes encore aux prémices.

Pour conclure, la transition écologique est aujourd'hui une formidable opportunité d'évolution pour le numérique. Et de par la nature des évolutions à réaliser c'est aussi une formidable opportunité d'intégrer les questions de sécurité à la source.

Focus - AN2V

TERRITOIRES DE CONFIANCE... NUMÉRIQUE : 34 935 COMMUNES À SOUTENIR !

Dominique Legrand

Président Fondateur d'AN2V

“ Comment aider (tous) les maires, surtout ceux situés en zone rurale, à mettre en place un système de vidéoprotection relié à un centre de supervision h24 et 365jours/an, en lien direct avec la gendarmerie ?

En zone rurale, le fonctionnement actuel des systèmes de vidéoprotection lorsqu'ils existent, souhaite répondre à différents objectifs tel que la sécurité des personnes, le secours des personnes (levées de doute, compréhension d'un site public contre l'incendie et les accidents, les attroupements inhabituels...), la prévention des atteintes aux biens, la prévention d'actes terroristes...

Il suffit de lancer une enquête sur un département parmi les 101 existants, pour observer les équipements et les fonctionnements des communes de moins de 2000 ou 5000 habitants, et pour constater que dès que l'on s'écarte des préfectures et des sous-préfectures dotés de véritable Centre de Supervision Urbaine (CSU) et qui intègrent un solide service informatique, les petites communes ne peuvent faire hélas que de leur mieux : un achat de 3 à 10 caméras de marque asiatique car peu coûteuses, parfois autonomes et sans connexion fibre optique (donc enregistrement en local), parfois avec un lien radio 4G/5G (à 40%) mais souvent non maintenu en central à la Mairie, pas de CSU actif ; pas d'opérateur, et donc aucun service h24. Enfin, lorsqu'on aborde le RGPD et le risque cyber sur ces dispositifs : peu ou pas d'expertise en la matière sur ces dispositifs. Il est de notoriété publique que le dispositif de vidéoprotection est souvent le maillon faible permettant à un hackeur d'entrer sur l'ensemble de l'informatique d'une mairie ! et même s'il est fréquemment soutenu que le système vidéo est isolé et « bien à part », une analyse rapide permet de trouver rapidement des liens IP avec les autres réseaux de la mairie, pour des raisons de maintenance, de mise à jour des serveurs, de partage de données sur certaines applications...

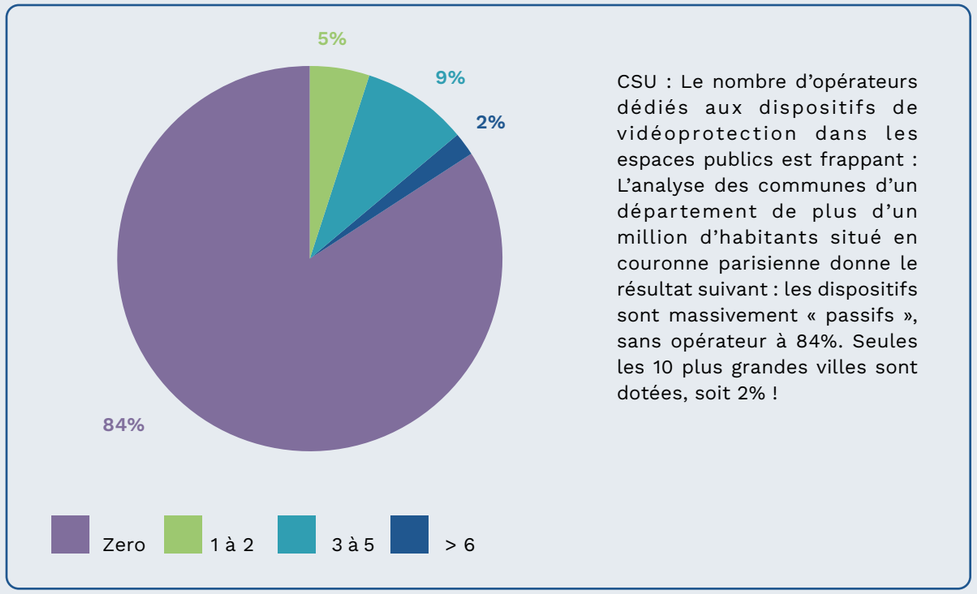
Il est donc utile d'imaginer une refonte importante de tous ces dispositifs afin d'intégrer sereinement de nouveaux usages (smart et durables), et de répondre au mieux aux nouvelles attentes de services pour tous nos concitoyens.

Dans tous les départements français, un réseau haut débit à base de fibre optique a été déployé sur l'ensemble de ses communes, et si ce n'est pas encore fait, c'est en passe de l'être à court terme sous quelques années avec l'abandon du cuivre chez l'abonné (Plan France Très Haut Débit lancé en 2013).
Les communes souhaitent intégrer les nouveaux usages et étudier les moyens de détection automatique apportés par l'analyse d'images (Intelligence Artificielle), l'interprétation des évènements provenant d'autres capteurs (IoT de confiance) ou d'applications externes (sur les smartphones des concitoyens). Il est alors indispensable d'imaginer une mutualisation technique et organisationnelle de tous les dispositifs, et le bon échelon semble être le Département.

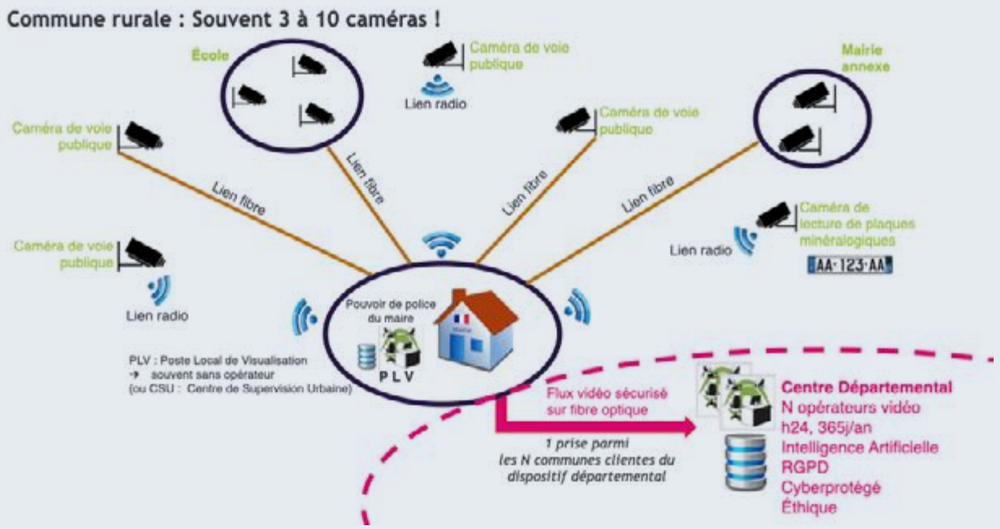
C'est aujourd'hui possible avec l'article 42 de la loi de sécurité globale préservant les libertés (Article L132-14 du CSI – Code de Sécurité Intérieur – Version en vigueur depuis le 27 mai 2021, modifié par la LOI n°2021-646 du 25 mai 2021 – Article 42).

La mutualisation des dispositifs de vidéoprotection à l'échelle d'un département est une source indéniable d'efficience : Elle permet d'un point de vue opérationnel d'atteindre la taille critique nécessaire à la création d'un centre superviseur doté de vidéo-opérateurs traitant les images en temps réel h24 365j/an, ainsi que la mise à disposition d'outils très performants de nouvelle génération (IA, recherches rapides...).

Elle permet en une seule fois de traiter la zone verte et orange du camembert ci-dessus (soit 89% des communes !) Elle permet en outre de couvrir un territoire plus large et plus cohérent, à l'échelle d'un bassin de vie comme le stipulait le rapport parlementaire de 2018 sur le continuum de sécurité réalisé par Alice Thourot et Jean-Michel Fauvergue.



CSU : Le nombre d'opérateurs dédiés aux dispositifs de vidéoprotection dans les espaces publics est frappant : L'analyse des communes d'un département de plus d'un million d'habitants situé en couronne parisienne donne le résultat suivant : les dispositifs sont massivement « passifs », sans opérateur à 84%. Seules les 10 plus grandes villes sont dotées, soit 2% !



L'intercommunalité était déjà prévue par le code de sécurité intérieur, il n'y avait pas lieu de légiférer sur ce sujet, mais cette mutualisation des dispositifs de vidéoprotection ne concerne que les communes situées dans un bloc communal. Les communes plus rurales n'arrivaient jamais à atteindre un volume justifiant la création d'un poste d'exploitation, y compris au sein de leur communauté de communes. L'AN2V dénonce donc depuis fort longtemps cette fracture de sûreté entre les territoires ruraux ou semi-ruraux et les villes et centres-villes.

Cette loi apporte depuis 2021 une solution très attractive pour les communes rurales. À ce jour, une quinzaine de départements au travers de leur syndicats mixtes numériques se sont lancés dans des études sur ce sujet, et en avril 2024, déjà 5 départements se sont équipés !

L'ACN et l'AN2V unissent leurs forces pour que ce type de projet voit le jour, car les défis techniques et organisationnels sont nombreux ! En effet, il est indispensable de bien maitriser :

• Les domaines de responsabilités techniques et juridiques entre les communes clientes et le porteur du dispositif central (exemple : le SMN – Syndicat Mixte Numérique), des conventions sont à rédiger ! Des relations officielle sont à créer avec les FSI – Forces de Sécurité Intérieures…

• Une définition transparente de l'organisation du projet, le «qui fait quoi quand» ! De la formation des opérateurs vidéo centraux, de leurs feuilles de missions jour et nuit…

• Le réseau d'interconnexion IP avec les réseaux de vidéoprotection de la commune cliente, son architecture réelle (à revoir parfois, adressage IP, QoS…),

• L'architecture informatique de stockage mutualisé (en local sur site et/ou chez un hébergeur) et éventuellement redondée en central et sur la commune,

• Un système de gestion de visualisation des flux vidéo supportant une telle charge (VMS – video management software), des milliers de flux vidéo à hiérarchiser ?

• Une suite logicielle d'IA mutualisée, de confiance, sur les sujets safe, smart et sustainable, et plus généralement, une relation étroite avec le DPO/DPD du projet afin que la donnée qui circule soit parfaitement encadrée au sens du RGPD et du respect des libertés individuelles,

• Une forte résistance à tout type d'attaque cyber, et a minima, un cloisonnement fort évitant tout effet domino. ”

5.2 Les tendances réglementaires

5.2.a. Paysage réglementaire européen : un marché unique du numérique de confiance à concrétiser

La transformation numérique continue de s'opérer au sein de l'UE. Les nouveaux risques qui découlent des nouveaux usages amènent les institutions européennes et les Etats membres à réfléchir aux moyens d'adapter notre arsenal législatif à ses évolutions et de permettre à l'Union européenne d'avoir la maîtrise de son avenir numérique. Le programme « Pour une Europe numérique », par lequel s'opère cette réponse, vise à faire de l'Europe un acteur majeur dans ce domaine, à renforcer sa souveraineté technologique et à assurer sa résilience dans un contexte de tensions croissante dans le cyberespace. Cette année, de nombreux projets de textes européens poursuivent leur parcours législatif et sont sur le point d'aboutir. Ces projets concernent le domaine de la cybersécurité, et plus particulièrement du renforcement de la résilience, de l'identité numérique, de la régulation du marché ainsi que la mise en place d'un cadre juridique pour l'intelligence artificielle.

L'ensemble de ces travaux sont prioritaires pour la filière de la confiance numérique. L'année 2024 est une année charnière du point de vue institutionnel en Europe et est marquée notamment par le renouvellement du Parlement et de la Commission européenne. En amont de ces élections, l'ACN a publié en avril 2024 ses priorités européennes et recommandations pour accélérer la transition vers un marché unique du numérique de confiance.

Le renforcement de la cybersécurité

Le projet de Cyber Resilience Act (CRA), visant à établir des exigences communes de cybersécurité pour les produits comportant des éléments numériques, poursuit son chemin législatif. Avant son adoption par le Parlement européen en mars 2024, de nombreuses modifications ont été apportées à ce texte, notamment dans le but de rapprocher ses dispositions à des textes déjà existants (directive NIS 2, Cybersecurity Act, ...). A date, le Conseil de l'UE doit encore adopter ce projet de règlement.

Face aux risques croissants de cybersécurité, le renforcement de la solidarité européenne dans ce domaine a également fait l'objet d'un traitement législatif à travers le Cyber Solidarity Act afin de mettre en œuvre un Bouclier Cyber européen, un Mécanisme d'Urgence Cyber, créant notamment une Réserve Cyber européenne, et un Mécanisme d'Analyse des Incidents de cybersécurité. Après un trilogue ayant amoindri le budget originel alloué àla Réserve Cyber européenne, le texte doit encore être adopté par le Conseil de l'UE, le Parlement l'ayant voté en mars 2024.

L'ACN a publié en 2024 ses priorités européennes de la filière de la Confiance Numérique.

Rapport ACN
« Priorités européennes de la filière de la confiance numérique 2024 » disponible sur www.confiance-numerique.fr

Enfin, après une légifération prolifique au début de l'année 2023, les Etats membres ont aujourd'hui plusieurs textes à transposer dans leur droit national. La directive NIS 2, la directive sur la Résilience des Entités Critiques (directive REC), ou encore les exigences du règlement DORA doivent être mis en œuvre entre la fin de l'année 2024 et le début de l'année 2025.

La mise en œuvre d'une identité numérique européenne interopérable

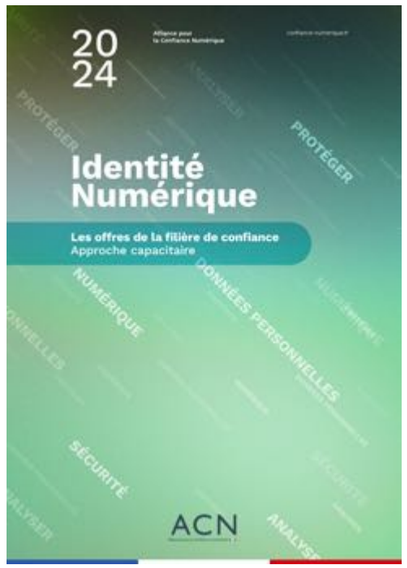
Les travaux de révision du règlement eIDAS visant à mettre en œuvre une identité numérique sécurisée et interopérable en Europe ont abouti le 30 avril 2024 avec sa publication au Journal Officiel de l'UE. L'Europe est donc sur point de permettre à l'ensemble de ses habitants de disposer d'un portefeuille numérique personnel utilisable sur l'ensemble de son territoire. Sa mise en œuvre se fera sur la base de normes techniques communes (Architecture and Reference Framework – ARF), toujours en discussion. Les Etats membres devront, dès 2027, permettre à tout citoyen européen de bénéficier gratuitement d'un portefeuille d'identité numérique.

Régulation du marché numérique

Le Digital Service Act (DSA) et le Digital Market Act (DMA) qui visent à protéger le marché numérique européen des contenus et produits illicites, mais aussi des pratiques déloyales de certains acteurs, sont tous les deux entrés en application. L'ensemble des entreprises désignées par ces règlements ont été identifiées dans le but de protéger la souveraineté technologique européenne.

Aussi, la révision de la directive sur la responsabilité du fait des produits défectueux (Liability for Defective Product) évolue afin d'intégrer à son champ d'application la vulnérabilité en matière de cybersécurité. La protection des utilisateurs est alors approfondie.

De plus, la Commission européenne tente de préparer la Banque Centrale européenne (BCE) à la mise en place d'une cryptomonnaie publique européenne à travers sa proposition « d'Euro numérique ». Le but est de compléter la monnaie fiduciaire et les solutions privées existantes. Les discussions sur ce projet suivent leurs cours au sein des institutions européennes, particulièrement au sein de la BCE, sans pour autant que le lancement d'un euro numérique ne soit garanti.



En complément des documents «**Offre capacitaire Identité numérique**», l'ACN a développé un site pour recenser et rendre visibles toutes les offres françaises d'identité numérique.

A retrouver sur le site :
https://identite.confiance-numerique.fr/

La concrétisation d'un cadre juridique européen applicable en matière d'intelligence artificielle

Le règlement sur l'intelligence artificielle (AI Act) a finalement été adopté par le Parlement et le Conseil de l'UE en début d'année 2024, après 3 ans de négociations. Les dispositions prévues par le règlement seront applicables dès la fin de l'année 2024, avec quelques exceptions pour les forces de l'ordre dans la prévention de la menace terroriste ou pour la recherche de victimes ciblées. La mise en œuvre complète de ce texte, guidée par le Bureau de l'IA qui se structure, est prévue pour 2026. La filière souligne l'importance de ces travaux. En effet, l'application d'un cadre juridique européen pour l'IA est à l'essence même de l'IA de Confiance que la filière s'est attachée à définir à travers son livre blanc dédié à l'IA de confiance.

Divulgation coordonnée de vulnérabilités : un élan européen à amplifier

La mise en place de politiques de divulgation coordonnée de vulnérabilités est désormais rendue obligatoire par la directive NIS 2 le Cyber Resilience Act. La question de la découverte et du traitement des vulnérabilités, en discussion depuis plusieurs années, est un sujet considéré comme central dans l'approche européenne de la cybersécurité et comme un outil majeur pour augmenter le niveau de protection et de résilience des entités européennes. Toutefois, les premiers éléments de réponse portés par les Etats membres de l'Union européenne mériteraient d'être homogénéisés par une approche holistique. Cela permettrait une harmonisation de la législation européenne et réduirait considérablement l'insécurité juridique à laquelle sont confrontés bon nombre de chercheurs en vulnérabilités, surtout dans des situations transfrontalières.

A l'inverse, les législations nationales de chaque Etat membre pourraient avoir un rôle d'aiguillon. En France, plusieurs pistes sont possibles, telles que la révision du Code pénal afin d'introduire un dispositif qui protégerait les chercheurs en vulnérabilités de bonne foi d'éventuelles poursuites judiciaires engagées à leur encontre. Une telle initiative nationale pourrait constituer un socle majeur pour dessiner le cadre juridique complet qui fait aujourd'hui défaut et augmenter ce faisant la protection et la résilience de notre pays et de l'Union européenne dans son ensemble. L'ACN a publié, en 2024, un livre blanc sur le sujet qui compare les différentes approches européennes et propose des pistes de réflexion pour adapter notre législation nationale et parvenir à ce que la divulgation coordonnée de vulnérabilités puisse apporter sa pleine contribution à la cybersécurité et à la résilience.

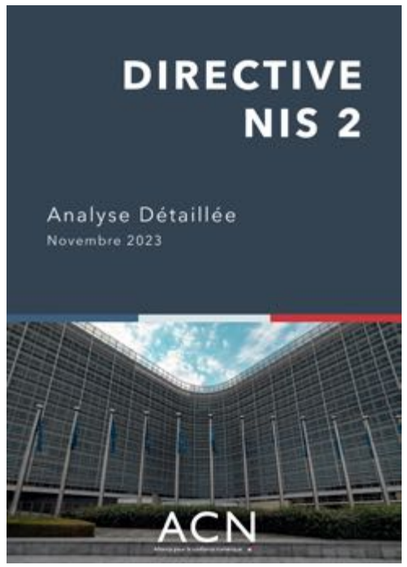
L'ACN a publié en mars 2024 un livre blanc sur la Divulgation coordonnée de vulnérabilités

Livre Blanc
« La Divulgation coordonnée de vulnérabilités »
disponible en téléchargement sur
www.confiance-numerique.fr

5.2.b Les initiatives nationales de confiance numérique

Pour répondre aux nouveaux défis soulevés par les évolutions du cyberespace et faire de la France un acteur mondial de la cybersécurité, une stratégie nationale pour la cybersécurité a été déployée dès février 2021 par le Président de la République. Elle place le développement de solutions innovantes de confiance et souveraines comme une priorité. En ce sens, trois vagues d'appel à projets ont été lancées afin de soutenir la sécurisation des infrastructures critiques, des suites collaboratives de travail, la résilience des plus petites structures ou encore l'évaluation de cybersécurité. En parallèle, la stratégie nationale pour l'intelligence artificielle (IA) poursuit son chemin. Un Comité de l'IA générative a notamment été lancé en septembre 2023 dans le but d'éclairer le Gouvernement et de faire de la France un pays à la pointe de la révolution de l'IA.

Aussi, la France se prépare à l'entrée en application de plusieurs textes européens. D'abord, la loi « Sécuriser et réguler l'espace numérique » (SREN) a définitivement été adoptée par le Parlement, le 10 avril 2024. Ce texte, destiné à adapter le droit national aux règlements européens sur les services numériques (DSA) et sur les marchés numériques (DMA), a été proposé par le gouvernement en mai 2023. En plus des dispositions relatives aux exigences des textes européens visés, la loi SREN inclut plusieurs initiatives visant à renforcer l'ordre public dans l'espace numérique et place la confiance numérique au cœur de son projet.
Enfin, un projet de loi visant à transposer la directive NIS 2 en droit français est en cours d'élaboration. La directive NIS 2 dispose en effet que ses exigences doivent être transposées dans le droit national des Etats membres avant le 17 octobre 2024. Ce projet de loi transposera également la directive sur la résilience des entités critiques (REC) et les exigences du règlement sur la résilience opérationnelle (DORA) des entités financières.



Rapport ACN « Analyse détaillée directive NIS 2 »

Disponible sur le lien suivant :
www.confiance-numerique.fr

Focus - Comités Stratégiques de Filière (CSF)

VISIONS CROISÉES DES COMITÉS STRATÉGIQUES DE FILIÈRE INDUSTRIES DE SÉCURITÉ ET SOLUTIONS NUMÉRIQUES DE CONFIANCE

Marc Darmon

Président du CSF Industries de Sécurité

Le partenariat stratégique de la filière des industries de sécurité avec l'État a été institué formellement il y a dix ans, pour répondre aux enjeux industriels majeurs de la protection de l'État, de l'économie, de la société. Il s'est renforcé avec la création du comité stratégique de filière (CSF) en 2018 dont le second contrat de filière (2024-2027) doit être prochainement signé.

Quel est le périmètre et le champ d'action du CSF ?

La filière Industries de sécurité (IS) pèse 32 Mds€ et 157 000 emplois (2021). Elle rassemble toutes les entreprises qui apportent les solutions et services technologiques de sécurité (lutte contre le terrorisme et la grande criminalité, sécurité du quotidien, secours aux personnes, protection des frontières, des infrastructures et des réseaux, cybersécurité, identifié numérique.

Le nouveau contrat de filière renouvelle les verticales traitées jusqu'à présent par le CSF IS (sécurité des JO et des grands évènements, cybersécurité, identité numérique, territoires de confiance, et numérique de confiance) et élargit son approche, en introduisant des horizontales : compétitivité des PME, normalisation, international, maitrise des technologies, attractivité et compétences, transition écologique, pour activer plus efficacement tous les leviers du développement de la filière.

Quelles sont les grandes priorités qui seront mises en œuvre dans ce cadre ?

Le second contrat s'articule selon quatre axes : croissance d'une filière compétitivité et d'excellence, maitrise des technologies clés d'avenir et des technologies critiques, attractivité et compétences, accompagnement de la transition écologique. Il s'est bâti avec pour objectifs d'intensifier au sein du CSF le dialogue avec l'État, notamment sur les sujets où la position de celui-ci conditionne les solutions ou influe sur les modèles économiques de l'industrie, et de conduire une réflexion stratégique permanente sur son avenir et sur les nouveaux sujets (IA de confiance, lutte contre la manipulation de l'information, ...). Par ailleurs, ce second contrat vise à permettre à la filière de progresser avec exigence vers des solutions de qualité, innovantes, compétitives et éthiques, en intensifiant le dialogue avec les marchés. Enfin, le renforcement du soutien aux PME de la filière, du lien avec la recherche et le développement d'actions transverses sont également privilégiés pour poursuivre l'édification d'une base industrielle forte et souveraine.

Quel rôle souhaiteriez-vous voir tenir à l'ACN, et plus largement aux entreprises du secteur de la confiance numérique dans vos travaux ?

L'ACN est un acteur central de la filière et un contributeur majeur, dès la création de celle-ci, aux travaux et aux avancées. Elle est en particulier au cœur de trois segments clés de la filière, l'identité numérique, la cybersécurité et l'IA de confiance. A travers les travaux techniques qu'elle mène et à ses actions proactives comme défensives sur les domaines législatif, réglementaire et normatif, elle constitue un chainon essentiel de l'écosystème et joue un rôle irremplaçable dans le dialogue stratégique avec l'État ainsi qu'avec l'échelon européen. Je souhaite que l'ACN poursuive dans cette voie avec dynamisme et aide la filière à mobiliser tous les grands leviers à sa disposition pour concrétiser ses objectifs-clés.

Michel Paulin

Président du CSF Solutions Numériques de Confiance

Quel est le périmètre et le champ d'action du CSF ?

La filière Solutions numériques de confiance réunit les éditeurs de logiciels et fournisseurs d'outils, de produits et de services numériques hors ESN et entreprises de conseil. Avec un chiffre d'affaires de 23,7 Mds€ en 2023 et une croissance de 10% par an, c'est l'une des filières les plus dynamiques de l'industrie française. Elle est composée d'acteurs représentant plus particulièrement les domaines du cloud, de l'intelligence artificielle, du quantique, des technologies immersives et des logiciels. Le Comité Stratégique de filière est l'organe qui réunit l'Etat et cet écosystème pour un dialogue stratégique sur son développement.

Quelles sont les grandes priorités qui seront mises en œuvre dans ce cadre ?

La mission de préfiguration du Comité Stratégique de filière a identifié 5 axes structurants qui définiront ses travaux pour les 3 prochaines années :
- Le développement de l'offre et le déploiement des infrastructures nécessaires aux innovations (IA etc.) dans le numérique de confiance,
- Le développement de l'accès à la formation et un travail conjoint avec l'Etat sur les dispositifs d'innovation pour favoriser le numérique de confiance,
- La définition des données sensibles et l'harmonisation des certifications et régulations,
- La facilitation de l'accès des acteurs numériques de confiance à la commande publique et privée,
- La croissance internationale du secteur.

Quel rôle souhaiteriez-vous voir tenir à l'ACN, et plus largement aux entreprises du secteur de la confiance numérique dans vos travaux ?

Les entreprises et structures existantes qui œuvrent en faveur du numérique de confiance jouent un rôle majeur de sensibilisation, de pédagogie, de mise en relation et de dynamisation de l'écosystème Solutions numériques de confiance. A ce titre, nous souhaiterions les inclure dans nos groupes de travail et leur proposer d'adhérer à l'association Solutions numériques de confiance pour bénéficier de leur expertise et de leurs travaux sur le numérique de confiance.

VI. LES TENDANCES TECHNOLOGIQUES

L'innovation technologique est le principal moteur de la croissance de la Confiance Numérique française et mondiale depuis plus de 10 ans et cette tendance devrait se poursuivre à minima durant les 10 prochaines années. Les développements technologiques affectent la Confiance Numérique de manières différentes et complémentaires.

6.1 Les innovations électroniques et numériques qui génèrent de nouveaux marchés

Les innovations issues des industries électroniques et numériques impactent presque tous les secteurs des économies modernes et génèrent de ce fait de nouveaux marchés pour la Confiance Numérique.

■ **Les systèmes et composants électroniques sont marqués par la miniaturisation couplée à la baisse des coûts.** Cette tendance, incarnée par la Loi de Moore, a marqué très fortement l'économie mondiale ces 50 dernières années et devrait se poursuivre à minima sur la décennie à venir avec le développement des mémoires 3D multicouches et la miniaturisation des processeurs. 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 seulement sept entreprises se maintiennent au niveau mondial : Samsung (Corée du Sud), TSMC (Taïwan) et Intel (États-Unis) dans les processeurs et Samsung (Corée du Sud), SK Hynix (Corée du Sud), Micron (États-Unis), Western Digital (Etats-Unis) et Toshiba (Japon) dans les mémoires.

En conséquence de la miniaturisation et de la baisse des coûts, les produits électroniques se démocratisent, y compris en matière de Confiance Numérique : capteurs, système de traçage et localisation, ainsi que tous les sous-systèmes inclus dans les segments électroniques de la filière. Il s'agit d'un phénomène de long terme. A court terme, la croissance des composants électroniques est cyclique et la période 2020-2022 a, au contraire, vu les prix des semi-conducteurs s'envoler. Depuis le début de l'année 2023, la baisse des prix de semi-conducteurs a repris son cours.

Dans les cinq années à venir, seules les augmentations des prix de l'énergie sont à même de contrebalancer la baisse des prix associée à la poursuite de la miniaturisation de l'électronique, en fonction de l'amplitude qu'elles vont avoir, en particulier en Europe.

■ **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 au travers du déploiement du **continuum *Cloud-to-Edge*** et ses débouchés en matière d'IoT industriels (logiciel embarqué, connectivité, *cloud*).

Le croisement de ces deux tendances génère de nombreux marchés émergents et porteurs pour la Confiance Numérique.

1. Sécurité des objets connectés. À terme, 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 depuis plusieurs années. Les progrès dans la standardisation et l'interopérabilité des architectures IoT sont à même d'accélérer la croissance future.

■ **Automobile connectée.** Le principal segment déjà en forte croissance est celui de la sécurisation des automobiles et de leurs communications : *Vehicle-to-Vehicle* (V2V), *Vehicle-to-Infrastructure* (V2I : péage, etc.), *Vehicle-to-Device* (V2D : *Smartphone*, etc.).

■ ***Smart & Safe City.*** Le développement des objets connectés dans les villes à des fins de sécurité est le deuxième segment qui a généré la croissance la plus importante au niveau mondial chez les acteurs de la sécurité numérique et de la cybersécurité en lien avec les objets connectés depuis 2015. 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.

■ **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 et *clouds* souverains. En parallèle du foisonnement technologique en matière d'électronique autour du stockage et du traitement des données (mémoires non-volatiles 3D multicouches, puces neuromorphiques, calcul quantique, calcul photonique, photonique intégrée, réseaux d'interconnexion photonique, calcul de haute performance (HPC), etc.), le nombre et le volume des bases de données croît de manière exponentielle (big data). La problématique de sécurisation de ces jeux de données prend de plus en plus d'importance, que ce soit pour des raisons régaliennes (services publiques, bases de données critiques), économiques (protection des données sensibles des entreprises), ou citoyennes (droits du citoyen, protection des données personnelles, droit à l'oubli...).
Lancée en mai 2021, la stratégie nationale « Cloud de confiance » a eu le mérite de poser les bases d'un cadre juridique visant à ce que les données des administrations françaises ne puissent pas être hébergées directement par des entreprises qui ne sont pas sous le contrôle exclusif de juridictions françaises. Cette stratégie s'articule autour de trois piliers que sont :

a) Le label Cloud de confiance délivré selon les référentiels de l'Agence nationale de sécurité des systèmes d'information (ANSSI).
b) La politique «Cloud au centre» pour l'administration (basée sur le référentiel SecNumCloud).
c) Une politique industrielle mise en oeuvre dans le prolongement de France Relance.

A cet égard, l'offre NumSpot, une collaboration entre Docaposte, la Banque des Territoires, Dassault Systèmes, et Bouygues Telecom, vise à établir une offre de cloud indépendant et souverain en France. Cette initiative utilise l'infrastructure cloud OUTSCALE de Dassault Systèmes, qualifiée SecNumCloud, pour offrir des services qui répondent aux standards de performance, sécurité, et responsabilité environnementale. Depuis son lancement en automne 2022, NumSpot a formé une équipe de cent experts et a établi des partenariats avec des acteurs majeurs du cloud. La première version de cette plateforme de cloud est prévue pour mai 2024 et inclura un catalogue de services managés en expansion.

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 numérique (« citoyenneté à distance »). La norme actuelle en France demeure l'existence simultanée de nombreuses identités décorrélées, avec un niveau de sécurité élevé (CNI, passeport), substantiel (identité numérique La poste, PVID) et faible (identités numériques délivrées très majoritairement par les acteurs du numérique américains du type GAFA pour le e-commerce), sans garantie de protection des données. L'alternative est le déploiement d'une identité forte 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 depuis 2022 au niveau français autour **du déploiement de la Carte Nationale d'Identité Electronique (CNIe) et de FranceConnect, 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.

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

En parallèle -et étant donné que la Confiance Numérique est elle-même constituée intégralement de solutions électroniques et numériques- **les innovations issues de la Confiance Numérique** en elle-même génèrent de **nouveaux produits**, de nouvelles applications et donc de la croissance.

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

■ **Cryptographie légère (*Lightweight cryptography*).** Le développement rapide de l'IoT a un impact énorme sur tous les aspects liés à la cybersécurité. De récentes attaques massives contre des configurations IoT ont montré que de solides techniques cryptographiques doivent être utilisées pour assurer une sécurité globale du système. Malheureusement, dans le cas de l'IoT, où le coût est un paramètre important, l'utilisation de la cryptographie peut être limitée par la taille, la puissance et les performances informatiques locales des objets. Cela a donné naissance à un domaine de recherche très actif autour de la cryptographie dite légère. En bref, la cryptographie légère recherche de nouveaux algorithmes ou protocoles cryptographiques adaptés à la mise en oeuvre dans des environnements restreints, y compris les étiquettes RFID, les capteurs, les appareils de santé et de soins. La cryptographie légère sera 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 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.

L'ACN a publié en mai 2021 un rapport sur les procédés cryptographiques avancés, dans lequel est décrit l'état de l'art pour chacune de ces technologies.

Rapport ACN
«Procédés cryptographiques avancés»
disponible en téléchargement sur
www.confiance-numerique.fr

■ **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 dans les prochaines années.

■ **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 dans les prochaines années.

2. Eléments 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 (SW) et de matériel (HW) et visant à être intégrés dans des dispositifs communicants afin de gérer de manière sécurisée toutes les interactions entre ces derniers et le monde extérieur en stockant des applications dédiées et des données confidentielles de manière chiffrée (cartes SIM, puces de cartes bancaires…).

Dans le contexte du développement des IoT, le segment des éléments sécurisés est marqué par le remplacement des cartes SIM (*Universal integrated circuit card*), par des éléments sécurisés miniaturisés et directement embarqués ou intégrés dans les systèmes auxquels ils se rattachent, voire sans aucune composante *hardware* (*soft secure elements*, *Trusted Execution Environment*). Le déploiement des éléments sécurisés embarqués (e-UICC) et des *Soft secure elements* a commencé et le déploiement massif des éléments sécurisés intégrés (i-UICC) ne devrait pas avoir lieu avant 2024, c'est-à-dire une fois que les problèmes d'assurance et de normalisation auront été résolus. La France domine actuellement ce secteur au niveau mondial avec l'Allemagne et devant la Chine, les Etats-Unis et la Corée du Sud. Les principaux concurrents des acteurs français au niveau mondial sont le néerlandais NXP, les allemands Infineon et Gieseke & 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 artificielle regroupe le développement d'algorithmes de machine learning (réseaux de neurones artificiels, multicouches ou non, supervisés ou non, réseaux antagonistes génératifs…) à des fins de prévision ou de classification, l'IA générative de texte tel que ChatGPT 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 la thématique implique une mise en place d'un cadre pour une IA de confiance.

•**La nécessité d'un cadre juridique:** Garantir que son développement et son utilisation s'alignent sur les valeurs fondamentales de la société. Cela implique la mise en place de travaux législatifs européens pour établir un cadre juridique stable qui protège à la fois les droits et les libertés des citoyens tout en permettant l'innovation technologique. Ce cadre doit prendre en compte plusieurs aspects de l'IA, tels que la nature technique et la responsabilité, et être élaboré de manière concertée pour former un socle cohérent et solide. L'enjeu est de réguler, en éliminant les risques potentiels, sans pour autant empêcher l'innovation afin de ne pas priver la société d'outils essentiels pour sa souveraineté numérique et son autonomie stratégique.

• **La définition d'une IA de confiance:** Les systèmes d'IA doivent être conçus pour être transparents, explicables et sécurisés. La confiance dans ces systèmes peut être renforcée par des normes strictes de cybersécurité et des processus de développement rigoureux pour anticiper les failles et les abus potentiels. En outre, les données utilisées pour la phase d'apprentissage de ces modèles d'IA doivent être gérées de manière éthique, avec des standards clairs pour éviter l'introduction de biais discriminatoires, afin d'assurer que les décisions prises par ces modèles soient justes et équitables.

• **Acceptation sociale de l'IA:** essentielle, elle doit être cultivée à travers une approche éthique de son déploiement. Respecter les principes éthiques, protéger les droits de l'homme et prioriser le bien-être humain dans le développement de l'IA sont fondamentaux. L'éducation et la sensibilisation du public, combinées à des démonstrations transparentes de l'utilité et de la sécurité de l'IA, comme lors d'événements majeurs, peuvent faciliter une meilleure compréhension et acceptation de ces technologies.

En matière d'intelligence artificielle, la France bénéfice d'une excellence en matière de formation et de recherche et les acteurs français de la sécurité prennent d'assez fortes positions en matière d'applications de sécurité (notamment Thales Digital Identity & Security et Idemia). Bien que distancée par les Etats-Unis et la Chine qui mettent a profit leur fort tissu industriel du numérique, la France dispose d'une industrie compétente dans l'IA industrielle et l'IA générative. Malgré cela, on observe toutefois une fuite des cerveaux de la France vers les Etats-Unis en la matière, qui menace les positions françaises à l'avenir y compris sur le secteur de la sécurité.

L'ACN a publié en mars 2024 un livre blanc sur l'IA de confiance

Livre Blanc
« L'intelligence Artificielle de Confiance »
disponible en téléchargement sur
www.confiance-numerique.fr

4. Blockchain. D'abord associée aux cryptomonnaies et au Bitcoin en particulier, la blockchain s'impose comme un nouvel outil indispensable de la confiance numérique. Ce protocole enregistre et stocke les transactions sous forme cryptée dans une base de données décentralisée. Les informations sont, de fait, infalsifiables et non modifiables. Registre distribué et sécurisé de transactions, la blockchain est à la fois un vecteur de confiance et un outil de lutte contre la fraude. Elle est soit publique (tous les participants peuvent intervenir dans le processus), soit privée. Dans ce cas, seuls certains participants enregistrent des transactions et autorisent ou non leur lecture. Les développements en matière de confiance numérique sont multiples : gestion des prestations sociales, protection des infrastructures des opérateurs d'importance vitale, mais aussi missions de sécurité civile ou intérieure et gestion du secret entre institutions.

Ces applications réduiront la dépendance à une autorité centrale mais elles nécessitent l'évolution du système de confiance centralisé actuel vers un système décentralisé pour les applications de type régalien ainsi qu'une nouvelle organisation des opérations. Les acteurs français maîtrisent plusieurs des technologies clés du domaine de la blockchain (cryptographie, méthodes formelles…). Cependant, il faut souligner 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.

5. Plateformes d'Open Hardware/Software pour l'edge computing et les IoTs. Le partage de code logiciel (Open Software) est déjà pratiqué depuis un certain temps, mais depuis quelques années, la tendance 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 re-publication en Open Source des nouveaux développements alimente le processus d'innovation et bénéficie à toute la communauté. Les atouts de la France dans ce domaine de l'Open Source sont nombreux. Le marché national est très développé, il représente le quart du marché européen. La communauté tant des chercheurs que des développeurs est sans conteste la plus nombreuse et la plus avancée. Cependant, la sécurité est peu présente dans le monde Open Source. Le marché de la sécurité est encore dominé par les grands éditeurs de logiciels propriétaires, nord-américains pour la plupart. Une politique d'achat volontariste et l'incitation au développement de briques technologiques et de plates-formes certifiées et orientées vers l'Open Source contribueraient au renforcement de ce domaine, en particulier pour les applications innovantes associées à l'edge computing ou aux IoTs pour lesquels la domination américaine ne se fait pas encore trop ressentir.

6. Analyse en temps réel des données d'observations locales et large zone. En matière d'observation et de surveillance locale, l'analyse en temps réel sera à terme la clé de voute du futur écosystème de la vidéosurveillance. Couplée à l'intelligence artificielle, elle permettra d'identifier en temps réel des individus recherchés ou de prendre automatiquement certaines décisions. L'imagerie satellitaire en temps réel se développe également avec de nombreux débouchés en matière d'observation large zone et de renseignement & collecte d'information. La France dispose des acteurs et du savoir-faire technologique pour bénéficier pleinement de ces développements technologiques.

7. Open Source Intelligence (OSINT). L'OSINT existe depuis des dizaines d'années sous une forme embryonnaire (sources humaines, documentation, bibliographie…). C'est avec l'explosion du nombre de données ouvertes disponibles en ligne depuis le début des années 2010 que le marché de l'OSINT se développe réellement, au travers du développement d'outils informatiques permettant la collecte et l'exploitation de ces données. Ces données proviennent de différentes sources : Réseaux sociaux, sites internet, médias, imageries géospatiales, forum, appareils de mesure, etc., lesquelles représentent une mine d'or d'information exploitable à des fins de renseignement. Jusqu'au début des années 2010, les utilisateurs de services d'OSINT se limitaient aux agences régaliennes à des fins de renseignement ou de répression des fraudes, crimes et délits, ainsi qu'à quelques

grandes entreprises, notamment par le biais des agences d'intelligence économique. Aujourd'hui on voit peut voir l'émergence d'un écosystème d'entreprises capable de fournir du savoir-faire OSINT, dont les plus importantes sont Chapsvision (notamment avec le rachat de Owlint), Palantir, Thales, Athea, Airbus (GEOINT), Anozr Way, Sekoia.io, etc.

6.3 Transformation numérique & miniaturisation : Vers des offres globales de *Security as a Service*

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

En effet, au niveau mondial, la Confiance Numérique est impactée par deux facteurs majeurs :

■ **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 numérique,** conduisant à une croissance toujours plus importante de la part qu'occupent les logiciels dans les outils de sécurité. En particulier, les producteurs de produits physiques et électroniques – où les marges sont en moyenne plus basses qu'en cybersécurité – tentent progressivement de monter en gamme dans la chaine de valeur en développant des compétences dans le logiciel. Ces derniers -à l'image de 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 auparavant composée que de moyens humains, son contenu technologique et électronique s'accroit continuellement (SOC, caméras de vidéosurveillance, etc.), grâce à la miniaturisation et à la baisse des coûts des produits électroniques. Dans la surveillance humaine, la rentabilité nette est très faible (1% en moyenne seulement en 2021 et dopée artificiellement par le CICE). Dans la sécurité électronique, elle est plus élevée, bien qu'avec des niveaux variables selon les entreprises. La volonté d'un grand nombre d'acteurs des services privés est donc de diversifier leurs services en y intégrant des produits électroniques et cyber et en montant en gamme. A titre illustratif, la grande entreprise espagnole Prosegur, l'un des leaders européens du gardiennage, a crée un fonds d'investissement doté de 30 M€ pour investir dans la sécurité électronique et cyber. Depuis 2016, ce fonds 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. 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.

Focus - CNRS, INRIA, CEA

LE PROGRAMME DE RECHERCHE (PEPR) DE LA STRATÉGIE NATIONALE POUR LA CYBERSÉCURITÉ
10 DÉFIS DE RECHERCHE FONDAMENTALE AU SERVICE DE LA FILIÈRE

Face à une menace cyber en constant développement et dans le contexte d'une compétition internationale accrue en matière de développement de solutions visant à protéger les citoyens, les acteurs économiques et institutionnels, la France s'est dotée d'une stratégie nationale pour la Cybersécurité, dans le cadre du plan d'investissement France 2030. Les objectifs poursuivis sont : tripler le chiffre d'affaires de la filière d'ici 2025, former plus de professionnels et développer des solutions souveraines alors que les enjeux en matière de cybersécurité sont toujours plus prégnants.

Objectifs
Financé à hauteur de 65 millions d'euros sur 8 ans, le programme de recherche (PEPR) Cybersécurité soutient des activités de recherche fondamentale au meilleur niveau mondial. Les résultats issus de ce programme nourrissent les actions plus aval de cette stratégie nationale comme le Programme de Transfert au Campus Cyber (PTCC), l'incubateur CyberBooster, le Grand Défi Automatisation de la Cybersécurité, les appels à projet Développement de Technologies Innovantes Critiques, entre autres. Lancé officiellement en Juin 2022, ce PEPR vise plus spécifiquement à :

• Lancer et financer des défis scientifiques en recherche fondamentale ;
• Structurer des communautés de recherche ;
• Obtenir des avancées scientifiques en cybersécurité ;
• Faire émerger des technologies de rupture bénéficiant à l'ensemble des acteurs français de la filière.

Une gouvernance partagée, une communauté académique mobilisée

Mené en étroite collaboration avec la communauté nationale de la recherche, son pilotage scientifique a été confié au CEA, au CNRS et à Inria.

Le cadrage de ce PEPR a bénéficié d'une grande mobilisation de l'ensemble de la communauté scientifique et des grands acteurs étatiques et socioéconomiques. Il mobilise désormais déjà plus d'une vingtaine d'universités et grandes écoles, représentant au total 300 chercheuses et chercheurs.

Afin de favoriser la valorisation des savoirs, technologies et outils développés dans le PEPR Cybersécurité ainsi que les synergies avec les autres actions de la stratégie nationale pour la cybersécurité mais aussi avec les autres stratégies d'accélération (Quantique, IA, Cloud, Réseaux du futur, TASE, Santé numérique), le PEPR Cybersécurité s'est doté d'une gouvernance. Celle-ci a pour ambition d'impliquer au mieux les acteurs socioéconomiques dans la définition de sa stratégie et dans les actions de dissémination et de communication. Les organes de gouvernance se décomposent comme suit :

• Comité de pilotage (COPIL), en charge du pilotage stratégique du programme
• Direction de programme (CODIR), en charge de la coordination du programme
• Comité de programme (COPROG), en charge de l'animation
• Conseil d'orientation stratégique (COS), composé d'acteurs académiques et socioéconomiques, consulté chaque année pour donner un avis sur le programme et les révisions de la feuille de route.

Présentation des dix projets de recherche lancés depuis 2022 :

• La protection des données personnelles (IPoP)
• La sécurité du traitement des données dans le cloud (SecureCompute)
• La sécurité des protocoles et du vote électronique (SVP)
• La sécurité des données multimédias (COMPROMIS)
• La défense contre les programmes malveillants (DefMal)
• La supervision et l'orchestration de la sécurité (SuperviZ)
• La sécurité matérielle et logicielle des systèmes embarquées (ARSENE)
• L'évaluation de la sécurité des logiciels (SecurEval)
• La résistance des systèmes cryptographiques (Cryptanalyse)
• L'exploitation des vulnérabilités en investigation numérique (REV)

Production, principales retombées et rayonnement du PEPR Cybersécurité

Le « PEPR Cyber Day » est un séminaire scientifique organisé chaque année, afin de présenter aux acteurs industriels et étatiques les derniers résultats issus des projets du programme et d'échanger sur leur valorisation voire leur transfert.

Depuis son lancement en 2022, le PEPR c'est déjà :
• 120 publications scientifiques au meilleur niveau mondial
• 40 doctorants recrutés
• 31 post-doctorants et ingénieurs recrutés
• 37 séminaires scientifiques
• 45 événements à destination du grand public
• 2 startups en cours de création
• 1 financement européen ERC accepté et plusieurs projets Horizon Europe en cours de dépôt
• Des logiciels et plateformes développés,
• 2 chercheuses distinguées par des prix scientifiques : Véronique Cortier (Médaille d'Argent du CNRS 2022), Anne Canteaut (Prix Irène Joliot-Curie 2023).

Pour contacter le PEPR Cybersécurité : contact@pepr-cybersecurite.fr

Pour suivre le PEPR Cybersécurité : www.pepr-cybersecurite.fr

Pour s'inscrire à la newsletter (trimestrielle) du PEPR Cybersécurité : https://evento.renater.fr/survey/newsletter-programme...-b1ixhs1z

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

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

Thales, à travers le rachat de Gemalto en 2019 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, Equans et IBM sont également positionnés sur des offres globales.

6.3.c ...open source...

Certains acteurs proposent des approches clef-en-main avec systèmes propriétaires. Ces approches sont de moins en moins plébiscitées par les clients qui se retrouvent dépendants d'un unique acteur privé pour l'entretien et l'amélioration future des interfaces. En conséquence, le développement de solutions *open source* se développe de plus en plus.

Dans le domaine particulier des systèmes nationaux de gestion d'identité (état civil) opérés par les Etats, la tendance à l'utilisation de solution en *open source* est aussi perceptible. Toutefois une très forte tendance à la modularité en briques fonctionnelles distinctes s'observe également, car les Etats souhaitent éviter d'être dépendants d'un seul et unique fournisseur ou prestataire pour ne pas en être prisonnier. Elle se traduit en particulier par l'utilisation d'API (*Application Programming Interfaces*) standardisées pour chaque brique fonctionnelle, assurant une indépendance complète dans leur conception, tout en permettant leur interconnexion de manière interopérable. Cette tendance se combine à celle de l'*open source*, car les briques fonctionnelles se reposent de plus en plus sur des solutions open sources. Cette problématique de standardisation d'API prend de l'ampleur sur de nombreux sujets, par exemple avec le concept d'*Open-Services Cloud* (OSC) visant à rendre interopérables les services cloud, réduisant la dépendance des utilisateurs cloud vis-à-vis des *hyperscalers* (voir l'étude de DECISION Etudes & Conseil réalisé début 2023 sur le sujet : Open-Services Cloud (OSC) Unlock Cloud interoperability to foster the EU digital market).

6.3.d ... et *As a Service*

En parallèle, on observe à la fin progressive de l'achat simple de produits (logiciels en mode licence, etc.), et le développement de la vente sous forme de service (SaaS: *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. En 2020, la fourniture de logiciels en mode SaaS représentait déjà 40% de la valeur totale du marché européen des logiciels d'entreprises (DECISION Etudes & Conseil, SITSI). Cette proportion croit d'année en année et devrait approcher les 80% à horizon 2030.

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.

A PROPOS DE L'ACN

L'Alliance pour la Confiance Numérique (ACN) est le syndicat professionnel qui représente les entreprises (leaders mondiaux, PME/TPE, et ETI) du secteur de la confiance numérique et notamment celles de l'identité numérique, de la cybersécurité et de l'IA de confiance. La France dispose dans ce domaine d'un tissu industriel très performant et d'une excellence internationalement reconnue grâce à des leaders mondiaux, des PME, des ETI et aux différents acteurs dynamiques du secteur.

On dénombre 2 178 entreprises réalisant en France 19 Milliards d'euros de chiffre d'affaires dans ce secteur en forte croissance (8% de croissance annuelle moyenne depuis 2016).

Les 120 membres de l'Alliance pour la Confiance Numérique (ACN), dont 87% de PME/TPE-ETI, représentent 2/3 du chiffre d'affaires des entreprises françaises de la Confiance Numérique dans le monde (fabricants de matériel, éditeurs de logiciels, intégrateurs, services, laboratoires d'évaluation de sécurité, recherche,...).

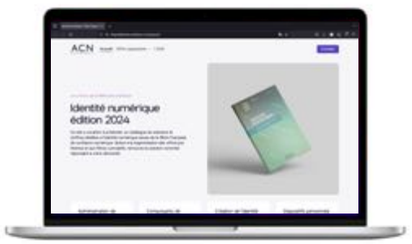
L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication), est membre associé du Campus cyber et participe activement aux travaux du CSF (Comité Stratégique de Filière) des Industries de Sécurité.

Par ailleurs, l'ACN est également membre fondateur de l'association représentant l'écosystème européen de la cybersécurité : ECSO (European CyberSecurity Organisation).

Dernières publications :

Nouveau : L'ACN a lancé un site pour recenser les offres françaises d'identité numérique :

https://identite.confiance-numerique.fr/



ACN
Alliance pour la confiance numérique

@ACN_SecNum ACN - Alliance pour la Confiance Numérique ykassianides@confiance-numerique.fr

Les Membres de l'ACN

Les partenaires de l'ACN

A PROPOS DE DECISION

Depuis 2017, DECISION conduit l'Observatoire de la filière de la Confiance Numérique pour le compte de l'ACN.

DECISION est un cabinet d'études et de conseil spécialisé dans la réalisation d'études économiques (analyse de marchés, prévisions, chaînes de valeur, etc.) et de missions de conseil et de stratégie, dans les domaines :

• Electronique (composants, équipements, systèmes) ;
• Aéronautique, Défense, Sécurité ;
• Electrique, Energies renouvelables et Industrie du future.

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

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

DECISION a également effectué depuis les études d'évaluation du poids économique de la filière de sécurité pour le gouvernement français:

• En 2015 sous l'égide du PIPAME (Pôle Interministériel de Prospective et d'Anticipation des Mutations Economiques), structure inter-ministérielle regroupant le Ministère de l'Economie (DGE), le Ministère de l'Intérieur (DMISC) et le SGDSN.
• En 2018 sous l'égide du CoFIS (Comité de la Filière Industrielle de sécurité), regroupant le Ministère de l'Economie (DGE), le Ministère de l'Intérieur (DMISC), le SGDSN, le CICS (Conseil des Industries de la Confiance et de la Sécurité), le GICAT et Milipol.
• En 2020 sous l'égide du Conseil Stratégique de Filière (CSF) des Industries de Sécurité, regroupant le Ministère de l'Economie (DGE), le Ministère de l'Intérieur (DMISC), le SGDSN, le CICS (Conseil des Industries de la Confiance et de la Sécurité), et le GICAT.
• En 2022, à travers un consortium regroupant le GICAT, l'ACN, le Ministère de l'Intérieur, le Ministère de l'Economie (DGE) et le SGDSN.

DECISION
ETUDES & CONSEIL

www.decision.eu

ACN
Alliance pour la confiance numérique

www.confiance-numerique.fr

Observatoire de la filière
de la confiance numérique 2024

Design graphique / Theo Broyer Alran & Arthur Pajaud.

English Version Available on :
www.confiance-numerique.fr

Partenariat presse