2025

confiance-numerique.fr

Observatoire de la Filière de la Confiance Numérique

ACN

ACN

Alliance pour la confiance numérique

Observatoire de la Filière de la Confiance Numérique

2025

achevé d'imprimer en mai 2025

SOMMAIRE

ACN
Alliance pour la confiance numérique

LE MOT DE L'ACN
ALLIANCE POUR LA CONFIANCE NUMÉRIQUE

Daniel Le Coguic
Président de l'ACN

À l'occasion de la publication de cette 11e édition de l'Observatoire ACN, il est essentiel de prendre un moment pour réfléchir ensemble à l'avenir de notre filière de la confiance numérique.
Ce document de référence constitue, par l'ensemble des données qu'il propose, une boussole stratégique incontournable pour appréhender le rôle de notre filière dans le monde actuel.

Le contexte économique et géopolitique actuel nous impose des défis considérables, mais il nous offre également des opportunités uniques pour défendre nos valeurs et renforcer notre souveraineté. Le monde traverse une période de tensions exacerbées. Les conflits armés, y compris sur le sol européen, les guerres commerciales et l'utilisation des droits de douane comme outils diplomatiques, la balkanisation du cyberespace, le développement exponentiel de l'empreinte numérique dans la société sont autant de signes d'un monde en mutation rapide.
Ces bouleversements géopolitiques et cette mutation numérique ont des répercussions directes sur notre économie et notre capacité à nous projeter dans le futur. Cependant, ces défis ne doivent pas nous décourager. Au contraire, ils doivent nous inciter à redoubler d'efforts pour transformer cette situation en levier d'opportunités pour notre filière et pour notre pays.

La confiance numérique est un pilier essentiel de nos sociétés modernes. Elle est devenue un sujet éminemment politique, au cœur des réflexions stratégiques de nos entreprises, de nos institutions et de nos citoyens. La nécessité de réduire nos dépendances, de renforcer notre souveraineté numérique et notre autonomie stratégique est plus évidente que jamais. Les entreprises de notre filière, qu'elles soient spécialisées dans l'identité numérique, la cybersécurité, la blockchain, les infrastructures de confiance ou l'IA de confiance, ont un rôle crucial à jouer dans ces défis.

Dans chacun de ces domaines, nous vivons des évolutions majeures. L'identité numérique, qui est la pierre angulaire de la confiance dans le numérique, connaîtra prochainement une accélération importante sous l'impulsion de la mise en œuvre du projet de portefeuille d'identités numériques de l'Union européenne.

« La confiance numérique est un pilier essentiel de nos sociétés modernes. »

Concernant la cybersécurité, le projet de loi « Résilience » qui transpose notamment les textes européens REC, NIS2 et DORA, sera également au cœur du renforcement de notre sécurité et de notre résilience collective, action indispensable au regard de l'explosion des menaces que nous constatons quotidiennement. La filière travaille main dans la main avec les pouvoirs publics, mais aussi avec les parlementaires et les territoires pour faire en sorte que ce texte de loi fondateur atteigne ses objectifs mais permette aussi de capitaliser fortement sur les solutions françaises et européennes d'excellence. En effet, si l'objectif premier du texte est la résilience générale de la Nation, celle-ci doit impérativement se doubler du renforcement de notre filière et de notre autonomie stratégique par la mise en place une véritable politique industrielle ambitieuse, nous permettant de réduire notre dépendance aux outils numériques extra-européens et reprendre en main notre avenir numérique.

L'intelligence artificielle, enfin, occupe de plus en plus, une place centrale dans les enjeux de confiance numérique. Le gouvernement ne s'y est pas trompé et a organisé l'AI Summit en février, plaçant ainsi la France au cœur des débats mondiaux dans ce domaine. L'ACN a contribué, lors de cet évènement, à replacer l'IA dans une logique de confiance : la compréhension accrue du besoin de souveraineté numérique et les projecteurs braqués sur ce thème nous incitent à travailler ensemble pour créer des référentiels communs juridiques, techniques et éthiques. Un code de conduite de la filière est en cours d'élaboration et sera prochainement rendu public. L'évolution de notre Observatoire, qui, dans cette édition 2025 intègre désormais pleinement l'IA de confiance dans sa segmentation, traduit cette nécessité de mieux observer, mesurer et comprendre l'évolution de ce domaine.

L'efficacité de nos actions repose sur une bonne coordination et la suppression des redondances. Le rapprochement entre l'ACN et l'Alliance Blockchain France, intervenu en début d'année, en constitue un exemple concret et a permis de créer un périmètre d'action plus cohérent, d'activer des synergies nombreuses et de rendre nos actions plus audibles mais aussi compréhensibles. Il est essentiel de poursuivre ce mouvement de rationalisation et de lisibilité des actions dans l'écosystème de la confiance numérique. En respectant les ADN de chaque structure, il nous appartient de créer une représentation institutionnelle unifiée. Ce type de rapprochement est un signal fort de la maturité de notre écosystème. Ce mouvement se double de la mise en place de passerelles d'échanges avec nos partenaires européens : dans la lignée du partenariat mise en place par l'ACN avec ses homologues allemands l'année dernière, plusieurs autres démarches similaires sont en cours de finalisation avec d'autres partenaires membres de l'UE.

En 2025, nous devons reprendre le contrôle sur le cours des événements. Que ce soit sur le plan géostratégique, social, économique ou technologique, la confiance numérique est le dénominateur commun de tous ces enjeux. Elle est l'outil de la préservation de notre modèle de société fondé sur des valeurs de démocratie et de liberté. L'ACN a l'honneur et le privilège d'assurer, en France, la représentation institutionnelle de cette filière stratégique.

Les défis sont nombreux, mais l'optimisme est de mise. Cette année sera, à n'en pas douter, une année charnière pour la confiance numérique. Plus que jamais, c'est ensemble que nous devons construire notre avenir et transformer les incertitudes en opportunités pour la France et l'Europe. La filière industrielle française de la confiance numérique doit être le fer de lance de notre souveraineté technologique et de notre indépendance stratégique.

« La nécessité de réduire nos dépendances, de renforcer notre souveraineté numérique et notre autonomie stratégique est plus évidente que jamais »

LE MOT DE LA MINISTRE

Clara CHAPPAZ

Ministre déléguée chargée
de l'Intelligence Artificielle
et du Numérique

À l'heure où les rapports de force mondiaux se recomposent sous l'effet de tensions géopolitiques accrues, l'intelligence artificielle s'impose comme une technologie de rupture majeure. Porteuse d'un potentiel de transformation inégalé, elle est aussi source de défis considérables. Le Gouvernement a pleinement saisi l'importance de cette révolution technologique pour renforcer notre souveraineté numérique, améliorer l'action publique et mieux protéger nos concitoyens.

L'IA est bien plus qu'un progrès technique : elle redéfinit nos usages, nos métiers, nos compétences. Et elle le fait à une vitesse inédite. L'irruption de l'IA générative dans nos quotidiens illustre cette accélération : en quelques mois, elle a bouleversé nos repères. Il est donc essentiel que l'État joue son rôle pour guider, encadrer et canaliser cette révolution, afin qu'elle soit alignée avec nos valeurs fondamentales. C'est tout le sens de la création d'un ministère de plein exercice dédié au Numérique et à l'IA : affirmer que l'État doit être présent là où se joue notre avenir.

Depuis 2018, la France a bâti une stratégie nationale d'intelligence artificielle claire, structurée autour de quatre piliers : l'excellence en recherche, le soutien à l'innovation, l'adoption dans l'économie réelle et la promotion d'une IA éthique et fiable. Cette stratégie s'est appuyée sur plus de 3 milliards d'euros d'investissement, et elle porte aujourd'hui ses fruits : la France est devenue le *leader* européen de l'IA, avec près de 2 milliards d'euros levés en 2024 et plus d'un millier de start-ups actives dans le domaine. Des acteurs comme Mistral, LightOn ou Preligens font désormais rayonner notre expertise à l'échelle mondiale.

Le Sommet pour l'Action sur l'IA, que nous avons organisé en février dernier, a permis d'inscrire cette ambition dans une dynamique internationale. Avec la création de la Coalition pour une IA durable ou encore de la Fondation pour une IA d'intérêt général, nous avons lancé une nouvelle phase de notre stratégie nationale autour de trois grandes priorités :

- Accélérer la diffusion de l'IA ;
- Renforcer notre souveraineté technologique ;
- Et prévenir les excès liés à ces technologies.

« la France est devenue le *leader* européen de l'IA, avec près de 2 milliards d'euros levés en 2024 et plus d'un millier de start-ups actives dans le domaine »

Ces priorités structurent mon action quotidienne.

La première d'entre elles – la diffusion de l'IA – implique une montée en compétences collective. L'IA ne doit pas rester l'affaire des seuls experts. Elle doit devenir un levier d'innovation, de productivité et de simplification pour l'ensemble des organisations. Dans l'administration, nous investissons massivement aux côtés de la DINUM pour développer des solutions concrètes comme le programme Albert ou l'incubateur Alliance, qui bâtissent les services publics numériques de demain.

Notre souveraineté numérique est l'autre grand défi. Aujourd'hui, une trop grande part de nos infrastructures numériques dépend d'acteurs étrangers. Cette dépendance nous expose à des risques majeurs. La souveraineté ne signifie pas le repli : elle signifie le choix. Nous devons pouvoir décider de nos outils, de nos standards, de nos valeurs. Cela suppose de maîtriser nos capacités de calcul, de soutenir nos industriels, et de former massivement aux compétences du numérique.

Enfin, cette souveraineté serait incomplète sans une vraie politique de protection numérique. Si l'IA est un formidable levier d'innovation, elle peut aussi être un facteur de dérives : désinformation, violences numériques, addiction. Ces risques, qui touchent d'abord les plus jeunes, nous imposent d'agir. La loi SREN apporte déjà des réponses pour mieux encadrer les plateformes et protéger les mineurs.

Le projet de loi Résilience numérique, quant à lui, viendra renforcer les exigences de cybersécurité dans tous les services publics.

Vous le savez mieux que quiconque : la confiance numérique n'est pas une option, elle est une condition de réussite. Elle repose sur un écosystème solide, engagé, et structuré. C'est ce que représente votre filière, que je souhaite saluer ici pour son rôle essentiel dans la sécurisation et l'éthique de notre transition numérique.

Plus que jamais, le numérique est un levier de souveraineté, et l'intelligence artificielle, un enjeu de société. Ensemble, nous devons faire en sorte qu'il soit aussi un vecteur de progrès partagé. L'État sera à vos côtés pour relever ce défi.

« Aujourd'hui, une trop grande part de nos infrastructures numériques dépend d'acteurs étrangers. Cette dépendance nous expose à des risques majeurs. »

- Les principaux segments de la confiance numérique en 2024
- Fondamentaux 2024
- Croissance France comparée 2017- 2024
- Répartition par taille d'entreprises 2024
- Top acteurs 2024

ÉLÉMENTS CLEFS

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

L'Alliance pour la Confiance Numérique (ACN) a été constituée pour regrouper et soutenir les acteurs de cette filière en France et en assurer leur 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 2025, couvrant le champ de la cybersécurité, de la sécurité numérique et pour la première fois, celui de l'IA.

La confiance numérique en France en 2024 c'est :

- **21,3 milliards d'euros de chiffre d'affaires,** soit 6,2% de croissance entre 2023 et 2024,
- **10 milliards d'euros** de valeur ajoutée,
- **107 000 personnes employées** dans le secteur,
- **un chiffre d'affaires** réparti à **53% pour la cybersécurité**, à **40% pour la sécurité numérique,** et à **7% pour l'IA de confiance.**

Les entreprises françaises de la confiance numérique dans le monde en 2024 c'est :

- **33,5 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).

- **17 milliards d'euros de chiffre d'affaires à l'international,** soit 51 % du CA total (CA exporté depuis la France et CA réalisé à l'étranger par des entreprises détenues par des capitaux français).

- **6,1 milliards d'euros de chiffre d'affaires à l'exportation depuis la France,** soit un taux d'export moyen de 29%.

La confiance numérique est une filière à part entière :

- **7% de croissance moyenne annuelle** en France sur la période 2018-2024, contre 0,8% 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.

21,3 milliards d'euros de chiffre d'affaires en France

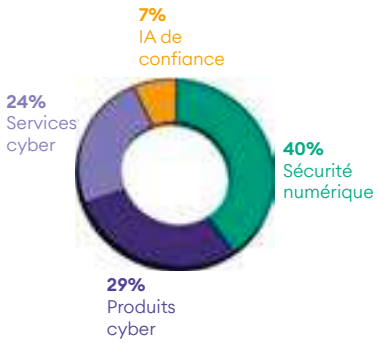
33,5 milliards d'euros de chiffre d'affaires à l'international

107 000 personnes employées en France

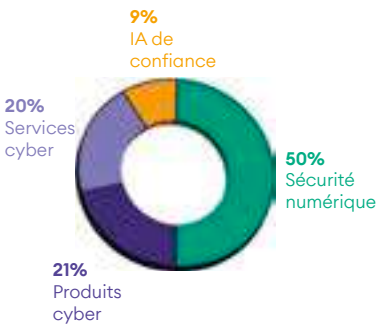
6,2% de croissance en France en 2024

Les principaux segments de la confiance numérique en 2024

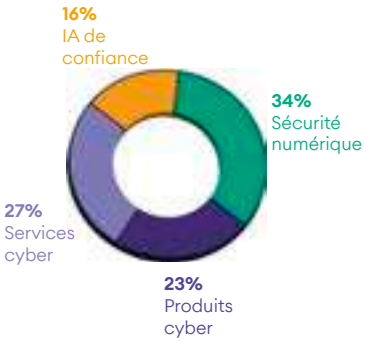
• Chiffre d'affaires



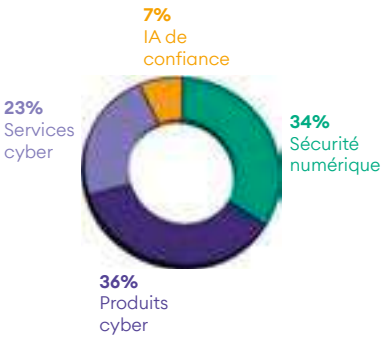
• Nombre d'entreprises



• Effectifs



• Valeur ajoutée



2 499 entreprises
dans la filière en France

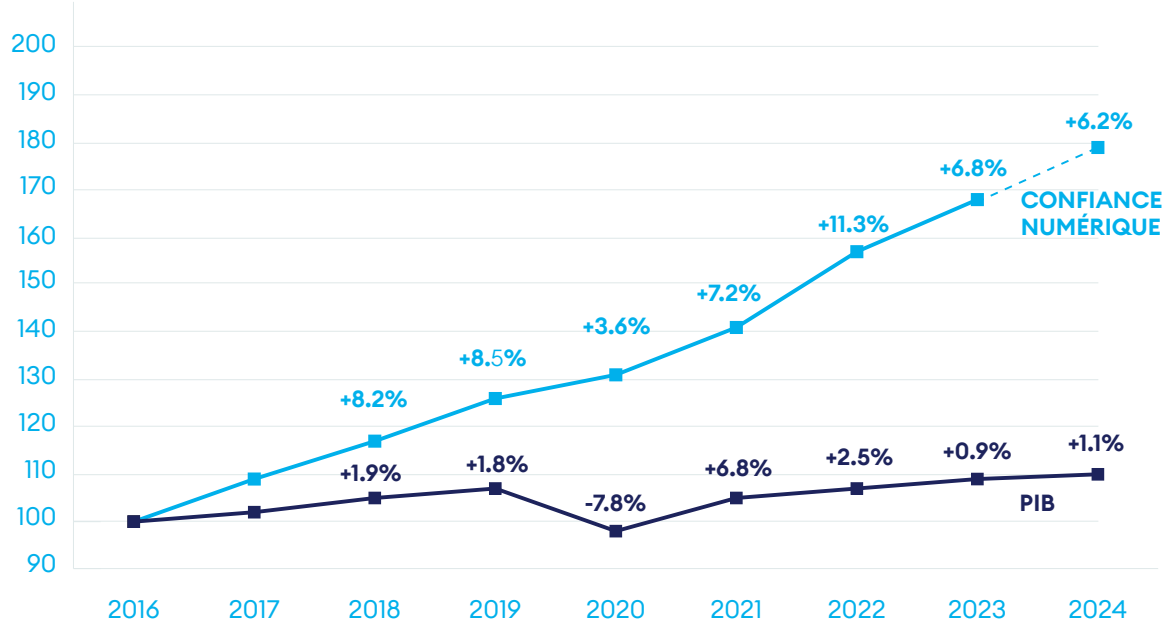
La confiance numérique est un écosystème d'entreprises de toutes tailles :

- **75 grandes entreprises ,**
- **72 ETI** (Entreprises de Taille Intermédiaire),
- **749 PME** (Petites et Moyennes Entreprises),
- **1 603 micro-entreprises.**

Fondamentaux 2024

CA Monde	**33.5 MDS €**
CA Hors de France	**12.1 MDS €**
CA France	**21.3 MDS €**
	dont export **6.1 MDS €**
Valeur ajoutée France	**10 MDS €**

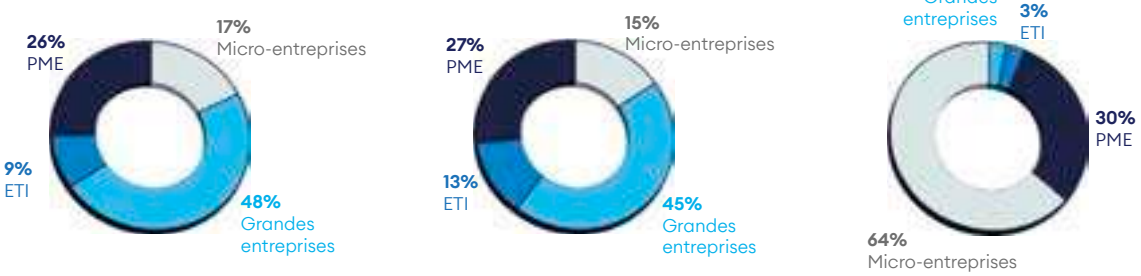
Croissance France comparée 2017- 2024



Base 100 en 2016

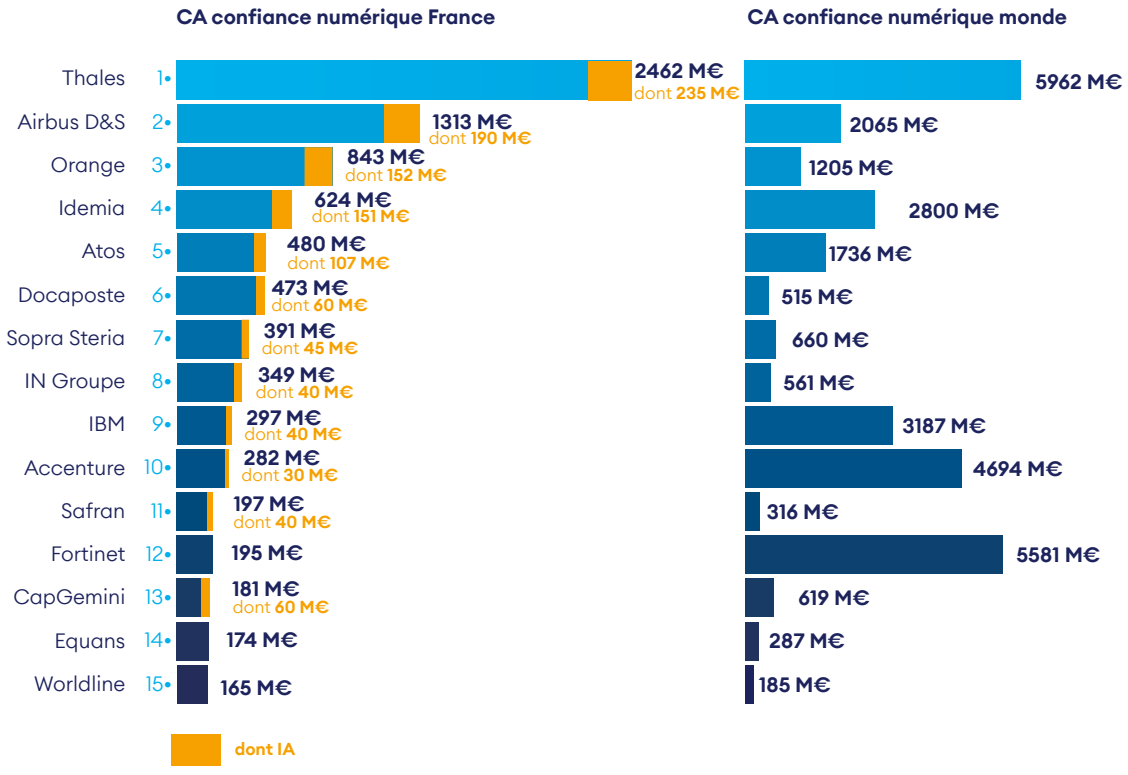
Croissance du PIB mesurée par l'INSEE, et par le FMI en 2024
Cette croissance ne prend pas en compte la croissance dans l'IA de confiance

Répartition par taille d'entreprises 2024



Chiffre d'affaires | **Effectifs** | **Nombre d'entreprises**

Top 15 acteurs France 2024



*** Note :** L'édition 2025 de l'Observatoire introduit un élargissement du périmètre d'analyse avec l'ajout du segment IA de confiance. Ce changement structurel a conduit à un réajustement des chiffres d'affaires associés aux entreprises concernées, impactant notamment leur classement dans le Top 15. Plusieurs groupes bénéficient ainsi de l'intégration de leurs activités en IA de confiance, à l'image de Thales, Airbus, Orange, Atos ou Idemia. Par ailleurs, certaines données ont été actualisées à la suite de nouvelles publications financières, notamment pour des entreprises dont les comptes n'étaient pas disponibles les années précédentes, comme c'était le cas d'Orange Cyberdéfense. Enfin, une part des activités relevant de l'IA de confiance a été réaffectée depuis d'autres segments existants. Pour l'ensemble de ces raisons, les résultats 2025 ne sont pas directement comparables à ceux des éditions antérieures.

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, et Imperva et Tesserent en 2023.

• **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 (Arismore, etc.).

• **Thales** comprend Gemalto et Ercom.

• **Ates** 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…

• **Chapsvision / Flandrin** technologies comprend Deveryware, Bertin IT, Vecsys, Elektron et Geotrend.

• **Idemia** comprend Otono networks.

• **IN Groupe** comprend Surys et Nexus.

• **Econocom** comprend Exaprobe.

• **Worldline** comprend Ingenico.

• **GFI Informatique** comprend SIS.

• **Cisco** comprend Sentryo.

• **Sogetrel** comprend Eryma.

Top 1-10 acteurs France

Top 11-20 acteurs France

CA confiance numérique France compris entre 125 M€ et 200 M€

Top 21-50 acteurs France

CA confiance numérique France compris entre 60 M€ et 120 M€

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

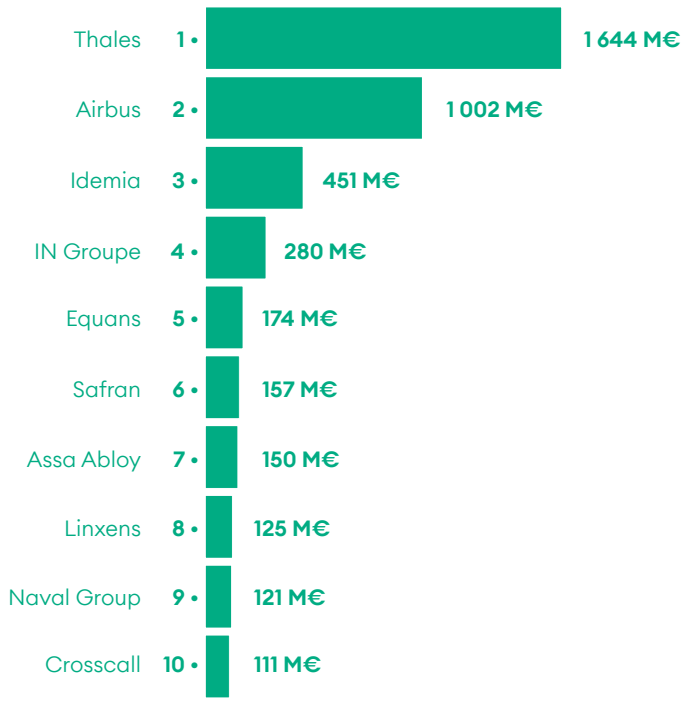
Parmi les acteurs situés entre la 10ème et la 20ème position et réalisant en CA confiance numérique supérieur à 125M€ depuis la France en 2024, on trouve des acteurs français tels que Cap Gemini, Nomios et I-Tracing (services cyber), Worldline (sécurité des paiements), Safran (dont IA spécifique), et Equans (sécurité numérique), 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 60 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.

FOCUS

Segment Sécurité numérique



• Croissance 2023-2024
+4%

• Chiffre d'affaires
8 493 M€

• Emplois
36 212

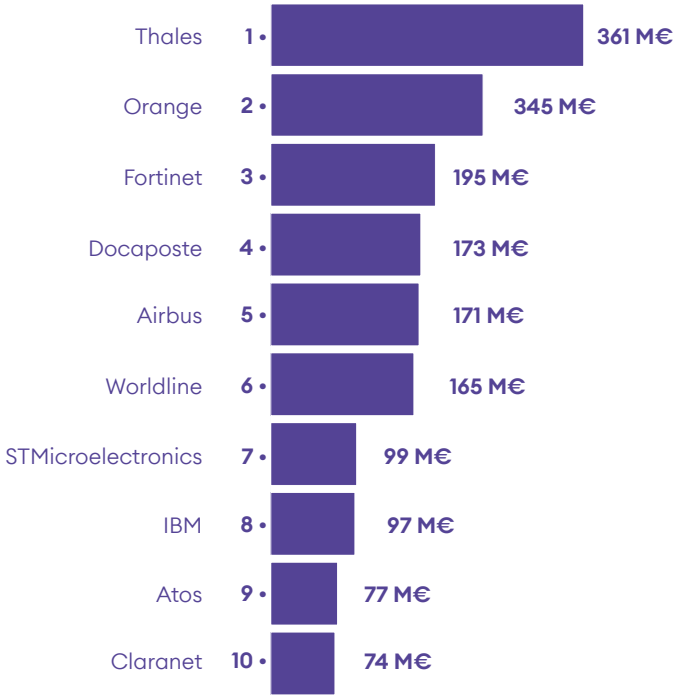
• Nombre d'entreprises
1 770

• Valeur ajoutée
3 410 M€

	Chiffre d'affaires M€	Emplois	Nombre d'entreprises	Valeur ajoutée M€
Systèmes et contrôle d'accès électronique	1 804	7 084	331	672
Identification et authentification des personnes	2 457	10 123	509	966
Observation et détection large zone	564	2 346	191	301
Traçage et localisation	621	2 631	221	233
Communications sécurisées	1 809	7 557	318	682
Commande, contrôle et aide à la décision	772	3 449	274	357
Renseignement et collecte d'informations	466	3 020	234	199

FOCUS

Segment Produits et solutions de cybersécurité



• Croissance 2023-2024
+9,2%

• Chiffre d'affaires
6 188 M€

• Emplois
24 641

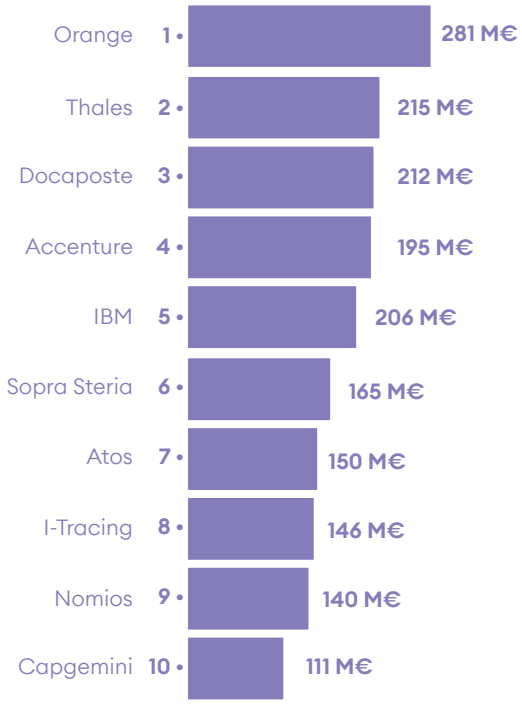
• Nombre d'entreprises
739

• Valeur ajoutée
3 627 M€

	Chiffre d'affaires M€	Emplois	Nombre d'entreprises	Valeur ajoutée M€
Gouvernance cyber	1 021	5 203	225	585
Gestion des identités et des accès	932	3 094	214	594
Sécurité des données	1 897	7 063	352	1 144
Sécurité des applications	397	1 474	172	274
Sécurité des infrastructures numériques	1 540	6 265	358	874
Sécurité des produits et équipements	401	1 542	162	157

FOCUS

Segment Services de cybersécurité



• Croissance 2023-2024
+6,6%

• Chiffre d'affaires
5 036 M€

• Emplois
29 271

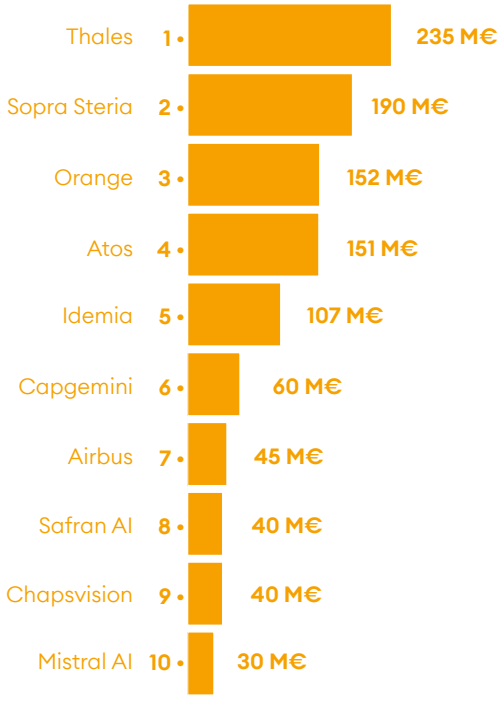
• Nombre d'entreprises
717

• Valeur ajoutée
2 332 M€

	Chiffre d'affaires M€	Emplois	Nombre d'entreprises	Valeur ajoutée M€
Audit, planning et conseil cyber	2 189	13 147	670	898
Mise en oeuvre cyber	1 614	9 938	468	699
Sécurisation de l'infogérance et exploitation	1 119	5 121	362	666
Formation en cybersécurité	115	106	205	69

FOCUS

Segment IA de confiance



• Croissance 2023-2024
+9,3%

• Chiffre d'affaires
1 586 M€

• Emplois
17 206

• Nombre d'entreprises
315

• Valeur ajoutée
730 M€

	Chiffre d'affaires M€	Emplois	Nombre d'entreprises	Valeur ajoutée M€
IA à usage général	284	3 080	125	131
IA spécifique	1 302	14 126	257	599

1. CONFIANCE NUMÉRIQUE

1.1 CYBERSÉCURITÉ, SÉCURITÉ NUMÉRIQUE ET IA DE CONFIANCE : TROIS 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).

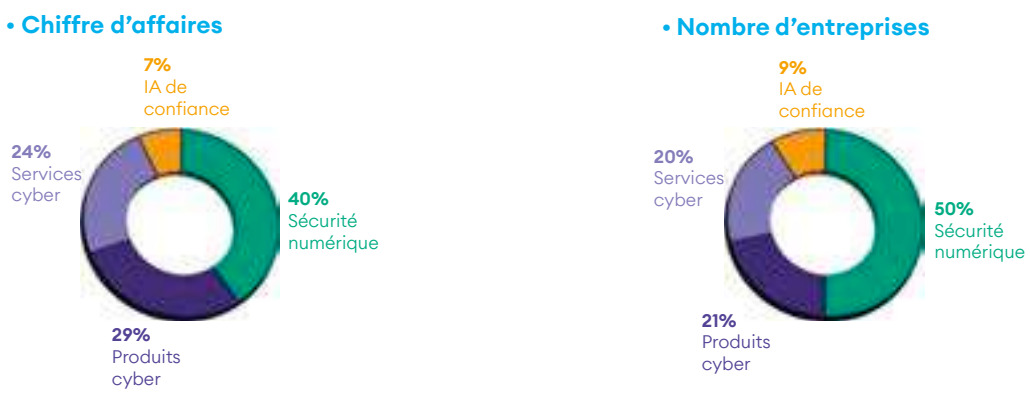
L'Observatoire de la confiance numérique couvre trois industries :

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

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

• **L'IA de confiance**, c'est-à-dire l'intelligence artificielle conçue et déployée selon des critères juridiques, techniques et éthiques exigeants. Elle repose sur des principes tels que la transparence, l'explicabilité, la robustesse, la sécurité, la maîtrise humaine et le respect de la vie privée. Elle inclut également une dimension de souveraineté, en se concentrant sur les solutions développées par des acteurs français. L'IA de confiance recouvre à la fois des modèles génératifs (LLM, SLM, IAG...) utilisés pour produire des contenus ou assister l'utilisateur (chatbot, recommandation, résumé automatique...), et des modèles spécifiques, développés pour des tâches ciblées (extraction d'informations, traitement de l'image ou de la voix, détection de fraude, maintenance prédictive, cybersécurité, etc.), en fonction des besoins métiers et des types de données traitées.

CA et nombre d'entreprises en 2024

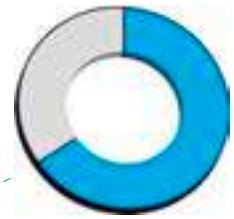


L'ACN est au coeur de la filière

Parmi les adhérents de l'ACN, on trouve :

• 15 grandes entreprises ou ETI, parmi lesquelles les 9 *leaders* français de la confiance numérique.
• Mais aussi 92 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

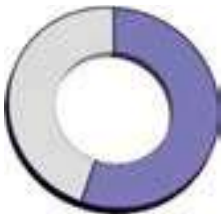


65%
Du CA des entreprises françaises dans le monde

17.3 MDS €
en 2024

82%
Du CA des entreprises françaises dans le monde en sécurité numérique

95%
Du CA des entreprises françaises dans le monde en IA de confiance



55%
Du CA des entreprises françaises dans le monde en cybersécurité

81%
Du CA réalisé à l'international par les entreprises françaises

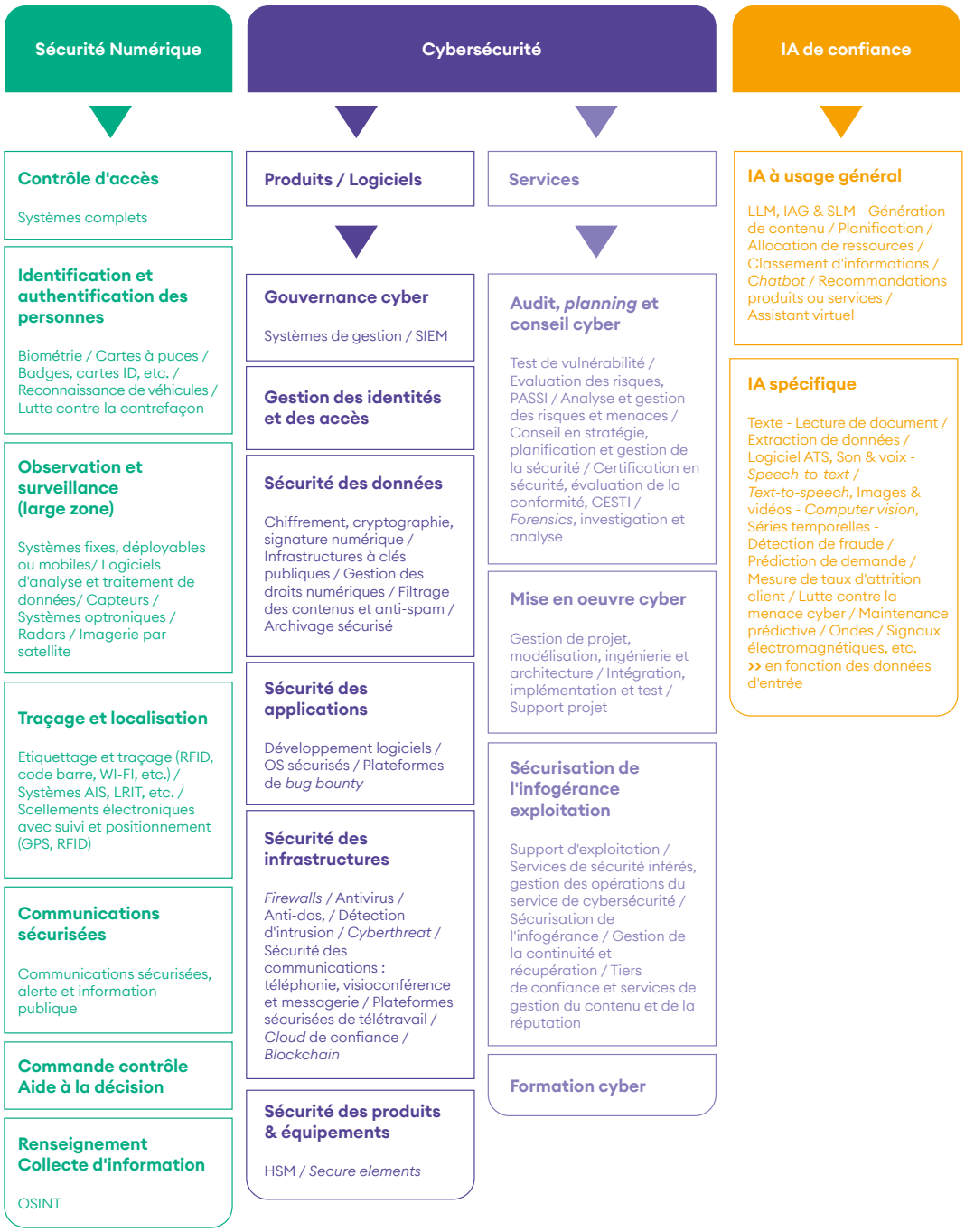
12.6 MDS €
en 2024

1.2 LE PÉRIMÈTRE DE LA CONFIANCE NUMÉRIQUE : SEGMENTATION

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

- **La sécurité numérique**, correspondants aux systèmes ou sous-systèmes électroniques de confiance ;
- **Les produits de cybersécurité**, correspondant au développement de logiciels de cybersécurité ;
- **Les services de cybersécurité**, correspondant aux services d'audit, de conseil, et de mise en oeuvre de produits cyber, de sécurisation de l'infogérance ou de formation cyber ;
- **L'IA de confiance**, correspondant à l'IA à usage général ou l'IA spécifique développée en France selon des critères de confiance.

Périmètre de la confiance numérique



1.3 MÉTHODOLOGIE

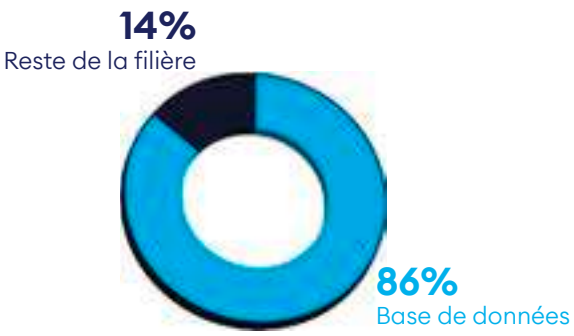
L'objectif de l'Observatoire de la filière de la confiance numérique est à la fois de définir le périmètre de la filière et d'en évaluer le poids économique et les caractéristiques.

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 985 entreprises parmi les 2 499 que compte la filière de la confiance numérique. Cette base de données prend en compte :

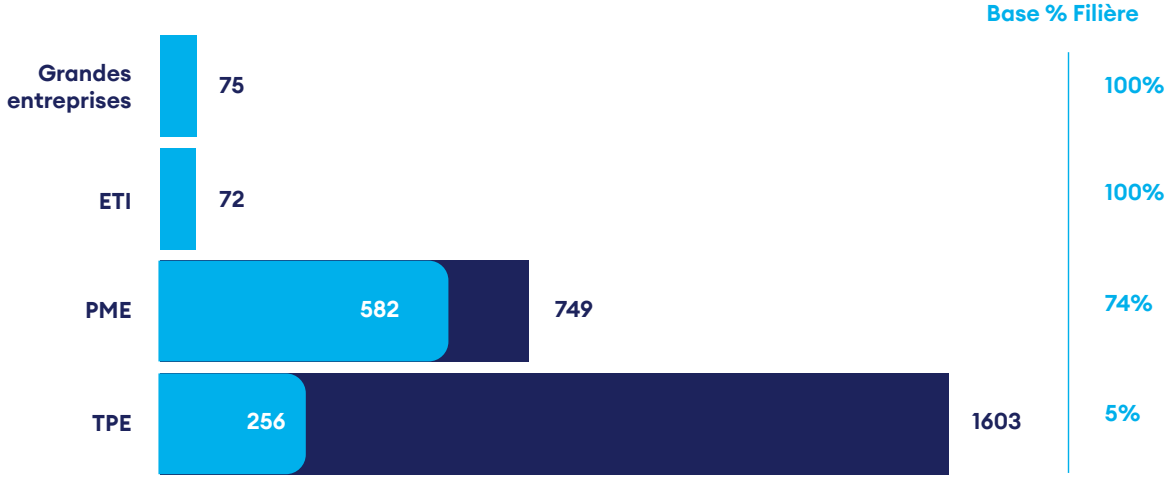
- La totalité des grandes entreprises de la filière (75/75) ;
- La totalité des entreprises de tailles intermédiaires (ETI) de la filière (72/72) ;
- La majorité des petites et moyennes entreprises (PME) de la filière (582/749) ;
- Les très petites entreprises (TPE) et *startups* les plus remarquables et innovantes (256/1603).

Ainsi, bien que seul 39% des entreprises de la filière soient prises en compte dans la base de données, celle-ci est représentative de 86% du chiffre d'affaires total de la filière de confiance numérique France.

Chiffre d'affaires



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 2015-2024 :** 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 19 segments de l'ACN. 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.
À 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 2025, les membres ayant répondu au questionnaire représentent 5% 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 Observatoires

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 2024 et en fonction de la nouvelle segmentation des acteurs. Les chiffres 2023 actualisés sont présentés dans les sections suivantes.

2. UNE FILIÈRE IMPORTANTE ET DYNAMIQUE

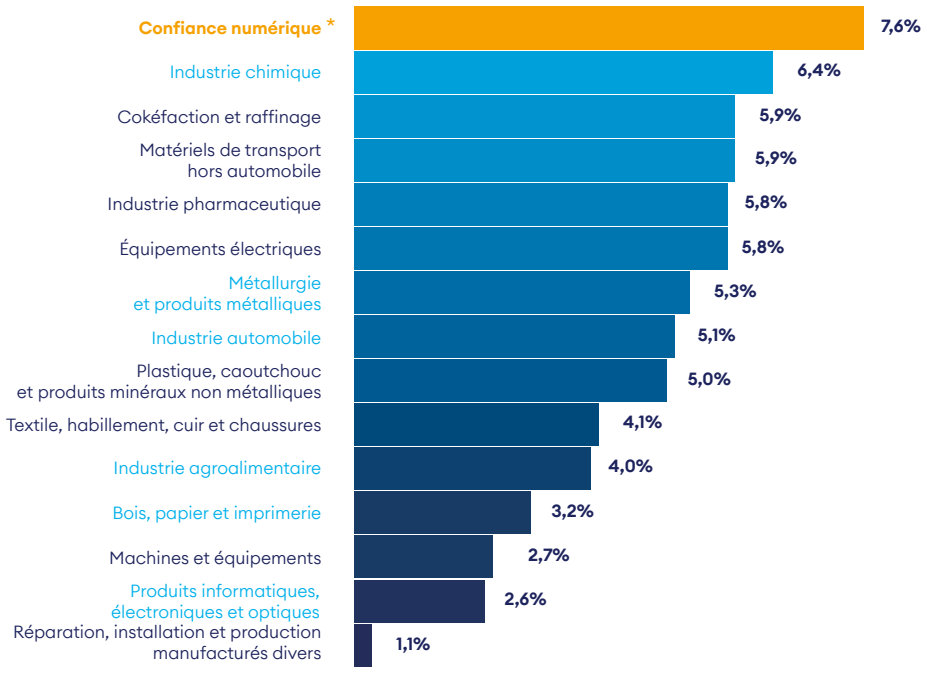
2.1 LA FILIÈRE FRANÇAISE AVEC LA PLUS FORTE CROISSANCE SUR LA PÉRIODE 2016-2023

Sur la période 2016-2023, la confiance numérique est la filière industrielle française qui bénéficie du plus fort taux de croissance, avec 7,6%/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 au dessus de 5% sont l'industrie chimique, la cokéfaction & raffinage, l'industrie pharmaceutique, l'industrie des équipements électriques, les matériels de transport hors automobile, l'industrie de la métallurgie et produits métalliques, ainsi que l'industrie automobile.
Les autres industries bénéficient d'une croissance annuelle moyenne entre 0% et 5% sur la même période.

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 à 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 2016-2023



LÉGENDE

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

---- 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, Observatoire de la confiance numérique
Source : DECISION, basé sur des données Eurostat de 2016 à 2023

2.2 UNE DES FILIÈRES DONT L'ACTIVITÉ EST LA PLUS CRÉATRICE DE RICHESSE EN FRANCE

La confiance numérique est la deuxième 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 deuxième le plus élevé, à 1% de la première position. 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.

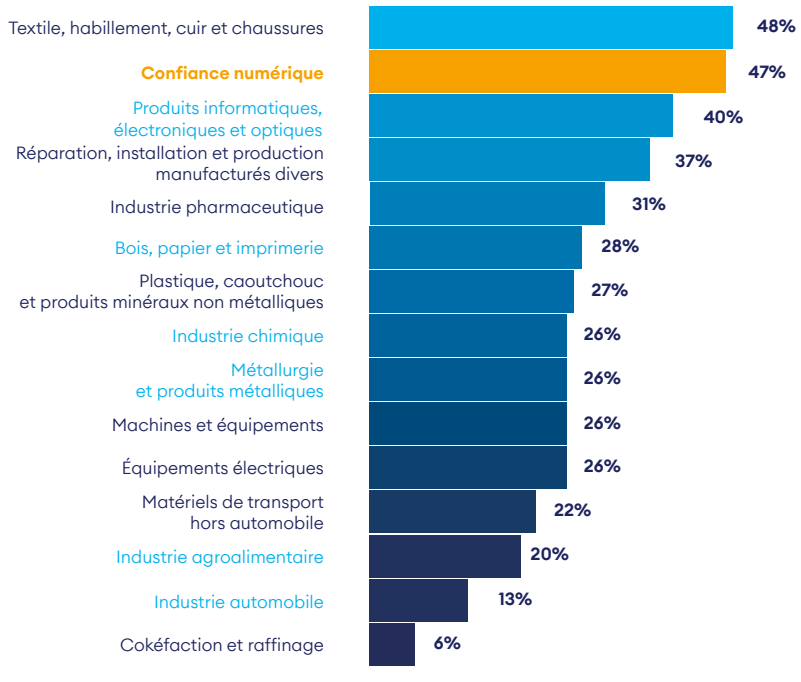
Ce phénomène s'explique principalement par trois facteurs :

1. **Le pourcentage de l'activité dédiée aux services est relativement élevé dans la filière française de confiance numérique** (24% en 2024), 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 40% du chiffre d'affaires total de la filière de la confiance numérique. Or, 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.). Étant 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 29% 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).

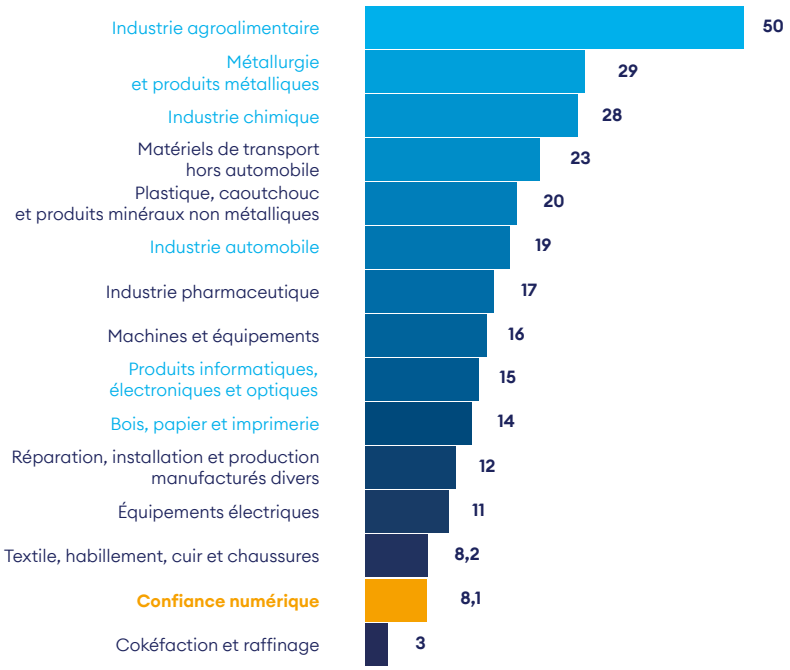
Taux de valeur ajoutée (VA/CA) des filières françaises en 2022



2.3 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. En termes d'emploi, elle dépasse largement la filière de cokéfaction et se rapproche de l'industrie pharmaceutique.

Valeurs ajoutées des filières françaises en 2022 (MDS €)



Emplois des filières françaises en 2022 (en milliers)

Source : DECISION, Eurostat, OCDE

2.4 LES ACTEURS FRANÇAIS SONT EN POINTE EN MATIÈRE DE COMPÉTENCES ET DE R&D

Grâce, notamment, à l'excellence française en matière de recherche et développement, la grande majorité des entreprises françaises de la confiance numérique 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.
La France voit également l'émergence de fleurons dans l'IA générative, à l'instar de Mistral AI devenue licorne française. Sur l'IA spécifique, la France bénéficie d'un large écosystème d'entreprises qui proposent des solutions métiers à différents marchés (santé, assurance, logistique, etc.).
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*.
• Cryptographie : La France fait historiquement partie des *leaders* mondiaux et maintient sa position.

• Technologies post-quantiques (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.
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 UNE CROISSANCE QUI 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. À 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 digitale. Accélérée par la crise du COVID en 2020, les entreprises et administrations du monde entier digitalisent 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, laquelle a notamment pour objectif de devenir un *leader* mondial du semi-conducteur, en production et en innovation, dans un futur proche.
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, ordinateurs quantiques, 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 15,8 milliards d'euros en 2024. 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 2024 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 (États-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.

On note toutefois quelques acquisitions ciblées de plus petite taille, à l'image de Hornetsecurity – entreprise allemande à capitaux américains – qui a racheté en l'espace d'un an deux entreprises françaises spécialisées dans la sécurisation des emails, Vade et Altospam.

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 (0,8%/an de croissance du PIB français sur la période 2018-2024), 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 UNE FILIÈRE À TRÈS FORT POTENTIEL SI LES BONS CHOIX STRATÉGIQUES SONT RÉALISÉS

La confiance numérique est une filière stratégique car :

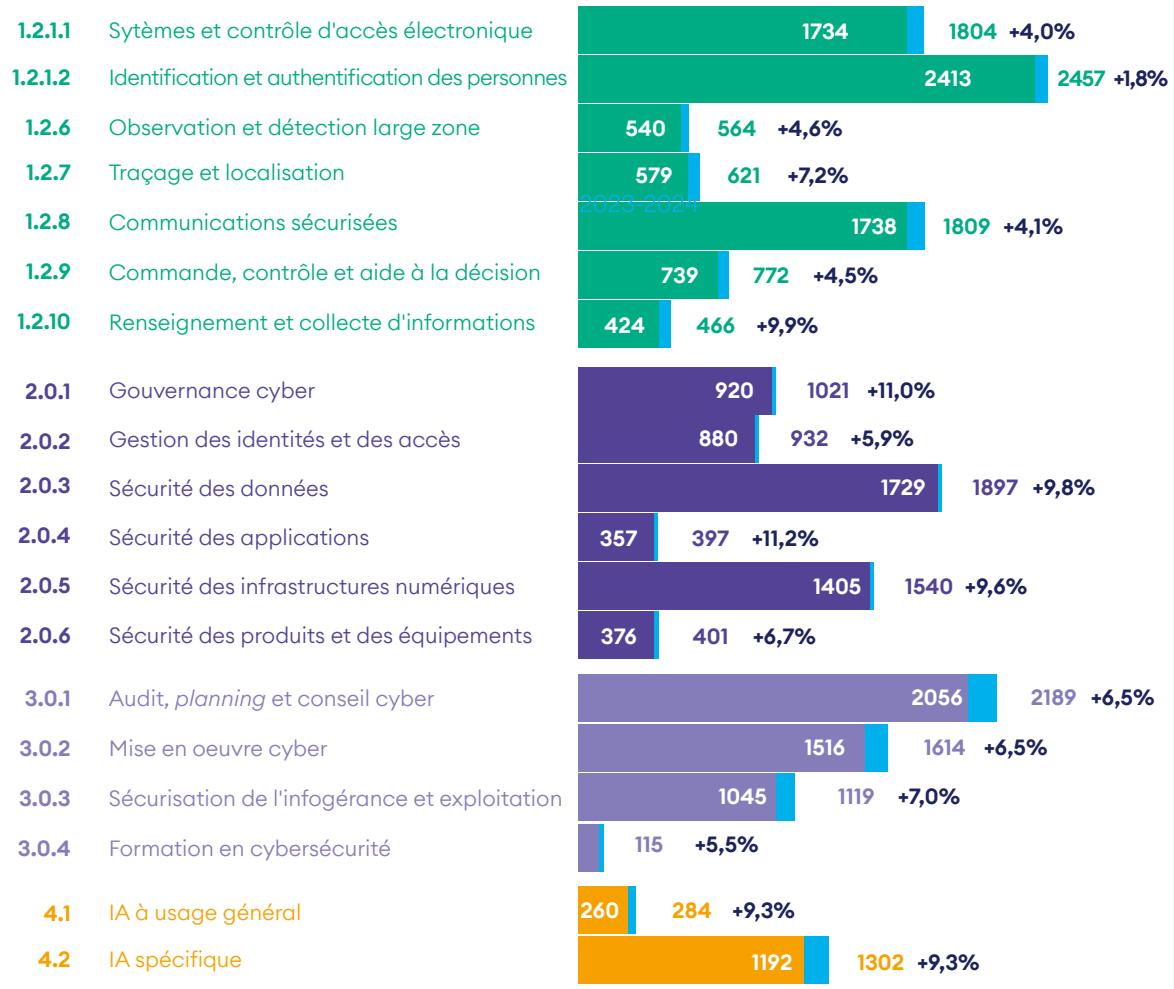
- Le **potentiel de croissance** est durablement supérieur à celui de toutes les autres industries françaises ;
- La confiance numérique est déjà de taille significative ;
- Les acteurs français sont à la pointe en matière de compétences et de R&D ;
- Ce secteur est essentiel à la **souveraineté numérique 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.

3. LES CHIFFRES CLEFS DE LA FILIÈRE

3.1 TAILLE ET CROISSANCE

CA de confiance numérique en France • 21,3 Mds € en 2024

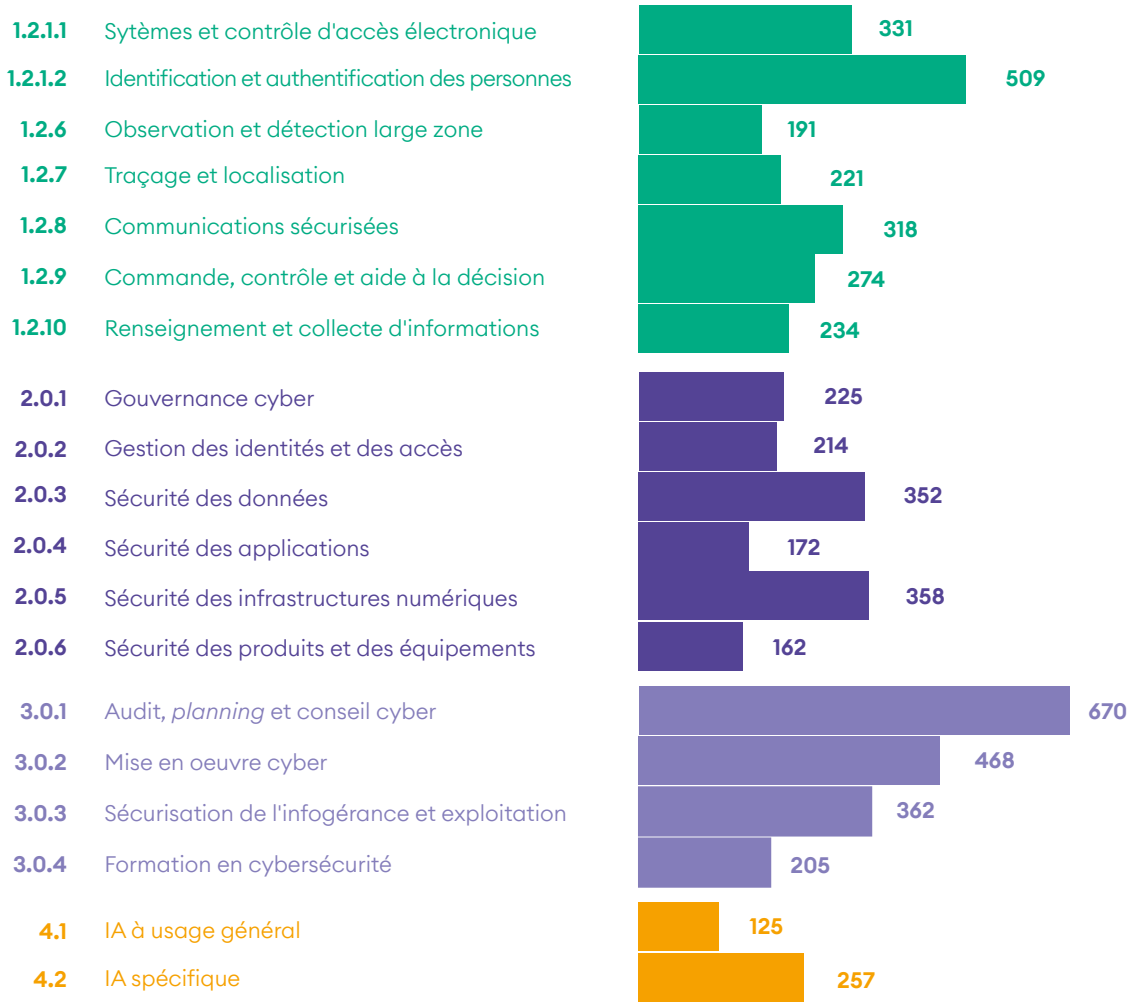


Sécurité numérique	Produits de cybersécurité	Services de cybersécurité	IA de confiance
8 493 M€ de CA	**6 188 M€** de CA	**5 036 M€** de CA	**1 586 M€** de CA
+4% en 2024	+9,2% en 2024	+6,6% en 2024	+9,3% en 2024

21 304 M€ de CA
de confiance numérique en France
+6,5% en 2024

Source : DECISION Etudes & Conseil

3.2 NOMBRE D'ENTREPRISES

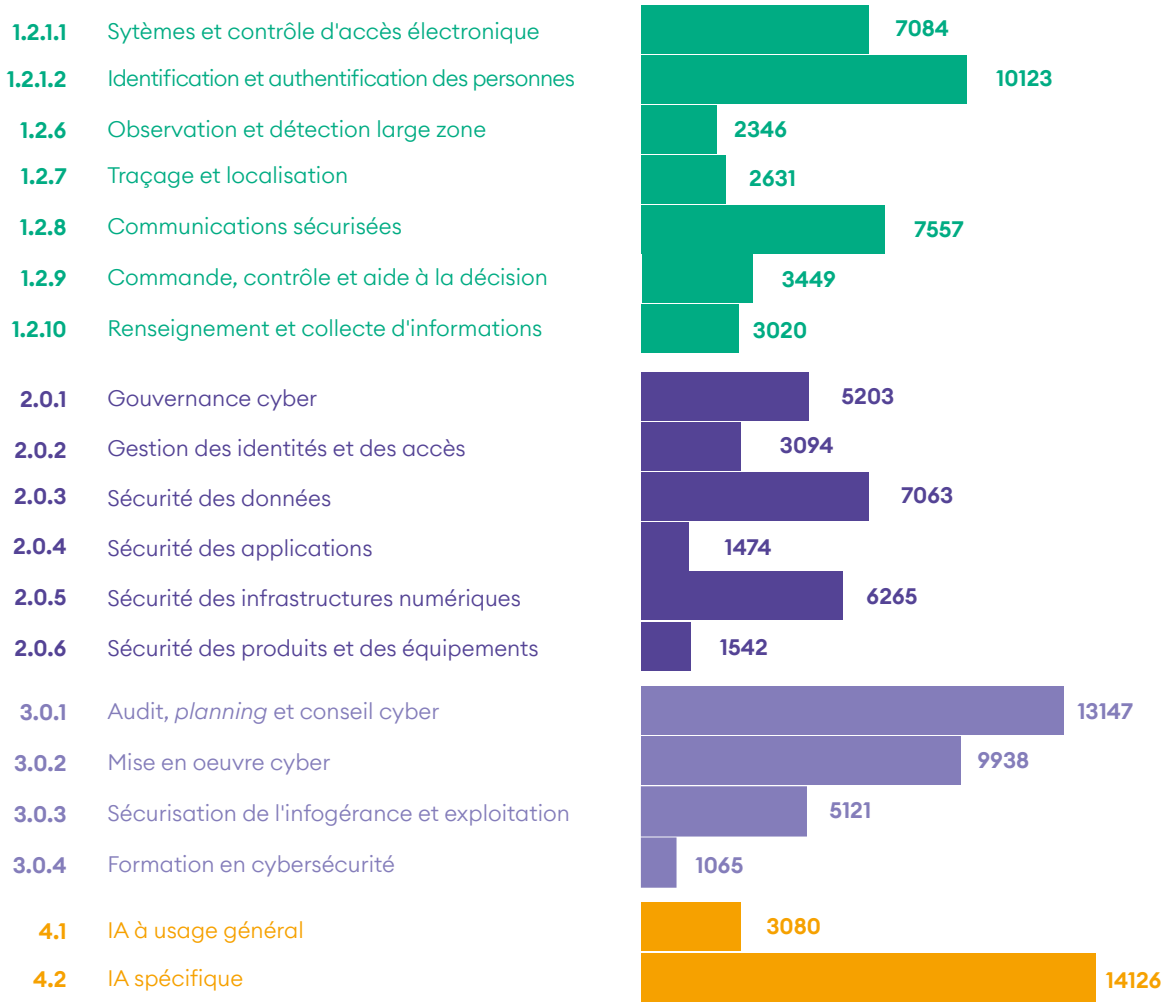


Sécurité numérique	Produits de cybersécurité	Services de cybersécurité	IA de confiance
1 770 entreprises	**739** entreprises	**717** entreprises	**315** entreprises

2 499 entreprises
de confiance numérique en France

Source : DECISION Etudes & Conseil

3.3 EMPLOIS

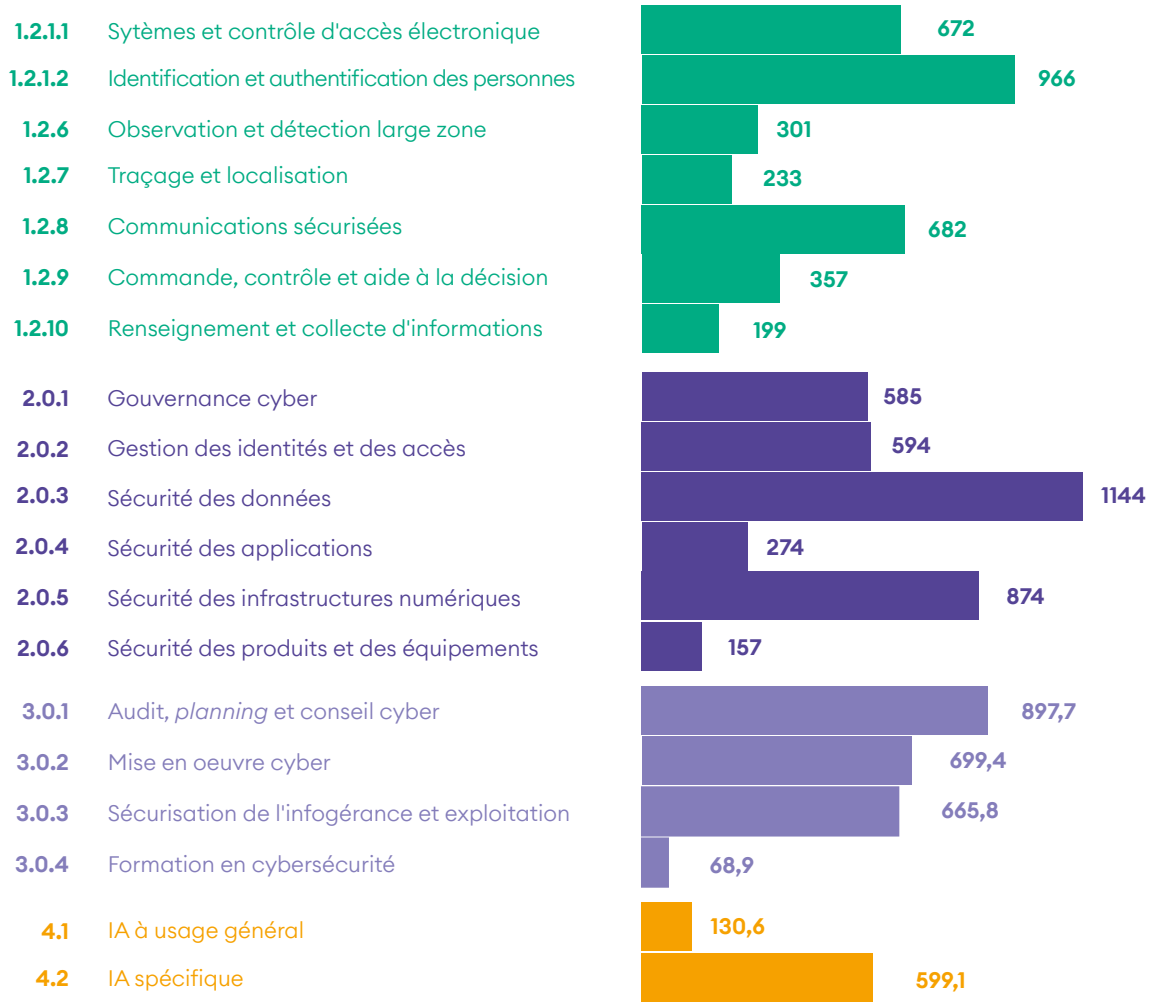


Sécurité numérique	Produits de cybersécurité	Services de cybersécurité	IA de confiance
36 212 emplois	**24 641** emplois	**29 271** emplois	**17 206** emplois

107 330 emplois
de confiance numérique en France

Source : DECISION Etudes & Conseil

3.4 VALEUR AJOUTÉE



Sécurité numérique	Produits de cybersécurité	Services de cybersécurité	IA de confiance
3 410 M€	**3 627 M€**	**2 332 M€**	**730 M€**
de valeur ajoutée	de valeur ajoutée	de valeur ajoutée	de valeur ajoutée

10 099 M€ de valeur ajoutée
de confiance numérique en France

Source : DECISION Etudes & Conseil

3.5 LES MOUVEMENTS DE FUSION - ACQUISITION

Entre janvier 2023 et mars 2025, 37 opérations de rachat d'entreprises dont le siège est situé en France ont été recensées dans la filière de la confiance numérique, soit une moyenne de 17 rachats par an. Ces opérations recouvrent à la fois des acquisitions entre entreprises, des rachats par des fonds financiers, et des transactions entre fonds.

Sur ces 37 opérations :

- 16 concernent des rachats d'entreprises françaises par d'autres entreprises françaises (43 %) ;
- 11 correspondent à des acquisitions d'entreprises étrangères par des entreprises françaises (30 %) ;
- 10 impliquent le rachat d'entreprises françaises par des entreprises étrangères (27 %).

La grande majorité des sociétés rachetées sont des PME (64 %), confirmant l'attrait des acheteurs pour des structures en croissance. Par rapport à la période 2017-2020, la fréquence des rachats reste globalement comparable, mais la taille des entreprises cibles est en moyenne plus réduite.

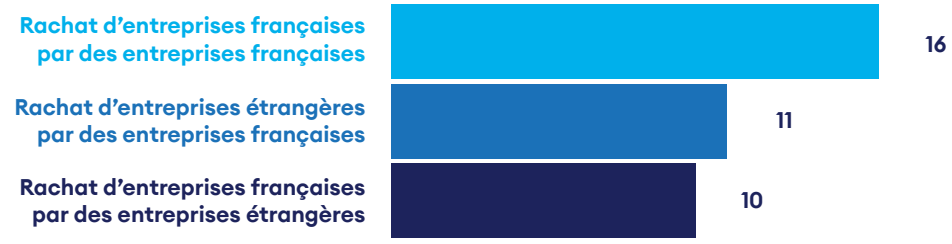
L'année 2024 se distingue par un volume de transactions plus faible (14 opérations), inférieur à la moyenne annuelle observée sur la période 2020 - 2023 (environ 20 opérations par an). Ce repli s'inscrit dans un contexte économique globalement moins favorable aux fusions-acquisitions.

En 2024-2025, les entreprises de taille intermédiaire en forte croissance – Nomios et I-Tracing – ont engagé des stratégies de développement européen par acquisitions, traduisant une nouvelle dynamique de consolidation du marché portée par une nouvelle génération d'acteurs français.

Sur les deux dernières années, les flux croisés entre la France et l'étranger tendent à s'équilibrer. Si la période 2017-2020 avait été marquée par une nette domination des rachats d'entreprises françaises par des capitaux étrangers, cette dynamique semble aujourd'hui moins marquée, en partie grâce à quelques opérations emblématiques menées par des groupes français sur des marchés voisins – à l'image des acquisitions d'Imperva et Tesserent par Thales en 2023. Pour autant, les États-Unis restent, en 2024, le principal acquéreur d'entreprises françaises de la filière, avec trois opérations notables : Expert Lines rachetée par Neverhack (entreprise française à capitaux majoritairement américains depuis sa levée de fonds auprès de Carlyle en 2023), Vade Security rachetée par Hornetsecurity, et PingCastle rachetée par Netwrix. Cette tendance s'est poursuivie début 2025, avec deux nouvelles opérations : Secure-IC rachetée par Cadence, et Altospam à nouveau par Hornetsecurity.

Les 37 mouvements de rachats sont résumés dans le diagramme ci-dessous :

Bilan : rachats d'entreprises sur la période 2023-2025



A• Les principales acquisitions depuis 2023 par les entreprises françaises

IN Groupe prépare le rachat stratégique d'IDEMIA Smart Identity pour consolider sa position mondiale dans l'identité numérique

En septembre 2024, IN Groupe est entré en négociations exclusives avec IDEMIA Group pour acquérir IDEMIA Smart Identity, l'une des trois divisions de l'entreprise. Cette opération majeure permettrait à IN Groupe de franchir un cap stratégique en atteignant une taille critique à l'échelle mondiale, avec un chiffre d'affaires combiné supérieur à un milliard d'euros. L'acquisition viendrait renforcer ses positions sur les marchés de l'identité physique et numérique,
avec une empreinte géographique étendue en Europe, en Afrique, au Moyen-Orient, en Amérique latine et en Asie. En accédant à des technologies de pointe telles que la conception de puces et de logiciels de sécurité, IN Groupe se doterait de capacités renforcées pour répondre aux exigences croissantes en matière de souveraineté, de cybersécurité et de conformité aux standards européens de protection des données.
Cette opération s'inscrit dans la continuité de la stratégie de croissance externe du groupe, amorcée depuis plus de dix ans.

Neverhack (ex-Pr0ph3cy) mène une ambitieuse campagne d'acquisitions en 2024

Depuis sa levée de fonds de 100 millions d'euros en 2023 auprès du fonds américain Carlyle, devenu actionnaire majoritaire à hauteur de 55 %, Neverhack a accéléré sa stratégie de croissance externe afin de créer un guichet unique de services cyber. En 2024, le groupe a réalisé trois acquisitions majeures : la société française Expert Line, le spécialiste estonien Cybers, et la multinationale italienne Innovery. Ces opérations renforcent ses compétences en SOC, sécurité offensive et intégration d'architectures IT, tout en étendant sa présence en Europe du Sud, dans les pays baltes et sur le continent américain.

ChapsVision poursuit sa stratégie de croissance externe dans l'IA et la gestion de crise

ChapsVision a réalisé deux acquisitions supplémentaires en 2024 et 2025, consolidant sa position dans le traitement de la donnée et l'intelligence artificielle. En novembre 2024, le groupe annonce le rachat de Sinequa, spécialiste mondial de la recherche d'entreprise augmentée par l'IA (RAG), afin d'intégrer ses technologies à la plateforme ArgonOS et accélérer son expansion internationale. L'opération est accompagnée d'une levée de 85 M€ auprès d'investisseurs dont Jolt Capital. En mars 2025, ChapsVision acquiert IREMOS, éditeur de logiciels de gestion de crise et spécialiste de la protection du secret défense. Cette opération renforce sa position de *leader* dans ce domaine, en combinant logiciels spécialisés et expertise métier, notamment grâce à l'intégration de RDI+, filiale d'IREMOS.

Safran se positionne dans l'IA de défense avec le rachat de Preligens

En septembre 2024, Safran annonce l'acquisition de Preligens, pépite française de l'intelligence artificielle appliquée aux secteurs de la défense et de l'aérospatial, pour 220 millions d'euros. L'entreprise, désormais rebaptisée Safran.AI, est rattachée à Safran Electronics & Defense.
Grâce à cette acquisition, Safran entend accélérer l'intégration de l'IA dans ses systèmes de surveillance, d'inspection et de prise de décision, tout en valorisant le savoir-faire de Preligens dans l'analyse automatisée d'images et de signaux.
Au-delà des applications militaires, le groupe prévoit également de transposer ces technologies aux usages industriels dans le cadre de sa stratégie Industrie 4.0.

Rachats vers l'Europe

Plusieurs entreprises françaises renforcent leur présence en Europe à travers des acquisitions ciblées. I-Tracing se distingue en rachetant en 2024 la société britannique Bridewell, spécialiste du conseil stratégique en cybersécurité.
Cette opération, soutenue par Eurazeo, Sagard NewGen et Oakley Capital, permet à I-Tracing d'atteindre plus de 1 000 consultants et d'étendre sa couverture au Royaume-Uni et aux États-Unis.
Deux autres acquisitions vers le Royaume-Uni ont également marqué l'année : Nomios rachète la société Dionach, experte en tests d'intrusion et audit de conformité, tandis que le fonds Keensight Capital prend une participation majoritaire dans MetaCompliance, acteur basé en Irlande du Nord, spécialisé dans la gestion des risques humains et la formation à la cybersécurité.

B• Les principaux rachats d'entreprises françaises par des capitaux étrangers

Les acteurs américains renforcent leur présence sur le marché français

Les entreprises à capitaux américains ont été particulièrement actives en France en 2024 et au premier trimestre 2025, avec cinq acquisitions marquantes. Le groupe Hornetsecurity, contrôlé par des capitaux américains, a successivement acquis les sociétés françaises Vade et Altospam, renforçant ainsi sa présence en France et son positionnement européen.

Le spécialiste américain de la conception de circuits électroniques Cadence a quant à lui racheté Secure-IC, spin-off de Telecom Paris et fleuron français de la cybersécurité embarquée. Cette acquisition permettra à Cadence d'élargir son portefeuille d'IP sécurisées et de solutions d'évaluation.

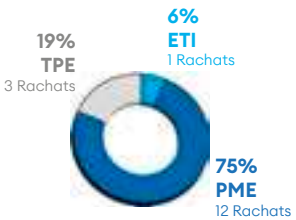
Dans le domaine de la sécurité des identités, Netwrix a acquis PingCastle, éditeur reconnu pour sa solution d'analyse de vulnérabilités *Active Directory*. Cette opération permet à Netwrix d'étoffer ses capacités de détection et de remédiation des failles dans les environnements hybrides.

Ces opérations témoignent d'un intérêt continu des groupes américains pour les technologies de cybersécurité développées en France.

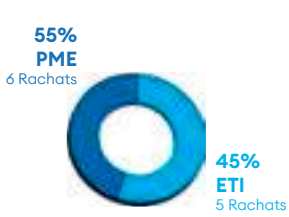
Des groupes européens élargissent leur empreinte en France

Les entreprises européennes ont également consolidé leur présence sur le territoire français à travers plusieurs acquisitions stratégiques. Le groupe norvégien Visma a racheté MyCompanyFiles, spécialiste des plateformes d'échanges sécurisés pour les experts-comptables, poursuivant ainsi sa stratégie de croissance dans les services *clouds* sécurisés pour les professionnels. Dans le domaine de la cybersécurité, l'irlandais Integrity360 a absorbé Holiseum, acteur français reconnu dans la sécurité des infrastructures critiques (IT/OT). Cette alliance permet à Integrity360 de renforcer son expertise industrielle et d'accélérer son déploiement en France.

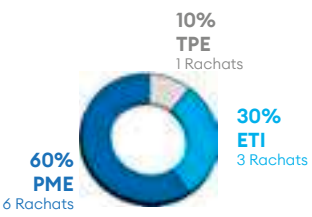
16 Rachats d'entreprises françaises par des entreprises français



11 Rachats d'entreprises étrangères par des entreprises françaises



10 Rachats d'entreprises françaises par des entreprises étrangères



3.6 UNE ANNÉE DYNAMIQUE POUR LES LEVÉES DE FONDS

Comme chaque année, le cabinet DECISION s'appuie sur le Baromètre de l'Investissement européen en cybersécurité de Tikehau Ace Capital, qu'il complète par ses propres recherches en prenant en compte la segmentation spécifique de l'ACN, qui englobe l'ensemble des activités de sécurité numérique au-delà de la cybersécurité.

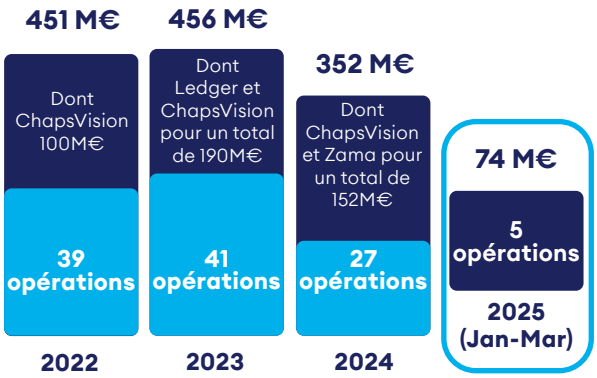
Après plusieurs années de croissance continue, 2024 marque un repli du nombre et du montant total des levées de fonds dans la filière de la confiance numérique en France. Sur l'ensemble de l'année, 27 opérations ont été recensées pour un total de 352 millions d'euros, contre 42 opérations pour 456 millions d'euros en 2023. Cette baisse en volume est toutefois à nuancer : le montant moyen par levée a atteint 13 millions d'euros en 2024, contre 11,1 millions d'euros l'année précédente.
La tendance s'est confirmée au premier trimestre 2025, avec seulement 4 opérations recensées pour un montant cumulé de 49 millions d'euros.
Malgré ce contexte plus difficile, la filière continue de se distinguer par des levées significatives : comme chaque année depuis quatre ans, des opérations d'envergure ont été réalisées, notamment par ChapsVision (87 millions d'euros) et Zama (67 millions d'euros).
En 2024, les membres de l'ACN ont représenté près de 60 % des montants levés, soit un total de 209 millions d'euros sur l'année. Cette dynamique souligne l'importance croissante des acteurs de l'écosystème ACN dans le paysage de la confiance numérique en France.

Parmi les investisseurs français qui ont soutenu les *startups* de la filière en 2024, on retrouve des acteurs majeurs tels que Bpifrance, Tikehau Capital, Alven, SWEN Capital Partners, Hi Inov, Adelie, Shapr Venture, Auriga Cyber Ventures, Kreaxie, Super Capital, Qualium Investissement, GENEO Capital et Elaia.

Dans un contexte économique et financier toujours peu favorable à l'investissement, la France fait preuve d'une résilience remarquable. Selon le baromètre européen de Tikehau Ace Capital, les montants levés en cybersécurité ont baissé pour la deuxième année consécutive à l'échelle européenne. Toutefois, contrairement à ses voisins, la France maintient une dynamique solide et s'impose cette année comme le premier pays européen en montant levé, devant le Royaume-Uni.

Ce positionnement confirme l'attractivité de l'écosystème français et sa capacité à attirer des financements significatifs, y compris en période d'incertitudes.

Montant des levées de fonds des *startups* françaises de la confiance numérique



Montant des levées de fonds dans l'intelligence artificielle

À titre de comparaison, les levées de fonds dans l'intelligence artificielle ont atteint des niveaux nettement supérieurs en 2024. Sur l'ensemble de l'année, les investissements dans les entreprises françaises de l'IA se sont élevés à 1,114 milliards d'euros, soit plus de trois fois le montant levé dans la cybersécurité sur la même période (352 millions d'euros). Cette dynamique a été largement tirée par quelques opérations exceptionnelles, notamment la série de levées réalisées par Mistral AI, qui totalise 1,09 milliards d'euros depuis 2023, dont 600 millions d'euros levés en 2024. On peut également citer H Company, qui a levé 200 millions d'euros en mai 2024.

Ce déséquilibre entre les deux segments ne remet pas en cause l'importance stratégique de la cybersécurité, mais reflète l'effet d'attraction exercé par l'IA auprès des investisseurs, dans un contexte de forte médiatisation et de promesses de transformation économique transversale.

Liste des levées de fonds des *startups* françaises de la confiance numérique

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	Qevlar 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
37	Inspeere		2023	0.6
38	Escape		2023	0.5
39	OneWave		2023	0.4
40	Bastion Technologies	**ACN**	2023	
41	Kubo Labs		2023	
	Total ACN			**167**

En 2024

	Entreprise	Syndicat	Année	Montant (M€)
1	ChapsVision	**ACN**	2024	85
2	Zama	**ACN**	2024	67
3	Filigran		2024	32.3
4	YesWeHack	**ACN**	2024	26
5	Stoïk	**ACN**	2024	25
6	Filigran		2024	15
7	Dfns		2024	15
8	BforAI		2024	14.4
9	Patrowl		2024	11
10	BforAI		2024	9.6
11	COMAND AI		2024	8.5
12	Tenacy		2024	6
13	Anozr Way	**ACN**	2024	6
14	Dotfile		2024	6
15	Probabl		2024	5.5
16	Mindflow		2024	5
17	Finovox		2024	3.9
18	Nijta		2024	2.1
19	Dipeo		2024	1.8
20	Alcyconie		2024	1.4
21	Kamae		2024	1.4
22	Nestor		2024	1.2
23	Daspren		2024	1
24	Soteria Lab		2024	0.8
25	Edamame		2024	0.4
26	Alphaguard		2024	0.2
27	LookUp Space		2024	
	Total ACN			**209**

En 2025

	Entreprise	Syndicat	Année	Montant (M€)
1	Riot		2025	27.7
2	Sekoia.io	**ACN**	2025	25
3	Cryptio		2025	15
4	CyGo Entrepreneurs		2025	5
5	Akidaia		2025	1.3

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 17,3 Mds € de chiffre d'affaires en 2024.

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 3,5 Mds € en 2024 (en additionnant les PME avec un chiffre d'affaires supérieur à 5 M €, les entreprises ayant bénéficié d'une levée de fonds pour un montant égal ou supérieur à 5 M € et les PME qui sont devenues des ETI depuis les années 2000).

Grands acteurs historiques

17,3 Mds € en 2024

Emergence d'un fort écosystème de PME

2,5 à 3,5 Mds € en 2024

Note : Les entreprises dont le logo est présent dans l'encadré sur l'écosystème des PME correspondent aux plus remarquables (les ETI, les entreprises ayant bénéficié des plus grandes levées de fonds ou les PME avec les plus grands chiffre d'affaires).

POINT DE VUE

HENRY MARCOUX

• DIRECTEUR GÉNÉRAL ADJOINT

TIKEHAU CAPITAL

« L'année 2024 se distingue par un rebond global spectaculaire pour le secteur de l'investissement en cybersécurité puisque les montants investis ont progressé de 30% par rapport à 2023 pour atteindre 12.1 Mds €, correspondant à 687 levées aux États-Unis, en Israël et en Europe. Après une année 2023 marquée par un recul des investissements en cybersécurité sous l'effet d'un contexte économique défavorable, l'intérêt des investisseurs se renforce.

Les États-Unis confirment leur domination avec des levées massives et une dynamique soutenue des tours de financement avancés (Series C, D, et E), tandis qu'Israël subit une forte baisse de ses investissements, impacté par les tensions géopolitiques.

L'Europe maintient une part significative de 25% des montants levés globalement et sur la dernière décennie, le marché européen de la cybersécurité continue de s'affirmer comme une opportunité d'investissement clé, avec une multiplication par 1,6 du nombre de levées et une augmentation de 12,5 fois des montants investis. Ces tendances témoignent d'un secteur en mutation, toujours attractif malgré un contexte économique mondial complexe et confirme l'évolution du marché vers des financements plus concentrés sur des entreprises en phase de croissance avancée.

Avec 342 M € en montants levés et 25 tours de table en 2024, la France fait preuve de résilience et conserve sa singularité dans l'écosystème de la cybersécurité européenne en occupant la première place européenne en montants levés, devant le Royaume-Uni.

Enfin, la dynamique de consolidation du secteur s'accélère en Europe en 2024, avec 134 entreprises européennes de cybersécurité rachetées, dont 71% par des acteurs européens, une hausse notable de 19% par rapport à 2023. En France, 12 acquisitions ont eu lieu, 92% d'entre elles ayant été réalisées par des sociétés françaises. »

Tikehau Capital, groupe mondial de gestion d'actifs alternatifs qui gère 49,6 milliards d'euros d'actifs (au 31/12/2024), est devenu depuis 2019 l'un des acteurs majeurs européens dans le domaine de l'investissement en cybersécurité. Tikehau Capital compte en particulier en portefeuille dans les domaines cybersécurité et technologies de confiance les participations françaises suivantes : ChapsVision, Claranet, Egerie, Ekimetrics, Glimps, QuarksLab, Oodrive, ProvenRun, Tehtris, TrustInSoft, Trustpair, Yogosha.

Les principales tendances de l'investissement en cybersécurité révélées par la **6ème édition du baromètre publié par Tikehau Capital** en partenariat avec InCyber Forum.

disponible en téléchargement sur :
https://urlr.me/h6BRMC

« Rebond des investissements en cybersécurité en 2024 au niveau mondial »

« La France prend la tête des pays européens en montants levés. »

+ 30%
investissement en cybersécurité en 2024

25%
des montants levés en Europe en 2024

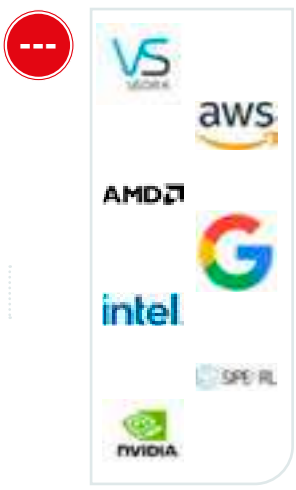
1ère place européenne
en montants levés en 2024

4. L'IA DE CONFIANCE : ENJEUX ET PERSPECTIVES D'AVENIR

4.1 LA CHAINE DE VALEUR DE L'INTELLIGENCE ARTIFICIELLE

L'Intelligence artificielle de confiance fait son apparition en 2024 en tant que nouveau segment de la filière française de la confiance numérique, au côté de la sécurité numérique ainsi que des produits et services de cybersécurité.
Ce chapitre positionne la filière française le long de la chaine de valeur de l'intelligence artificielle de confiance (1), distingue l'IA à usage général et l'IA spécifique en matière de besoin en données (2) et de création de valeur pour la filière française (3). Enfin, ce chapitre dresse des perspectives pour la structuration d'une filière française du *cloud* de confiance au service de la filière française de l'IA spécifique de confiance.

Positionnement de la filière française le long de la chaine de valeur de l'intelligence artificielle



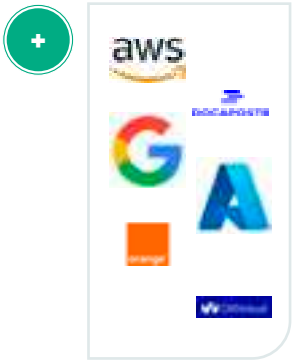
Fabricants de processeurs : une dépendance structurelle vis-à-vis des acteurs américains

La production d'intelligence artificielle repose en amont sur les fabricants de processeurs spécialisés - GPU, NPU, ASIC... - nécessaires à l'entraînement et à l'inférence des modèles.
Ce segment est dominé par des entreprises américaines comme NVIDIA, AMD, ou encore Intel. Ces entreprises, souvent *fabless*, se concentrent sur le *design* électronique des puces, qu'elles font ensuite produire dans des fonderies, principalement en Asie, notamment chez TSMC à Taïwan. Les *hyperscalers* comme Google ou AWS investissent ce segment en développant leurs propres puces (TPU, Trainium).
La France est quasiment absente de cette étape critique. Quelques rares *fabless* comme SiPearl, VSORA ou Kalray tentent de se positionner, mais l'écosystème reste modeste et naissant.
Les grands producteurs européens de semiconducteurs (ST Micro, NXP, Infineon) se concentrent sur les marchés embarqués (automobile, aéronautique, défense...), et n'ont pas pour objectif d'investir pour concurrencer les géants américains dans les puces d'intelligence artificielle.

Équipementiers *data centers*, supercalculateurs, etc. : une présence française limitée

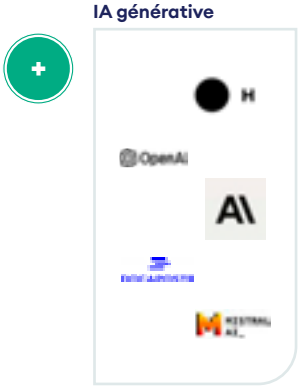
Le segment des équipements matériels - serveurs haute performance (HPC) et supercalculateurs - est dominé par les acteurs américains et chinois comme HP, Dell, IBM, ou encore Lenovo. Ces acteurs s'approvisionnent en processeurs auprès des fabricants pour assembler des solutions d'infrastructure adaptées aux besoins de l'intelligence artificielle. Les deux acteurs français qui jouent un rôle significatif sur ce segment sont Atos -au travers de sa filiale Bull- et dans une moindre mesure OVH. Ces deux entreprises conçoivent l'architecture de leurs serveurs et les assemblent. Toutefois, cette présence française reste isolée et fragile dans un secteur où la concurrence internationale est intense. Les capacités françaises sont loin d'égaler celles des grands industriels américains et chinois.

Note : Sont positionnés sur ce visuel les acteurs français ou étrangers les plus emblématiques sur chacun des segments.
En conséquence, l'absence du logo d'une entreprise dans un segment ne signifie pas qu'elle est absente de ce segment.
À titre d'exemple, Thales est positionné à la fois sur le segment des éditeurs d'IA, sur celui des ESN et sur celui de l'intégration.
Source : DECISION Etudes & Conseil



Fournisseurs de services *cloud* : un marché dominé par les *hyperscalers*

Les fournisseurs de services *cloud* offrent les infrastructures nécessaires à l'entraînement et au déploiement des modèles d'intelligence artificielle. Les *leaders* mondiaux - AWS, Microsoft Azure, Google Cloud- disposent de capacités de calcul massives et proposent également leurs propres briques technologiques d'IA (GPT, Vertex AI, Azure OpenAI, etc.), devenant à la fois hébergeurs et éditeurs. La France tente de bâtir un écosystème alternatif, avec des acteurs comme OVHcloud, Numspot, Outscale, Docaposte, Platform.sh ou encore Scaleway. Ces initiatives offrent une alternative souveraine aux solutions américaines, bien qu'elles restent pour le moment loin des capacités des *hyperscalers*.

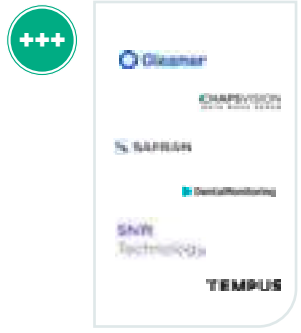


Éditeurs d'intelligence artificielle : une dynamique française en pleine croissance

Les éditeurs développent des solutions logicielles fondées sur l'intelligence artificielle, le plus souvent commercialisées sous la forme de services applicatifs (SaaS). Ce segment recouvre deux grandes catégories d'acteurs :

- Les éditeurs de modèles génériques, qui conçoivent des modèles fondamentaux (LLM, diffusion, etc.), destinés à être utilisés ou adaptés dans divers contextes,
- Et les éditeurs de solutions métier, qui développent des modèles sur mesure pour répondre à des besoins spécifiques dans un secteur donné.

En France, Mistral AI -qui développe des LLM *open source* à usage général- est l'un des rares acteurs de la première catégorie.
Dans la seconde, on trouve de nombreuses entreprises françaises qui conçoivent leurs propres modèles adaptés à des données et des problématiques ciblées : Shift Technology (fraude dans l'assurance), Gleamer (radiologie), Exotec (robotique logistique), Dental Monitoring (suivi orthodontique), ou encore Wintics (analyse vidéo pour les villes et infrastructures). Ces solutions reposent parfois sur l'adaptation de modèles externes, mais sont toujours conçues comme des produits à part entière.
À l'international, on observe une structuration similaire : des éditeurs de modèles généralistes comme OpenAI, Anthropic ou Cohere, et des éditeurs spécialisés comme Tempus (santé), Darktrace (cybersécurité), Trax (retail intelligence), ou SambaNova (analyse scientifique et industrielle).



Entreprises de services numériques (ESN)

Les ESN jouent un rôle clé dans le déploiement concret de l'intelligence artificielle dans les entreprises. Elles développent des modèles sur mesure, en fonction des données, des systèmes d'information et des objectifs métier de leurs clients.

Elles assurent aussi l'intégration, le conseil et l'accompagnement dans la mise en œuvre de l'intelligence artificielle. La France bénéficie d'un tissu très solide avec des entreprises comme Sopra Steria, Capgemini, Atos, Thales, Orange Business ou encore Wavestone.

Intégrateurs

Les intégrateurs assurent le lien entre les technologies (modèles, logiciels, API...) et les cas d'usage concrets en entreprise, notamment dans des secteurs industriels ou souverains.
Ils déploient des solutions dans des environnements métier spécifiques, souvent en les combinant à d'autres briques technologiques ou systèmes embarqués. Ces acteurs jouent un rôle structurant dans la diffusion de l'intelligence artificielle au sein du tissu économique, en l'intégrant directement dans des systèmes ou équipements complexes. Thales, Airbus Defence & Space, Idemia ou Safran font partie des grands intégrateurs de la filière de la confiance numérique. La France dispose de grands intégrateurs dans d'autres filières (énergie, automobile, santé...).

4.2 INTELLIGENCE ARTIFICIELLE À USAGE GÉNÉRAL OU SPÉCIFIQUE : DES BESOINS EN DONNÉES DIFFÉRENTS

L'intelligence artificielle à usage général est principalement composé de solutions d'IA générative et désigne les modèles capables de produire de nouveaux contenus -textes, images, sons, ou vidéos- à partir d'instructions textuelles, visuelles ou vocales. Ces modèles, comme les LLM (*Large Language Models*), ou les SLM (*Small Language Models*), sont pré-entraînés sur d'énormes volumes de données généralistes.
Ils peuvent ensuite être adaptés à différents usages : génération de texte, classification d'informations, planification, recommandation de produits ou services, ou encore chatbots et assistants virtuels.
La filière française dispose de plusieurs acteurs positionnés sur ce segment :

• **Mistral AI** est la *startup* française emblématique du secteur, spécialisée dans le développement de modèles LLM *open source* à vocation générale, utilisés pour des tâches de génération et de dialogue.

• **DALVIA Santé** est l'assistant médical de Docaposte basé sur l'IA générative, permettant de produire des comptes rendus d'hospitalisation à partir de notes audios et de documents du parcours patient. Hébergée sur le *cloud* souverain NumSpot, la solution est conçue pour garantir la sécurité des données et s'intégrer aux logiciels métiers hospitaliers. Elle vise à faire gagner du temps aux professionnels de santé, tout en améliorant la coordination entre acteurs.

• **Assist'Act** est l'outil d'aide à la rédaction d'actes administratifs de Docaposte pour les collectivités locales, intégrant un assistant conversationnel basé sur l'intelligence artificielle. Il permet la génération, la recherche et la gestion optimisée des actes publics.

• **IRIS**, développé par Sopra Steria en partenariat avec IBM et IVèS, est le premier assistant conversationnel en langue des signes. Ce «signbot» permet des interactions en temps réel en LSF, LSQ, LSA et LST, en combinant l'IA conversationnelle (via IBM Watson) et les solutions d'accessibilité développées par IVèS.

L'intelligence artificielle spécifique, à l'inverse, désigne des solutions conçues pour des cas d'usage précis dans des environnements métiers définis. Ces IA s'appuient sur des données d'entrée très ciblées (textes, sons, images, vidéos, signaux, séries temporelles, etc.) et sont entraînées sur des volumes plus limités mais hautement qualifiés.
Elles permettent, par exemple, d'automatiser la lecture de documents, la détection d'anomalies visuelles, la prédiction de pannes ou la détection de comportements à risque.
La filière française dispose d'un grand nombre d'acteurs très bien positionnés sur ce segment :

• **Safran AI** développe des algorithmes d'analyse automatique d'images satellites haute résolution, de vidéos *Full Motion* et de signaux acoustiques. Ces solutions, destinées au secteur de la défense, permettent la détection d'objets ou d'événements présentant un intérêt militaire. Elles reposent sur une chaîne de traitement sécurisé, avec une traçabilité complète des données, et sont conçues pour être intégrées à des systèmes critiques.

• **Gleamer** offre une solution d'analyse des lésions osseuses à partir d'images médicales et génère un pré-diagnostic automatisé pour les radiologues. Le praticien conserve la main sur la validation du compte rendu. La solution est déployée dans plus de 50 hôpitaux et cliniques en France, dont l'Hôtel Dieu et Ambroise Paré, et a été récompensée par le *Best New Radiology Vendor Award* aux Eurominnies 2023.

• **Wintics** offre une solution d'analyse vidéo intelligente afin d'améliorer la sécurité des infrastructures, la fluidité des déplacements ou encore l'aménagement urbain. Ces outils permettent aux acteurs territoriaux (aéroports, ports, opérateurs de transport public, collectivités…), de prendre des décisions basées sur l'analyse de comportements, de flux ou d'anomalies détectées dans l'espace public.

Les besoins en données varient selon qu'il s'agit d'IA générative ou d'IA spécifique. L'IA générative repose sur l'accès à d'immenses volumes de données hétérogènes, souvent issues du web ou de grands corpus textuels. L'objectif est de maximiser la couverture et la diversité des données pour permettre aux modèles d'apprendre à générer du contenu pertinent dans un large éventail de contextes. Cette logique de *big data* soulève des enjeux majeurs d'accès aux grands jeux de données pour rester compétitifs face aux solutions américaines ou chinoises - notamment dans les secteurs sensibles de la santé, de l'éducation ou des transports.

À l'inverse, l'IA spécifique s'appuie sur des données ciblées, métier et fortement qualifiées. Ces modèles sont conçus pour des cas d'usage restreints, et nécessitent des jeux de données plus modestes mais parfaitement structurés, annotés et contextualisés. L'accent est mis sur la qualité des données, bien plus que sur leur quantité. Dans ce cadre, l'entraînement peut souvent être réalisé en local, sans infrastructure de calcul massive. Un exemple est celui de Safran AI, dont les équipes intègrent des analystes spécialisés chargés d'annoter manuellement les images satellites utilisées pour entraîner les algorithmes. Cette annotation humaine garantit une précision maximale, en permettant aux modèles de distinguer finement les objets ou anomalies d'intérêt. Cette approche itérative, fondée sur la qualité des données et l'expertise métier, limite le recours à des infrastructures massives tout en assurant des performances élevées dans des contextes critiques comme la défense ou la sécurité.

4.3 L'IA SPÉCIFIQUE GÉNÈRE EN FRANCE PLUS DE VALEUR QUE L'IA À USAGE GÉNÉRAL

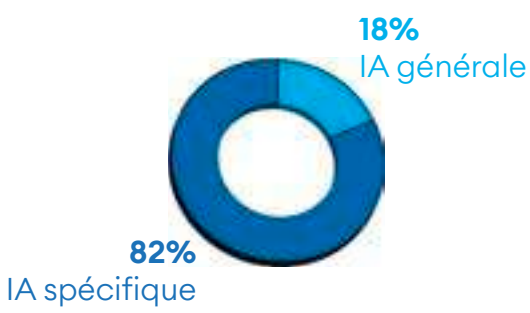
Dans le cadre de cet Observatoire, l'analyse de la production d'intelligence artificielle en France se concentre sur l'intelligence artificielle « de confiance », c'est-à-dire une intelligence artificielle conçue et déployée en respectant un ensemble de critères à la fois juridiques, techniques et éthiques. Cette notion combine les principes définis dans le Livre blanc de l'Alliance pour la Confiance Numérique (ACN) - transparence, explicabilité, robustesse, sécurité, respect de la vie privée, maîtrise humaine - avec une dimension de souveraineté, en intégrant la notion de nationalité des entreprises.

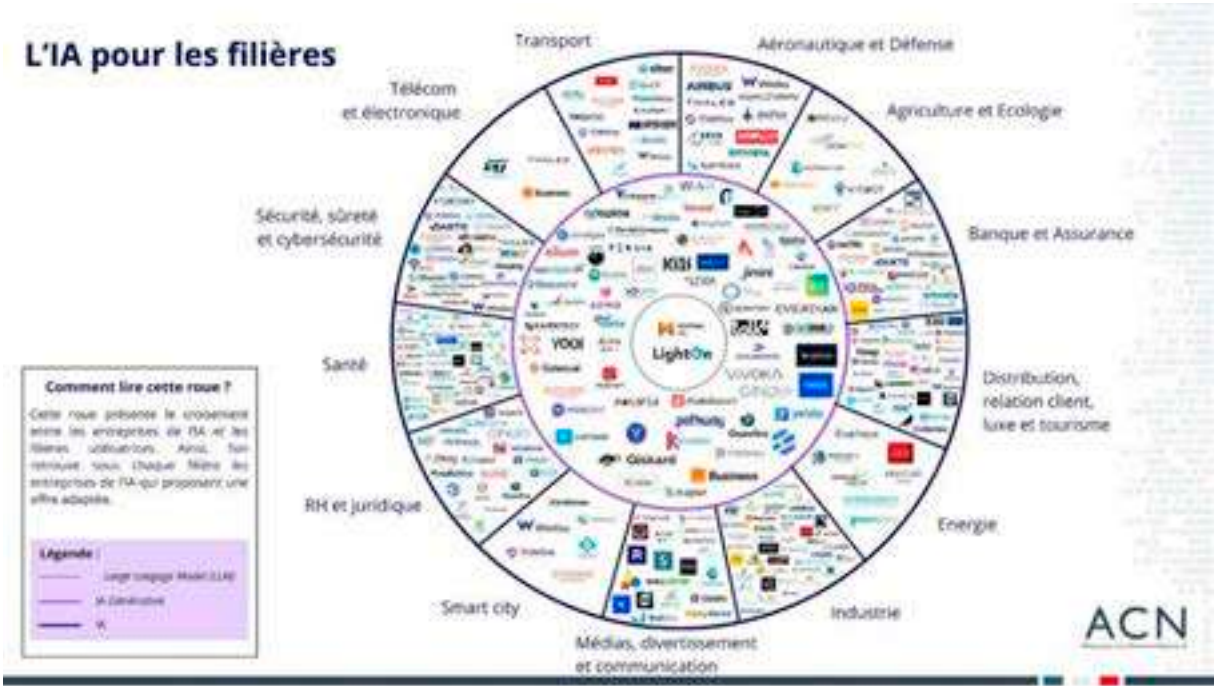
Malgré l'engouement médiatique et financier suscité par l'IA générative - notamment depuis l'émergence des LLM comme GPT ou des modèles *open source* comme ceux de Mistral AI - l'IA spécifique représente 82% du chiffre d'affaires généré depuis la France en 2024 (1,3 Mds €), contre seulement 18% pour l'IA à usage général (280 M €).

Cet écart entre visibilité et réalité économique s'observe également dans les levées de fonds. Si l'on considère uniquement les principaux tours de table réalisés en 2024, l'IA générative a concentré plus de 820 millions d'euros d'investissements, portés par des acteurs comme Mistral AI (1,09 Md€ depuis 2023, 600 M€ en 2024), H Company (200 M€), Dust (20 M€), ou encore Lighton (12 M€). À l'inverse, les entreprises positionnées sur l'IA spécifique, bien que plus nombreuses et actives sur un large éventail de cas d'usages, ont levé des montants plus modestes : un peu plus de 130 millions d'euros au total pour les principales levées. Parmi elles, on trouve Photoroom (59 M€), Gleamer (36 M€), ou encore Pollen Robotics (2,4 M€).

Enfin, ce constat se retrouve dans l'analyse financière des *startups* françaises de l'IA. On observe en 2024 une immaturité des business modèles particulièrement prégnant chez les éditeurs d'IA générative, avec un écart entre le montant des levées de fonds et le montant des ventes bien plus grand que chez les éditeurs d'IA spécifique. Au-delà, le segment de l'IA de confiance reste globalement immature en 2024, avec un chiffre d'affaires moyen par employé bien plus faible que dans les autres segments de la confiance numérique (92 000 €).

Proportion IA générale / IA spécifique





4.4 *CLOUD* DE CONFIANCE ET IA DE CONFIANCE : QUELLES OPPORTUNITÉS POUR LA FILIÈRE FRANÇAISE ?

On observe une division de la chaine de valeur de l'IA de confiance entre :

• Une chaine de valeur de l'IA générative, qui soulève des enjeux éthiques et techniques liés à l'accès aux jeux de données les plus vastes possibles, et dans laquelle les *hyperscalers* américains apparaissent difficilement contournables.

• Une chaine de valeur de l'IA spécifique, qui nécessite l'accès à des données spécifiques dont disposent bon nombre d'intégrateurs français et dont la sensibilité rend incontournable le recours aux acteurs français du *cloud* de confiance.
En 2024, c'est cette seconde chaine de valeur qui concentre 82% du chiffre d'affaires de la filière française, et pour laquelle une maîtrise de bout en bout est envisageable.

Bien que la maitrise de la chaine de valeur de l'IA générative s'annonce comme un beau combat à mener, les perspectives de création de valeur - en France comme à l'export - pour la filière française semblent aujourd'hui résider dans la structuration d'une offre intégrée « *cloud* de confiance dédié à une IA spécifique de confiance ».

5. POINT SUR LA MENACE INFORMATIQUE

5.1 PANORAMA ANSSI DE LA CYBERMENACE 2024

Le rapport annuel 2024 de l'ANSSI met en lumière une intensification de la menace cyber, marquée par trois axes dominants : les opportunités conjoncturelles (Jeux Olympiques de Paris), les vulnérabilités techniques persistantes, et les moyens toujours plus industrialisés des attaquants, qu'ils soient étatiques ou cybercriminels.

Panorama ANSSI de la cybermenace 2024

disponible en téléchargement sur :
urlr.me/Zpqtk3

L'année 2024 a été marquée par des événements majeurs tels que les Jeux Olympiques de Paris, catalyseurs de nombreuses tentatives de cyberattaques. Si aucune attaque n'a empêché le déroulement des compétitions, les opérations d'espionnage, de déstabilisation et d'extorsion ont été significatives, notamment en raison du contexte géopolitique tendu.

L'un des constats les plus frappants concerne l'exploitation des vulnérabilités dans les équipements de sécurité, notamment les passerelles VPN et les pare-feux. Ces dispositifs, exposés sur Internet, sont devenus des points d'entrée privilégiés pour les attaquants. Le rapport met en évidence que les vulnérabilités connues sont parfois exploitées plusieurs mois après la publication des correctifs, ce qui souligne un déficit de réactivité dans la gestion des risques au sein des organisations.

Les chaînes d'approvisionnement, autre point sensible, sont ciblées pour leur potentiel de rebond vers des cibles stratégiques. Les attaquants exploitent les relations de confiance et les interconnexions entre entreprises et prestataires pour accéder aux systèmes des entités finales. Le cas de l'attaque contre un industriel français via un sous-traitant illustre parfaitement cette menace latente. L'attaque n'a pas abouti à une latéralisation mais démontre une persistance dans les tentatives.

Le rapport souligne également l'essor du mercenariat cyber et de la commercialisation de capacités offensives à grande échelle. Les acteurs étatiques et cybercriminels utilisent de plus en plus les mêmes infrastructures, outils *open source*, voire rançongiciels, rendant leur attribution difficile. Le phénomène ADINT, exploitant les flux publicitaires pour mener des opérations de surveillance ou d'espionnage, ouvre de nouvelles perspectives inquiétantes pour la cybersécurité des citoyens et des entreprises.

Enfin, les attaques se multiplient selon trois logiques principales : la recherche de profit (rançongiciels, extorsion de données), le renseignement stratégique (espionnage ciblant télécoms et institutions), et la déstabilisation (sabotages, DDoS, opérations d'influence). L'ANSSI appelle à un renforcement généralisé de la supervision, à une sécurisation accrue des SI et à une plus grande réactivité face aux vulnérabilités publiées. Les prochaines années verront croître l'exigence de résilience cyber, tant pour les entités publiques que privées.

« Les attaquants liés à l'écosystème cybercriminel ou réputés liés à la Chine et la Russie constituent les trois principales menaces. »

« En 2024, les attaques à finalité de déstabilisation ont connu une hausse, notamment par des groupes hacktivistes. »

4386

événements de sécurité traités par l'ANSSI en 2024, soit une augmentation de 15 % par rapport à 2023.

50% +

plus de la moitié des opérations de cyberdéfense de l'ANSSI ont été déclenchées à la suite de l'exploitation de vulnérabilités sur des équipements de bordure.

x2

le nombre d'attaques par déni de service distribué (DDoS) a doublé en 2024 par rapport à 2023, avec une activité accrue pendant la période des Jeux Olympiques et Paralympiques de Paris 2024.

Pour la première fois, la France attribue formellement des activités cybercriminelles (APT28) au renseignement russe !

En avril 2025, l'État français, par la voix du Ministère de l'Europe et des Affaires étrangères a, pour la première fois, attribué des activités criminelles (APT28) au renseignement russe. Le Ministère a, dans une communication du 29 avril 2025, indiqué que « la France condamne avec la plus grande fermeté le recours par le service de renseignement militaire russe (GRU) au mode opératoire d'attaque APT28, à l'origine de plusieurs cyber-attaques contre des intérêts français » et précise que « depuis 2021, ce mode opératoire d'attaque (MOA) a été utilisé dans le ciblage ou la compromission d'une dizaine d'entités françaises. Ces entités sont des acteurs de la vie des Français : services publics, entreprises privées, ainsi qu'une organisation sportive liée à l'organisation des Jeux olympiques et paralympiques 2024. Par le passé, ce mode opératoire a également été utilisé par le GRU dans le sabotage de la chaîne de télévision TV5Monde en 2015, ainsi que dans la tentative de déstabilisation du processus électoral français en 2017 ».

Le mode opératoire d'attaque APT28 contre des entités françaises depuis 2021 a été décrit dans un document technique rédigé à partir des constatations réalisées par le Centre de coordination des crises cyber (C4), qui réunit dans sa forme technico-opérationnelle l'ANSSI, la DGSE, la DGSI, le COMCYBER et la DGA . Ministères, entreprises du secteur de la défense, think tanks, entité impliquée dans l'organisation des JOP24... Les cibles françaises récentes d'APT28 sont nombreuses, et principalement visées à des fins d'espionnage, voire de déstabilisation.

5.2 REGARDS CROISÉS DES EXPERTS DU SECTEUR

Maxime ALAY-EDDINE
CEO

2024 : une année record pour les vulnérabilités

« L'année 2024 s'est distinguée avec plus de 40 000 nouvelles entrées dans la base CVE. Face à cette avalanche – plus de 100 vulnérabilités par jour ! – il est crucial d'adopter une stratégie de priorisation claire et actionnable pour éviter que les équipes ne se noient sous l'information. Les RSSI peuvent s'appuyer sur des approches modernes comme la priorisation 3D, qui combine l'analyse des scores techniques (CVSS, EPSS) avec des données officielles issues d'autorités reconnues (CERT-FR de l'ANSSI, CISA KEV aux États-Unis). Faciles à automatiser et à intégrer, ces méthodes permettent d'éliminer jusqu'à 90 % des vulnérabilités non critiques, libérant ainsi les équipes pour se concentrer sur les véritables menaces : bien gérer ses vulnérabilités, c'est capter le signal et éliminer le bruit. »

Roland ATOUI
CEO

Fabricants IoT : face aux cybermenaces et aux nouvelles obligations

« Les objets connectés envahissent notre quotidien, mais derrière cette innovation se cachent de nouvelles menaces. En novembre 2024, le groupe Matrix a exploité des appareils mal sécurisés pour mener des attaques DDoS massives. Avec la Directive RED (2025) et le *Cyber Resilience Act* (2027), les fabricants et les organismes de notifications font face à des exigences strictes de sécurité et de certification. CyberPass, notre plateforme SaaS, leur permet d'automatiser et de simplifier la mise en conformité des produits connectés, tout en réduisant coûts, efforts et délais. »

Frédérique BAJAT
Product Owner Surveillances et Remédiations

De l'importance de se protéger face à la pratique croissante du cybersquatting

« Les cybercriminels usent de manière grandissante de noms de domaine pour mener leurs attaques, enregistrant souvent des noms d'apparence légitime pour faciliter la perpétration de fraude. L'entreprise visée est exposée à des pertes financières, atteintes réputationnelles et sécuritaires. Cette pratique, le cybersquatting, s'avère très aisée et est marquée par une utilisation croissante des nouvelles extensions génériques (.poker, .music, .paris...). L'enjeu pour les entreprises est de protéger leurs clients et leur marque, en sécurisant leurs noms de domaine, au risque d'affaiblir leur image. Il est donc essentiel de mettre en place des stratégies de surveillance afin de détecter au plus tôt les noms de domaine frauduleux et de réagir via des mesures appropriées en cas d'usurpation. »

THALES

Walter CAPILATTI
VP Cybersecurity Premium Services Business Line Thales

Une évolution rapide du paysage cyber, caractérisée par une sophistication des stratégies d'attaque

« En 2025, notre équipe mondiale d'intelligence des menaces cyber (CTI) Thales prévoit une sophistication des attaques et l'intégration accrue de l'intelligence artificielle dans les procédures des attaquants.
Les tendances clés incluent l'augmentation des campagnes de ransomware, des risques sur la chaîne d'approvisionnement et l'exploitation de vulnérabilités liées aux objets connectés et équipements physiques. Les organisations doivent adopter une approche cyber globale en surveillant leurs infrastructures IT et OT grâce à des Centres de supervision de Sécurité. Ils doivent développer des stratégies de réponse aux incidents, soutenues par des informations sur les menaces via des services d'intelligence cyber pour identifier proactivement les failles et renforcer leur posture de sécurité. »

IDAKTO

Stéphane CAUCHIE
Security Innovation Officer

Face à la fraude, une protection proactive de l'identité

« En 2025, les cybercriminels continueront d'adapter et d'affiner leurs techniques, exploitant les vulnérabilités des systèmes d'authentification traditionnels et les capacités avancées de l'IA pour contourner les protections existantes. Avec la démocratisation des portefeuilles d'identité, une nouvelle approche de la protection des utilisateurs émerge. Un Wallet proactif intégrant des mécanismes de détection de fraude avancés constitue une approche innovante. Grâce à l'analyse en temps réel des comportements suspects, ces solutions visent à anticiper et neutraliser les attaques avant qu'elles n'affectent l'utilisateur, tout en garantissant la confidentialité. Face à des attaques toujours plus sophistiquées, l'innovation demeure notre meilleure défense. »

Phragma

Frédéric CERCLET
Gérant

L'essor des fraudes à l'identité numérique: les défis d'une sécurité homogène et interopérable

« L'usurpation d'identité continue de progresser, évoluant au rythme des avancées technologiques qui rendent ces attaques de plus en plus accessibles aux cybercriminels. Ce phénomène se manifeste notamment par l'utilisation croissante de deepfakes, visant à contourner les systèmes d'authentification par reconnaissance faciale ou à rendre plus crédibles les arnaques en ligne. L'élaboration de cadres réglementaires et techniques constitue un enjeu fondamental pour le développement et la crédibilité du marché de l'identité numérique. Des avancées ont été réalisées, comme la certification PVID, tandis que l'adoption de l'EUDI Wallet prévue pour 2026 représente une avancée prometteuse, offrant de nouveaux usages aux citoyens tout en garantissant le contrôle de leurs données grâce au principe ZKP. »

rubycat

Jonathan CLAIREMBAULT
CTO

Talon d'Achille : la chaîne d'approvisionnement

« Les nombreuses divulgations de données personnelles des derniers mois, associées à la montée en puissance du *social engineering* assisté par l'IA, vont intensifier le risque sur la chaîne d'approvisionnement.
De plus, dans ce contexte international ou les cartes sont rebattues, il faut s'attendre a des attaques étatiques assistées par certains fournisseurs. Face à cela, la souveraineté numérique, la formation, la supervision des tiers, le «*Zero Trust*» et l'analyse comportementale seront essentiels pour sécuriser l'écosystème numérique. »

Benjamin COSTÉ
Chercheur en cybersécurité

L'essor de la menace informationnelle

« Les infrastructures numériques ne sont plus les seules cibles des attaquants qui menacent désormais nos cerveaux. Comme le montrent les événements récents (élections en Roumanie, opération *overload* contre les journalistes, campagne RRN visant les medias européens, etc.), la menace se généralise et s'intensifie. Les défis sont immenses : hybridité des modes opératoires cyber et informationnel, démocratisation de l'IA générative qui brouille notre relation à l'information, gestion du facteur humain… En réponse, la défense peine à se structurer notamment du fait des multiples champs d'expertise impliqués (informatique, droit, psychologie, géopolitique…).
Ce processus de mutation globale devrait se poursuivre encore en 2025, appelant à un effort global d'adaptabilité et de résilience. »

Luc DECLERCK
Directeur Général

Maîtriser le risque tiers : l'enjeu clé de NIS 2 et DORA»

« Avec NIS 2 et DORA, l'évolution du cadre réglementaire vient répondre, sans surprise, à une accélération de l'état de la menace, où l'on comptabilise un nombre croissant de cyberattaques réussies par le biais de la compromission d'un tiers (fournisseur, partenaire, client). Face à cette réalité, il est urgent de proposer des solutions efficientes, capables d'aider les organisations et les entreprises à passer à l'échelle sur la maîtrise du risque tiers. »

François DERUTY
Chief Intelligence Officer

Les équipements de bordure : cible privilégiée des acteurs de la menace

« Au cours des derniers mois, une tendance notable en cybersécurité a été l'intensification des attaques ciblant les *edge devices*, illustrées par des menaces comme Volt Typhoon ou PolarEdge. Menées par des groupes d'attaquants sophistiqués, elles visent particulièrement les dispositifs produits par des acteurs plus modestes de l'industrie. Les cybercriminels exploitent l'IA pour mener une reconnaissance automatisée des vulnérabilités présentes sur ces équipements de moyenne gamme, leur permettant ainsi de déployer des infrastructures malveillantes de manière plus efficace. Cette tendance souligne l'urgence pour les entreprises de renforcer la sécurité de leurs appareils périphériques, d'assurer une supervision étendue de leur système d'information ainsi que la résilience de leur supply chain. »

David DUBUS
Président

La nécessité d'une approche systémique de la cybersécurité

« Longtemps considérée comme une problématique technique, nous observons ces dernières années la prise en compte du facteur humain indispensable à une couverture optimale de la sécurité des systèmes d'information. Cependant, ce rééquilibrage aussi nécessaire qu'il soit ne doit pas mettre au second plan la nécessité de continuer à identifier les vulnérabilités des services et applications déployés. À ces deux piliers indissociables, il est capital d'y adjoindre la mise en place d'une gouvernance : unique dispositif permettant de vérifier que l'évolution de son niveau de maturité cyber est conforme aux objectifs fixés. »

Khadija HUEBRA
Directrice Générale Adjointe

Quand le phishing se dope à l'IA, le DMARC est un rempart de choix

« Le *phishing* représente, selon l'ANSSI, la part la plus importante des cyberincidents enregistrés au sein des entreprises françaises. Sa force de frappe est désormais renforcée par les capacités de l'IA générative. L'usurpation d'identité numérique devient donc un défi stratégique primordial pour les entreprises, dont la réputation peut être entachée. Face à ce constat, la mise en place d'un protocole DMARC rigoureux est impérative. Il est urgent d'accompagner les experts en sécurité en analysant les configurations DNS et en identifiant les vulnérabilités susceptibles d'être exploitées, tout en fournissant des recommandations précises pour renforcer la sécurité des domaines. Face à des menaces diversifiées et sophistiquées, une sécurisation proactive de l'identité numérique devient indispensable. »

Philippe LOUDENOT
Directeur stratégie cybersécurité

Vos données, un enjeu crucial

« Vos données sont des mines d'informations précieuses qu'il convient de protéger. Pourtant, tous les jours, des données sensibles sont transférées, échangées sans protection. Des solution françaises, souveraines et conçues pour répondre aux exigences des entreprises en matière de sécurité et de confidentialité des données sensibles existent. Alliant simplicité d'utilisation, sécurité avancée et conformité réglementaire, elles proposent une alternative fiable aux outils de transfert de fichiers traditionnels tout en garantissant une protection optimale des échanges. Les choisir, c'est opter pour des solutions qui protègent vos données, respectent la réglementation européenne et vous assurent une tranquillité d'esprit totale dans la gestion de vos fichiers sensibles. »

Philippe LUC
CEO et Cofondateur

Les vulnérabilités humaines : premier vecteur d'attaque

« La menace cyber évolue rapidement, avec une montée de l'ingénierie sociale automatisée. Les cybercriminels utilisent l'IA pour orchestrer des attaques sophistiquées exploitant tous les aspects de l'identité numérique, tant professionnelle que personnelle. 70 % de l'exposition des dirigeants provient de leur vie personnelle et de leur entourage ! Ces attaques peuvent aller de la fraude au président à la manipulation d'informations via des DeepFakes. Il est donc essentiel que les organisations impliquent leurs équipes dans une démarche outillée de protection de l'empreinte numérique : avec un triple avantage : protéger les entreprises face aux attaques, protéger les employés contre les fraudes personnelles et se conformer à la réglementation NIS2. »

Jean-Yves MARION
Professeur

IA Cyberoffensive : Systèmes d'Armes Cyber Autonomes

« L'objectif de l'agent autonome M32 est d'infiltrer une entreprise de haute technologie; il embarque les dernières mises à jour et peut être considéré comme un des Systèmes d'Armes Cyber Autonomes (SACA) les plus avancés. M32 a étudié sa cible et lance l'attaque. Après plusieurs semaines d'infiltration, l'agent M32 exfiltre les informations pertinentes et corrompt des données sensibles. La capacité d'analyse, de génération et de prise de décision de l'IA permet d'envisager la construction de SACA, à l'instar de l'agent fictionnel M32. Les campagnes de cyberattaques pourraient alors être totalement automatisées, amplifiant le nombre d'attaques, leur vitesse d'exécution, et amplifiant les conséquences et les dégâts. »

Catherine NOHRA CHINA
CEO

Sécuriser les chaînes d'approvisionnement pour mieux se protéger des cybermenaces

« La menace informatique en 2024 affecte toute la chaîne d'approvisionnement (fournisseurs, partenaires et sous-traitants). Cette *supply chain* est de plus en plus ciblée par les cybercriminels qui exploitent les vulnérabilités d'un maillon pour accéder aux systèmes et aux données d'un autre. Dans la plupart des cas, les techniques d'attaques ciblent les données et les droits d'accès dont elles exploitent les mauvaises configurations. L'identification et l'évaluation des risques liés aux partenaires et sous-traitants devient donc plus que cruciale pour mieux se protéger et c'est notamment ce que prévoit la directive NIS 2 qui tend à renforcer la sécurité de la *supply chain* via la mise en place de contrôles de sécurité incluant audits et exigences contractuelles. »

Benoit PARIZET
Directeur Général Adjoint – Secteur Public

Remettre la confiance numérique au cœur des usages publics

« La donnée est au cœur de la transformation de l'action publique. Les usages qu'elle permet sont multiples : optimisation des processus métiers, renforcement de la maîtrise budgétaire, amélioration de la relation avec les usagers, facilitation de l'attribution d'aides publiques... Mais ils s'accompagnent d'enjeux. En premier lieu : la protection des données, souvent sensibles. De la collecte au stockage, en passant par le traitement, chaque étape de la chaîne de valeur de la donnée doit être maîtrisée. Or, les petites collectivités, souvent moins protégées, sont particulièrement exposées. Bien que l'État encourage largement le recours au *Cloud* à travers la doctrine « *Cloud* au centre », qui vise à renforcer la sécurité, cette approche n'est ni une obligation pour les petites collectivités, ni une garantie de la protection de leurs données. Il apparaît donc nécessaire que les services traitant des données sensibles privilégient des solutions certifiées SecNumCloud, et ce, quelle que soit la taille de l'administration concernée, afin d'assurer le plus haut niveau de sécurité et de garantir la confiance numérique dans nos services publics. »

Dr. Florin PAUN
Président Cofondateur

La souveraineté de nos industries et sociétés dépend de l'accès à des données pertinentes

« L'avenir de nos industries sera construit sur des données pertinentes et fiables, ou ne connaîtra aucun avenir du tout ! La souveraineté industrielle se construit sur des solutions innovantes permettant d'accéder à des données pertinentes et de réduire le flux de données fausses et biaisées lors de toutes les utilisations de l'IA. La qualité, la pertinence des données ne peut être imposée à toutes les parties prenantes, mais elle est le résultat des processus cognitifs, des capacités innovantes à intégrer démocratiquement toute la diversité des opinions et perceptions des impacts des données dans un processus hautement inclusif, grâce, par exemple, à la nouvelle typologie de l'IA Qualificative - QuAI, reconnue par la communauté scientifique ayant complété le Paradoxe Condorcet et le théorème Arrow. »

Caroline RESTOUX
Manager & Lead Consultant Conformité & Gouvernance Cybersécurité

2025 : une année stratégique pour les responsables de la sécurité de l'information

« Au-delà de la prise en compte des menaces qui ne cessent d'évoluer tant sur leur nombre que sur leur typologie, les organisations font face à de plus en plus d'enjeux stratégiques et réglementaires. NIS2, DORA, CRA, IA Act, ou encore le projet de certification des sous-traitants en cours d'étude par la CNIL : l'année 2025 s'annonce riche et orientée conformité ! Ces différentes réglementations poussent les organisations à se structurer et à penser la sécurité de manière multi-référentielle. Une bonne base pour l'implémentation de l'ensemble de ces réglementations ? L'implémentation de l'ISO/CEI 27001 par le biais de la prise en compte de ses risques et dans une démarche d'amélioration continue. »

NetExplorer

Bertrand SERVARY
CEO

Reprendre la main sur nos dépendances technologiques

« Les crises récentes – sanitaires, énergétiques, géopolitiques – ont révélé un fait désormais incontestable : la dépendance technologique est une vulnérabilité systémique. En 2025, nombre d'organisations se retrouvent encore captives d'infrastructures, de logiciels ou de services développés hors de leur sphère de souveraineté. Cette dépendance conditionne notre capacité à protéger les données et à assurer la continuité de nos activités. Reprendre la main suppose d'identifier les points critiques de la chaîne de valeur numérique, de soutenir des alternatives européennes, et d'investir dans l'indépendance à long terme. Il ne s'agit pas de repli technologique, mais de stratégie d'émancipation. La souveraineté numérique commence par la capacité à choisir librement, sans contrainte extérieure. »

FOCUS BAROMÈTRE DOCAPOSTE-CYBLEX DE LA CYBERSÉCURITÉ 2024

Ce baromètre national est né d'une volonté partagée par Docaposte et Cyblex Consulting de mesurer année après année l'évolution de la maturité cyber des entreprises et organisations publiques.
Les résultats sont tirés d'entretiens téléphoniques réalisés en 2024 auprès de plus 450 répondants, parmi lesquels 27% travaillent pour le secteur public et 53% sont des spécialistes IT.
Résultats et parallèle avec la première édition.

Baromètre de la cybersécurité Docaposte - Cyblex 2024

disponible en téléchargement sur :
urlr.me/RXcF89

Les 7 grands enseignements du baromètre Docaposte-Cyblex 2024 :

1. Les entreprises se sentent davantage menacées que l'année dernière (+10pts)
Le risque varie selon la taille de l'entreprise et le secteur d'activité :
Le top 5 des secteurs qui se sentent le plus être une cible sont : le secteur financier, les services administratifs, l'hébergement et la restauration, les services de production d'eau et d'électricité et les acteurs publics.
Plus l'entreprise est grosse, plus elle se sent fortement exposée (29% entre 50 et 249 salariés vs 57% plus de 1000 salariés).

2. Les efforts mis en place pour réduire les risques sont en hausse (+8 pts)
Des disparités budgétaires sont observables en fonction de la taille des entreprises ou organisations. Le budget cyber augmente pour 2/3 des entreprises :
• Une hausse qui concerne beaucoup plus d'entreprises que lors de la dernière édition (+21 pts),
• Une hausse portée par les entreprises de plus de 50 salariés.

3. Le nombre de cyberattaques est plus élevé qu'en 2023 (+11 pts) avec 1/3 des répondants qui déclarent avoir été victimes d'une cyberattaque au cours des 12 derniers mois
Des typologies d'attaques variables selon la taille de l'entreprise, marquant une professionnalisation des attaquants avec la mise en place d'actions ciblées.

Désormais, le 1er impact n'est plus le vol de données qui était en tête en 2023 mais le blocage des systèmes d'information (18%) :

• les TPE et PME subissent du *phishing* (33%) et du *ransomware* (27%),

• les ETI et grands groupes subissent davantage l'arnaque au président (3 fois plus que les autres types d'entreprises) et le DDOS déni de service.

33% Phising

27% Ransomware

24% Vol/perte de données

4. Les doutes sur l'efficacité des actions restent identiques à l'année dernière avec 1/3 des entreprises qui n'ont pas confiance dans les actions qui ont été mises en place

Le top 3 des actions engagées sont :
• La sécurisation des postes de travail,
• La mise à jour régulière des logiciels,
• Une gestion renforcée des mots de passe.

Les plus fortes progressions sont :
• La sécurisation physique des accès,
• La sécurisation du réseau d'entreprise,
• La sécurisation des postes de travail,
• Les exigences vis-à-vis des fournisseurs.

5. L'intérêt des entreprises vis-à-vis d'un système souverain est en nette progression avec 52% des répondants qui jugent important ou très important de disposer d'une solution souveraine (vs. 20% en 2023). Plus que les entreprises, les acteurs publics jugent la souveraineté des solutions comme un critère « très important ».

6. L'accompagnement par un partenaire spécialisé devient majoritaire : 2/3 des entreprises déclarent faire appel à une ressource externalisée traduisant ainsi le fait que la cybersécurité est une réelle expertise métier.

7. Le *Cloud* reste encore en dehors du *scope* de la cybersécurité pour la majorité des entreprises : seul 1/3 des entreprises étendent leurs actions de cybersécurité dans le *cloud*.

5. Point sur la menace informatique
Observatoire ACN de la filière de la Confiance Numérique 2025

Olivier Vallet
Président Directeur Général, Docaposte

« Les technologies numériques sont au centre des enjeux sociétaux, géopolitiques, environnementaux et économiques.

Ces évolutions majeures s'accompagnent d'une montée en puissance de la cybercriminalité, qui constituent aujourd'hui un défi pressant pour l'ensemble des acteurs.

Tandis que la réalité de cette menace est désormais incontestable, les grandes entités ont réagi en conséquence en investissant massivement dans leur sécurité et en intégrant des technologies de pointe afin d'anticiper et de contrer les cyberattaques. Cependant, les acteurs de moindre envergure, les TPE, ETI, collectivités, dépourvus des ressources et de l'expertise nécessaires, se retrouvent démunis face à ces enjeux. Le sujet de la cybersécurité deviendra encore plus crucial avec l'essor des technologies émergentes comme l'intelligence artificielle.
Ces innovations, bien que prometteuses, élargissent la surface d'attaque des cybermenaces.

Nous devons accompagner ces structures moins bien protégées afin de limiter notre dépendance excessive à l'égard des géants technologiques étrangers pour maîtriser les infrastructures de cybersécurité, notamment lorsqu'il s'agit de données sensibles. »

Christophe Vendran
Président Directeur Général, Cyblex

« Chaque année, les enjeux de la cybersécurité prennent une ampleur nouvelle, reflétant la complexité croissante d'un monde toujours plus interconnecté.

Une disparité notable persiste encore entre les grandes organisations souvent bien équipées, et les TPE/PME qui restent très vulnérables.

Ce baromètre invite chaque acteur à mesurer pleinement l'importance d'une posture proactive pour faire de la cybersécurité non pas un frein, mais un levier de confiance et de croissance.

Les cybermenaces jouent désormais un rôle structurant dans des secteurs essentiels portés par des écosystèmes numériques en pleine expansion.

La sécurité grandit lorsqu'elle est partagée. Ensemble, partageons ces connaissances et renforçons notre résilience face aux défis de la cybercriminalité. »

6. LES TENDANCES DE MARCHÉ

6.1 LES TENDANCES GÉNÉRALES

6.1.a. La croissance de la filière française

L'année 2024 confirme le ralentissement du rythme de croissance amorcé en 2023, après une année de forte croissance. La croissance annuelle globale s'établit à 6,4% en 2024, un niveau similaire à celui de 2023 (6,8%), mais bien en dessous des performances exceptionnelles observées entre 2021 et 2022 (11,3%).

Ce ralentissement s'explique en partie par un contexte économique et politique incertain. L'année 2024 a été marquée par des tensions budgétaires persistantes, ainsi que par des élections législatives anticipées et un changement de gouvernement, qui ont eu un impact négatif sur les décisions d'achat public. Or, le secteur public représente une part significative de la demande dans la confiance numérique, notamment au niveau des collectivités territoriales (communes, petites structures de l'État, etc.).

La sécurité numérique poursuit sa tendance ralentie : après une croissance modérée de 3,8 % en 2023, le segment progresse de 4 % en 2024. Le recul des grands projets liés à l'identité et à la biométrie, combiné à une demande publique moins soutenue, explique ce tassement.

La cybersécurité affiche une croissance plus soutenue, bien que légèrement en retrait : 9,2 % en 2023, puis 8 % en 2024. La dynamique reste tirée par les produits (logiciels, matériels, éléments sécurisés), qui progressent de 9,2 %, tandis que les services ralentissent à 6 %, affectés par les arbitrages budgétaires des clients dans un environnement économique plus contraint.

Du côté des industriels, les *leaders* de la filière enregistrent également des croissances plus modérées en 2024, à l'image de Thales, dont l'activité dans l'identité numérique progresse d'environ 1 %.

Quelques exceptions se distinguent néanmoins, notamment parmi les ESN émergentes comme Nomios ou I-Tracing, qui continuent d'afficher une croissance supérieure à la moyenne du secteur.

L'année 2022 demeure un point haut dans la dynamique récente de la filière, avec une croissance globale supérieure à 11 %.

La cybersécurité avait renoué avec ses tendances de long terme (11,5 %), tandis que la sécurité numérique atteignait un niveau exceptionnel (11 %), portée par des projets d'envergure en identification et contrôle d'accès, menés notamment par Thales, Airbus, IN Groupe et IDEMIA.

Plusieurs facteurs avaient amplifié cette dynamique : un effet rebond post-COVID, une hausse des prix liée à la pénurie de semiconducteurs (impactant positivement la valeur des produits sécurisés), et un contexte porteur, marqué par la montée des tensions géopolitiques, les projets de sécurisation aux frontières et les préparatifs des grands événements comme les JO de Paris 2024.

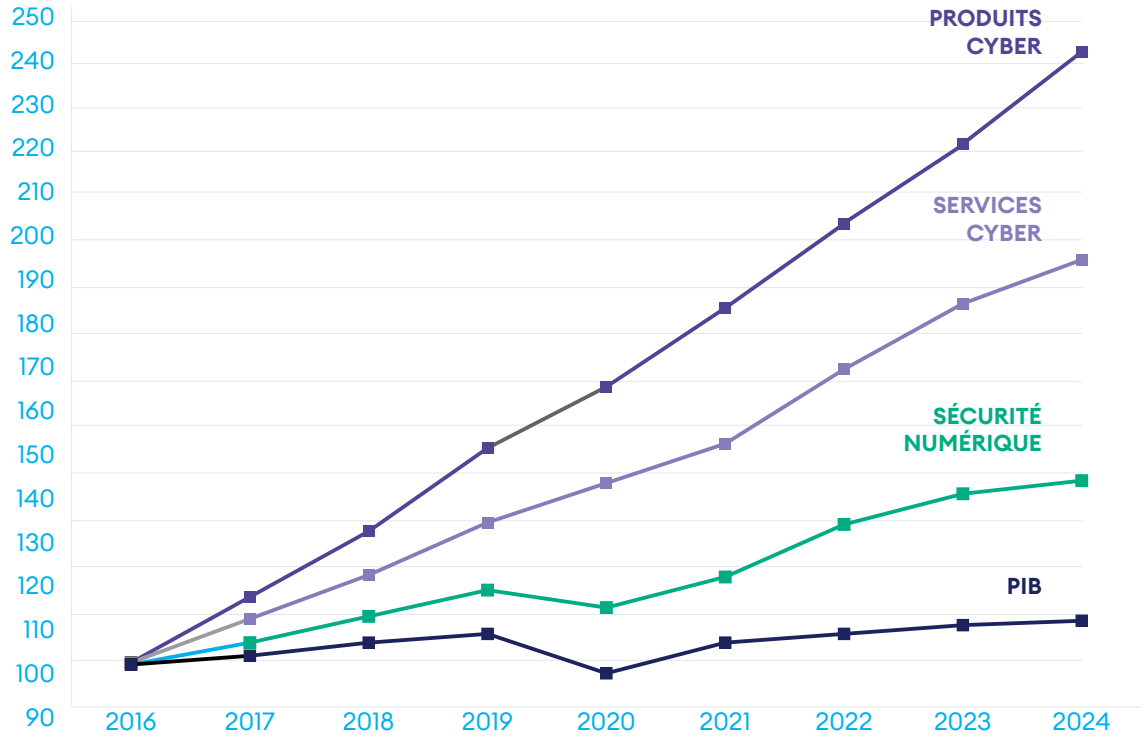
« Le rythme de croissance global de la filière se stabilise en 2024, autour de 6% »

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 2017-2024.

Croissance France comparée 2017-2024

Croissance							
Segments	2018	2019	2020	2021	2022	2023	2024
Confiance numérique	8,2%	8,5%	3,6%	7,3%	11,3%	6,8%	6,2%
Produits cyber	13,9%	14,0%	10,9%	8,8%	12,6%	9,0%	9,2%
Services cyber	9,9%	10,3%	5,8%	8,9%	10,3%	9,4%	6,6%
Sécurité numérique	4,7%	4,8%	-1,7%	5,2%	11,0%	3,8%	4,0%
IA de confiance							9,3%
PIB	1,9%	1,8%	-7,8%	6,8%	2,5%	0,9%	1,1%

Source: INSEE, FMI pour 2024



Source : DECISION Etudes & Conseil

6.1.b. Les marchés de la filière

I / Les marchés en 2024

Comme le montre le diagramme, le secteur public au sens large, c'est-à-dire en incluant les transports et la santé, représente près d'un tiers du marché français (6,3 Mds € en 2024), les deux tiers restants provenant du secteur privé (13,3 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'État 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.

Au-delà du secteur public, qui reste le premier marché et un levier important de croissance,
les secteurs banque / finance / assurance et énergie sont, depuis plus de trois ans, les principaux moteurs de la filière, devant la santé.

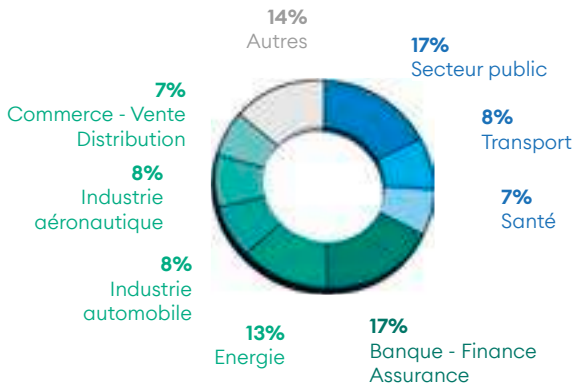
II / L'émergence d'un marché des PME/TPE et des petites collectivités territoriales

La série de diagrammes ci-contre, issue de l'édition 2024-2025 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'État, les Opérateurs d'Importance Vitale (OIV) et les grandes entreprises (hors OIV) représentent plus de 75% du marché des grandes entreprises de la filière, et plus de 80% de leurs perspectives de croissance pour les années à venir.

Ces grandes entreprises fournisseurs de solutions de confiance représentent 48% du chiffre d'affaires de la filière en France en 2024 (77% 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 : État, OIV et grands comptes privés.

Principaux marchés de la filière en 2024



Source : DECISION Etudes & Conseil, questionnaire renseigné par les entreprises de la filière en de 2022 à 2025.
Réponse en % des répondants pondérés par leur poids dans la filière.
L'échantillon représente 8% de la filière en chiffre d'affaires.

À contrario, l'État et les OIV ne représentent que 19% du marché des PME et TPE de la filière. Ce sont les grandes entreprises (31%), les PME / TPE (28%) 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 de l'activité des PME et TPE de la filière, on observe l'émergence de deux marchés :

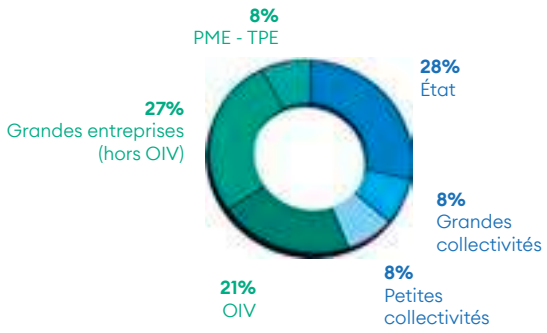
• Celui des collectivités locales, y compris les petites collectivités locales. Par extrapolation, on peut estimer le marché des petites collectivités locales à 3,5 milliard d'euros en 2024.
• Mais surtout, le développement du marché associé au besoin de produits et services de confiance de la part des PME et TPE françaises. Par extrapolation, on peut estimer ce marché à 3,3 milliards d'euros en 2024. Ce marché se caractérise par des offres dédiées : offres standardisées, déploiement rapide, faible coût, souvent sans support *hardware*...

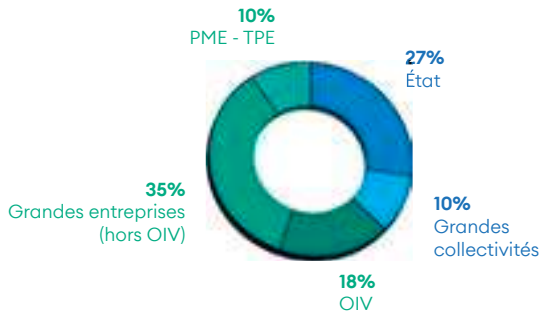
Le développement de ce marché des PME et TPE françaises a été ralenti en 2020 par la crise du COVID. En effet, les PME et TPE françaises ont été plus affectées par les restrictions associées au COVID que les grands clients traditionnels de la filière de la confiance numérique (État, OIV, grandes entreprises) 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.

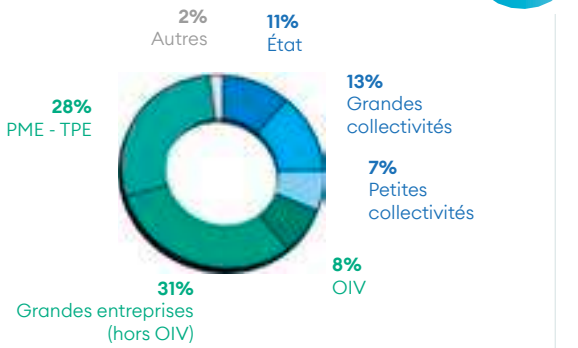
Enfin, bien qu'encore négligeables, on observe l'apparition de marchés de sécurisation des associations ou encore des particuliers.

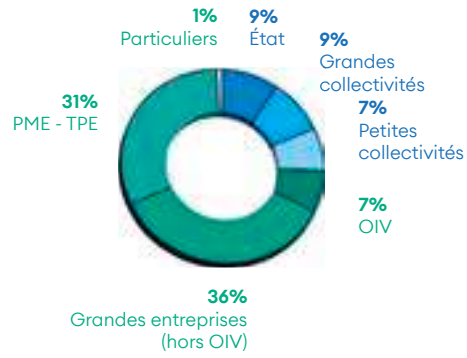
Grandes entreprises





TPE - PME





Source : DECISION Etudes & Conseil, questionnaire renseigné par les entreprises de la filière en de 2022 à 2025.
Réponses en % des répondants pondérés par leur poids dans la filière.
L'échantillon représente 8% de la filière en chiffre d'affaires.

POINT DE VUE

CHRISTOPHE HUSSON

• GÉNÉRAL DE DIVISION
• CHEF DU COMCYBER-MI

« L'Alliance pour la Confiance Numérique (ACN) joue un rôle majeur dans la structuration, l'animation et la représentation des entreprises du numérique, participant à la consolidation d'une filière industrielle et technologique stratégique, dans un domaine en mutation rapide.

Dans ce contexte, le commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI) s'impose comme un acteur central de la lutte contre la cybercriminalité. Service à compétence nationale rattaché au directeur général de la Gendarmerie nationale, le COMCYBER-MI repose sur quatre piliers structurants : l'anticipation des menaces, la stratégie ministérielle de lutte contre la cybercriminalité, l'appui opérationnel aux services d'enquête, et la formation. En moins de deux ans d'existence, il a démontré sa capacité à mobiliser des compétences rares, à agir en soutien des grands événements comme les Jeux Olympiques et Paralympiques de Paris 2024, à projeter des experts en métropole comme en outre-mer, et à sensibiliser les acteurs économiques via des outils comme le MOOC Sensycrise par exemple.

Pour autant, la cybercriminalité ne cesse de se transformer. Les réseaux criminels se professionnalisent, exploitent les failles du numérique, et menacent la sécurité des citoyens, des entreprises et des institutions.

Face à cela, la réponse doit être collective. C'est pourquoi la collaboration entre le COMCYBER-MI et l'ACN revêt une importance toute particulière. Elle se concrétise à travers une convention structurée autour de quatre axes : le partage d'informations, la participation conjointe aux travaux, l'échange réciproque de productions, et la mise en œuvre d'actions ciblées. Elle permet d'unir les efforts publics et privés pour construire des solutions de confiance à la hauteur des enjeux actuels, qu'ils relèvent de la souveraineté, de la sécurité ou de la compétitivité.

En associant la force de l'action publique à l'agilité de l'innovation industrielle, ce partenariat renforce notre capacité collective à anticiper les menaces, à répondre efficacement aux crises cyber et à bâtir une résilience nationale. Ensemble, nous portons une ambition commune : faire du cyberespace un espace sûr et digne de confiance, au service de nos libertés, de notre économie et des valeurs de la République.

« Nos forces, pour votre cyberprotection ». »

6.2 LES TENDANCES RÉGLEMENTAIRES

6.2.a Europe : vers un marché unique du numérique de confiance

La transformation numérique continue de s'opérer au sein de l'UE. Dans un contexte géopolitique où les tensions sont vives, la concrétisation d'un marché unique du numérique de confiance est plus que jamais une nécessité pour tous les acteurs de la filière. Les nouveaux risques qui découlent des nouveaux usages amènent les institutions européennes et les états membres à réfléchir aux moyens d'adapter leur arsenal législatif à ces évolutions et de permettre à l'Union européenne de mieux maîtriser 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 croissantes dans le cyberespace. Cette année encore, 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. Comme l'année 2024, l'année 2025 est une année charnière du point de vue institutionnel en Europe. En partenariat avec son homologue allemand Teletrust, l'ACN a publié en avril 2024 ses priorités européennes et recommandations afin d'accélérer la transition vers un marché unique du numérique de confiance et n'a pas manqué de les transmettre à l'ensemble de eurodéputés. L'ACN souhaite s'inspirer de la réussite de cette coopération avec ses homologues allemands pour l'étendre et ambitionne de concrétiser des partenariats avec les représentants de la filière de la confiance numérique dans plusieurs autres pays européens. L'objectif de cette coopération des représentations de filière intereuropéennes est de parvenir à mieux se connaitre et à élaborer des messages communs pour les porter avec plus de force.

Document ACN « Priorités de la filière de la confiance numérique pour les élections européennes 2024 »

disponible en téléchargement sur :
urlr.me/rwy7zJ

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 états membres devront, dès 2027, permettre à tout citoyen européen de bénéficier gratuitement d'un portefeuille d'identité numérique.

La concrétisation d'un cadre juridique européen pour l'intelligence artificielle

Le règlement sur l'intelligence artificielle (AI Act) a été adopté par le Parlement et le Conseil de l'UE en début d'année 2024, après 3 ans de négociations. L'AI Act a été publié au Journal Officiel de l'UE le 12 juillet 2024 et est entré en vigueur le 1er août 2024. Les premières interdictions prévues par le règlement sont désormais applicables et le dispositif s'étendra progressivement aux autres catégories d'usages en fonction du niveau de risque qui leur est associé.

Le 4 février 2025, la Commission européenne a publié des lignes directrices sur l'article 5 du règlement portant sur les pratiques interdites puis, le 7 mars 2025, l'acte d'exécution portant création du groupe scientifique a été adopté. La mise en œuvre complète de ce texte, guidée par le Bureau de l'IA qui se structure, est prévue pour 2026.

Rapport ACN « Analyse détaillée Règlement sur l'intelligence artificielle – AI ACT »

disponible en téléchargement sur :
urlr.me/SJU2sj

Le renforcement de la cybersécurité

Le règlement sur la cyberrésilience (*Cyber Resilience Act* - CRA) a été adopté 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*, ...). Le 20 novembre 2024, le règlement est paru au Journal Officiel de l'Union Européenne, et il est entré en vigueur le 10 décembre 2024. Celui-ci vise à établir des standards communs européens de cybersécurité pour les produits qui seront mis sur le marché interne européen. Le CRA vise également à renforcer la responsabilité des fabricants et des fournisseurs de produits comportant des éléments numériques (PEN) en imposant la mise en place de garanties de cybersécurité adéquates.
La mise en œuvre du CRA sera progressive : 18 mois après son entrée en vigueur, donc, a priori au printemps 2026, les organismes d'évaluation seront habilités à vérifier la conformité des produits. À compter de l'été 2026, les fabricants devront déclarer les vulnérabilités et incidents. D'ici à 2027, toutes les exigences du CRA s'appliqueront, y compris les normes minimales avant la commercialisation, la gestion des vulnérabilités et le devoir de transparence envers les utilisateurs.

Rapport ACN « Analyse détaillée – Règlement sur la cyberrésilience *Cyber Resilience Act* - CRA »

disponible en téléchargement sur :
urlr.me/urQveD

Par ailleurs, 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 à la Réserve Cyber européenne, le texte a été adopté par le Conseil de l'UE le 2 décembre 2024 avec l'amendement du *European CyberSecurity Act* l'accompagnant. Il est entré en vigueur le 4 février 2025.
Enfin, les états membres sont en train de transposer plusieurs textes dans leur droit national. La directive NIS2, la directive sur la Résilience des Entités Critiques (directive REC), ou encore les exigences du règlement DORA qui devaient être mis en œuvre entre la fin de l'année 2024 et le début de l'année 2025 sont en cours d'examen et de transposition au sein des pays membres de l'Union européenne.

Rapport ACN « Analyse détaillée directive NIS 2 »

disponible en téléchargement sur :
urlr.me/VWAHzj

La résilience opérationnelle numérique du secteur financier

Le règlement DORA et la directive associée sont entrés en vigueur le 16 janvier 2023. Ils fournissent un cadre réglementaire innovant qui s'attaque aux risques posés par la profonde transformation numérique des services financiers, l'interconnexion croissante des réseaux et des infrastructures critiques ainsi que par la multiplication des cyberattaques, de plus en plus sophistiquées, à l'encontre des acteurs du secteur financier. En parallèle, la révision des directives REC (Résilience des Entités Critiques) et NIS2 viennent renforcer le cadre général de cybersécurité.
Le règlement sur la Résilience opérationnelle numérique (DORA) définit les exigences uniformes pour renforcer et harmoniser la gestion des risques liés aux technologies de l'information et de la communication (TIC) et à la sécurité des réseaux et des systèmes d'information au niveau de l'UE. Il prévoit également la mise en place d'un mécanisme de surveillance direct des prestataires de services TIC critiques au niveau de l'UE.
Le règlement s'applique à l'ensemble des États membres de l'UE depuis le 17 janvier 2025. Au cours des deux prochaines années, la Commission publiera des actes délégués sur la base de projets finaux de normes règlementaires techniques et d'exécution.

Rapport ACN « Analyse détaillée règlement DORA »

disponible en téléchargement sur :
urlr.me/9M2Ubf

6.2.b Les initiatives nationales de la confiance numérique

Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité (transposition REC-NIS2-DORA)

Le 17 janvier 2023, la directive NIS 2 est entrée en application après avoir été publiée au Journal Officiel de l'Union européenne par la Commission européenne le 27 décembre 2022. Cette directive a pour vocation d'assurer un niveau commun élevé de cybersécurité dans l'ensemble de l'Union européenne afin de garantir un cyberespace de confiance pour les citoyens et les entreprises et à renforcer la coopération entre les états membres.
Les États membres disposaient de 21 mois pour la transposer en droit interne : elle aurait donc dû être transposée avant le 17 octobre 2024. Beaucoup de pays européens, dont la France, sont en retard sur ce calendrier.

La Commission a fourni également, en juillet 2023, des lignes directrices clarifiant l'application des actes juridiques sectoriels de l'Union.
Le 15 octobre 2024 lors du Conseil des Ministres, le ministre de l'Économie, des Finances et de l'Industrie, le ministre de l'Enseignement supérieur et de la Recherche, et la secrétaire d'État auprès du ministre de l'Enseignement supérieur et de la Recherche, chargée de l'Intelligence artificielle et du Numérique, ont présenté le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité permettant la transposition de la directive NIS 2 en droit français, ainsi que des textes REC et DORA. Le projet de loi a été déposé au Sénat le même jour qui a mis en place commission spéciale chargée d'examiner ce projet de loi.

>>> 24 janvier 2025 : L'ACN a été auditionnée par le Sénateur Olivier Cadic, Président de la Commission spéciale Cybersécurité, les Sénateurs Hugues Saury, Patric Chaize et Michel Canevet, rapporteurs sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

L'intégration des textes REC/NIS2/DORA dans un seul projet de loi de transposition démontre un effort manifeste de cohérence et l'ACN s'en félicite. En effet, la lisibilité des exigences et la bonne compréhension par les entités régulées de l'ensemble de l'édifice est un élément majeur de réussite dans l'objectif général d'amélioration du niveau de sécurité et de résilience de notre pays.
Pour atteindre cet objectif, l'ACN appelle à une transposition puis à une mise en œuvre la plus rapide possible des dispositions adoptées afin de répondre dans les meilleurs délais aux deux défis qui nous font collectivement face, que sont le renforcement de notre résilience collective mais aussi celui de notre autonomie stratégique. En effet, il est essentiel que ce texte soit un levier de développement pour l'écosystème français et européen de la confiance numérique combinant ainsi souveraineté et résilience.

La France dispose d'une filière de la confiance numérique très performante et agile composée d'entreprises de toutes tailles (grands groupes, ETI, PME et *start-up*) qui proposent des solutions adaptées et immédiatement disponibles pour répondre aux besoins générés par ce projet de loi.
Il apparaît également majeur que la mise en œuvre de ce texte s'accompagne d'un effort massif de communication, de sensibilisation, de diffusion de bonnes pratiques, d'accompagnement et de formation à destination des entités régulées qui, pour beaucoup d'entre-elles, seront soumises à des obligations en matière de cybersécurité pour la première fois.
L'ACN a été force de propositions pour diffuser les priorités de la filière dans les travaux parlementaires. Nous avons notamment proposé que les dispositifs soient complétés par un mécanisme d'incitation financière de type « Crédit d'impôt cybersécurité » afin d'alléger l'investissement des entités régulées (notamment les TPE-PME) et de les mettre en mesure de remplir leurs obligations. Un tel soutien public à l'effort de sécurisation du pays est susceptible de présenter un fort retour sur investissement, notamment si on le compare au coût de l'inaction et à ses effets sur tout le tissu économique et social national. Par ailleurs, des dispositifs de subvention européens dédiés à aider les entreprises, en particulier les PME, à se conformer aux nouvelles exigences en matière de cybersécurité, pourraient également être mis en place.
L'ACN souhaite également qu'une instance, associant les représentants de la filière, soit créée en vue de contribuer à l'élaboration des décrets et de suivre, dans le temps, leur mise en œuvre et leur efficience afin d'être en mesure de les adapter face notamment à l'évolution des techniques et des menaces. En vue de l'atteinte des objectifs du texte, des dispositions complémentaires pourraient être mises en place pour :
- renforcer la prise en compte du facteur humain dans le projet de loi ;
- obliger les entités régulées à se doter d'une politique de divulgation de vulnérabilités. ;
- prévoir, dans le dispositif, un encadrement législatif créant un doit commun pour les activités d'OSINT.

Le 12 mars 2025, le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité a été adopté au Sénat et transmis à l'Assemblée nationale pour examen. Une commission spéciale chargée d'examiner le projet s'est constituée le 8 avril 2025. Le projet de loi devrait être adopté à l'été 2025.

POINT DE VUE

OLIVIER CADIC

• PRÉSIDENT DE LA COMMISSION SPÉCIALE CYBERSÉCURITÉ AU SÉNAT
• SÉNATEUR REPRÉSENTANT LES FRANÇAIS ÉTABLIS HORS DE FRANCE
• VICE-PRÉSIDENT DE LA COMMISSION DES AFFAIRES ÉTRANGÈRES, DE LA DÉFENSE ET DES FORCES ARMÉES

« Présider la commission spéciale chargée d'étudier le projet de loi relatif à « la résilience des infrastructures critiques et au renforcement de la cybersécurité» fut pour moi une responsabilité exigeante mais essentielle. Ce texte, voté au Sénat le 12 mars 2025, est le fruit d'un travail rigoureux, concerté et profondément ancré dans les réalités du terrain. Il vise à transposer trois directives européennes majeures : REC, NIS2 et DORA. Mais au-delà d'une transposition, nous avons souhaité porter une vision : celle d'une cybersécurité solide, partagée, construite avec les professionnels pour les professionnels.

Mon état d'esprit a toujours été clair : il ne s'agit pas d'empêcher les cyberattaques – elles sont inéluctables – mais d'en limiter l'impact, de garantir la continuité, de bâtir une véritable résilience. Cela suppose d'éviter les injonctions contradictoires, comme l'introduction de « *backdoors* » dans les systèmes de chiffrement, qui affaibliraient nos défenses au lieu de les renforcer. Grâce à un amendement que j'ai défendu, cette dérive a été empêchée : le Sénat reste, à mes yeux, la maison des libertés.

Tout au long de nos travaux, j'ai voulu associer étroitement les acteurs économiques, les collectivités, les experts et les autorités de régulation. Le dialogue public-privé n'est pas un luxe, c'est une condition de succès. Nous avons organisé sept auditions publiques, consulté les représentants de la cybersécurité, les élus, les entreprises, pour bâtir un texte opérationnel, évitant toute surtransposition inutile. Car si la sécurité est un impératif, elle ne doit jamais devenir un fardeau illisible ou inapplicable.

J'ai alerté sur le risque d'un déséquilibre entre les obligations fixées par la loi et les détails laissés à une quarantaine de décrets : trop de zones grises, et l'administration seule aux commandes. C'est pourquoi nous avons formulé des recommandations claires : simplifier les mesures d'application, éviter la surtransposition ou la sous-transposition, accompagner les collectivités dans cette mutation et veiller à une vraie lisibilité des normes.

Ce texte n'est qu'un point de départ. Sa réussite dépendra de la qualité de sa mise en œuvre. Il devra être porté politiquement, non simplement géré techniquement. C'est à ce prix que nous renforcerons la confiance dans notre écosystème numérique.

Par ailleurs, le travail n'est pas fini, car il faudra avec l'Assemblée nationale parvenir à un accord sur un texte commun en commission mixte paritaire. C'est un objectif important que ce projet de loi soit adopté à la plus large majorité possible, car l'enjeu de la cybersécurité concerne tous les français.

Je salue le travail exceptionnel des trois rapporteurs de la commission spéciale que j'ai présidée pour préparer ce texte : Michel Canévet, Hugues Saury, Patrick Chaize. Toujours à notre écoute, Clara Chappaz, ministre déléguée chargée de l'intelligence artificielle et du numérique, aura été un heureux élément de continuité dans ce processus, ce qui est à souligner. »

POINT DE VUE

PHILIPPE LATOMBE

• PRÉSIDENT DE LA COMMISSION SPÉCIALE CYBERSÉCURITÉ À L'ASSEMBLÉE NATIONALE
• DÉPUTÉ DE LA 1ÈRE CIRCONSCRIPTION DE LA VENDÉE
• VICE-PRÉSIDENT DU GROUPE D'ÉTUDES ÉCONOMIE, SÉCURITÉ ET SOUVERAINETÉ NUMÉRIQUES

« Le projet de loi Résilience des infrastructures critiques et renforcement de la cybersécurité est arrivé opportunément au Parlement, à un moment où les relations transatlantiques et le contexte géopolitique international ont accéléré une prise de conscience des enjeux de cybersécurité, même au sein d'entreprises ou de collectivités qui n'appartiennent pas aux secteurs dits « stratégiques » et n'ont pas encore franchi le cap de la sécurisation de leurs systèmes d'information. Il était temps. Il faut bien considérer que cette transposition de la directive NIS 2 et de ses corollaires, REC et DORA, n'est pas une simple évolution réglementaire, imposée par une Union européenne qui chercherait obsessionnellement à compliquer l'existence des acteurs concernés, mais bien un tournant majeur dans la manière dont les risques numériques doivent être gérés, à tous les niveaux, et ce par les 15 000 structures qu'elle concerne, (contre seulement quelques centaines pour NIS 1).

Ce dont tout le monde doit prendre conscience avant tout, c'est que la protection de toute donnée, si anodine puisse-t-elle souvent être en apparence, constitue un défi majeur pour les citoyens, les entreprises et l'État, a fortiori avec la très rapide montée en puissance de l'intelligence artificielle et du quantique, qui permettent de traiter très rapidement une masse considérable d'informations. Il s'agit d'un risque vital pour nos sociétés et nos économies.

Être président de cette commission spéciale se situe dans la continuité d'un travail parlementaire que je mène depuis bientôt huit ans et en constitue un moment majeur. J'ai depuis longtemps la conviction qu'il va falloir faire en sorte que les acteurs économiques, les collectivités, les experts et les autorités de régulation jouent collectif. Il va falloir impliquer ainsi toute la chaîne de valeur, ce qui n'est pas une mince affaire, simplifier les modalités d'application et trouver une juste mesure entre sous et surtransposition.

Cela doit cependant servir de ligne directrice au législateur. Il est essentiel que cette transposition d'une directive européenne soit vécue, non comme une contrainte bureaucratique supplémentaire, mais comme une gestion raisonnée de risques qui concernent tout le monde.
C'est aussi prendre conscience qu'il y a là une obligation et une opportunité de faire monter en puissance des solutions françaises ou européennes souveraines, capables de nous protéger des menaces extérieures, qu'elles soient étatiques et/ou criminelles, l'occasion de muscler notre confiance en notre écosystème numérique.

J'aimerais aussi que ces discussions soient l'occasion de s'intéresser à la place de l'OSINT (*Open Source INTelligence* (le Renseignement d'Origine Sources Ouvertes, ou ROSO), une pratique encadrée par quelques textes spéciaux qui mériterait l'élaboration d'un droit commun permettant de clarifier juridiquement toutes les situations encore trop nombreuses à ne pas être concernées par les textes existants.

Contrairement à ce que d'aucuns pourraient penser, le projet de loi Résilience des infrastructures critiques et renforcement de la cybersécurité est avant tout un texte éminemment politique, non un simple ajustement technique ou administratif. C'est donc au politique qu'il faut laisser la main et le contrôle.
Un tel sujet, dont la finalité rassemble, ne devrait pas faire l'objet de querelles de clocher mais, bien au contraire, permettre de travailler dans la sérénité pour le bien commun, l'occasion pour moi de poursuivre une pratique qui m'est chère, le dialogue transpartisan. »

FOCUS

POUR UNE SÉCURITÉ JURIDIQUE DE L'OSINT : PRÉSENTATION DES TRAVAUX DU GROUPE DE TRAVAIL

Partenariat ACN - Chaire Cyber IHEDN

Le Professeur Michel Séjean, le Professeur Bertrand Warusfel et la Docteure en droit Emilie Musso ont co-dirigé, depuis 2023, un groupe de travail sur l'OSINT. Nous les avons questionnés sur le chemin qu'ont emprunté leurs travaux, et sur le résultat de ces deux années de réflexion.

« Avant tout, pouvez-vous nous expliquer ce qu'est l'OSINT ?

Il existe plusieurs définitions de l'OSINT (*Open Source Intelligence*) ou ROSO en français (Renseignement d'Origine Sources Ouvertes). Par exemple, la CNIL explique qu'il s'agit de la pratique qui « consiste à identifier des individus ou des entités, en utilisant des informations publiquement disponibles. » .

L'OSINT est pratiqué dans un grand nombre de secteurs, qu'il s'agisse du journalisme d'investigation, de la généalogie, du secteur régalien ou bien encore celui de la cybersécurité.

Notre groupe de travail propose une définition susceptible d'englober un large éventail de cas de figure. Nous ne parlons pas d'OSINT mais de « recueil d'informations en sources ouvertes », et nous avons, par exemple, précisé que cette activité englobe même le recueil d'informations obtenues à la suite d'une « connexion à un compte ».

Quelles furent les raisons de la création de ce groupe de travail ?

Nous sommes partis d'un constat de départ : les seules personnes qui peuvent faire de l'OSINT en toute sécurité ont la chance de bénéficier d'un texte qui le leur dit expressément, et qui fixe les limites de leur exercice.

Par exemple, VIGINUM dispose d'un décret qui lui permet de faire de pratiquer l'OSINT pour accomplir sa mission, mais sa liberté ne va pas jusqu'à introduire dans ses techniques d'OSINT de la reconnaissance faciale ou de l'identification vocale.

Tant mieux pour VIGINUM : ce service bénéficie d'un cadre clair ! Mais les autres ? Toutes les personnes et les entités qui ne peuvent pas s'appuyer sur un texte de droit spécialement écrit pour elles, comment font-elles de l'OSINT sans avoir l'impression de prendre un risque de condamnation ? Aucune règle générale n'énonce clairement la liberté d'user de méthodes d'OSINT.

Cette insécurité juridique est telle que nombre d'offreurs de solutions informatiques d'OSINT de l'écosystème français ont exprimé leur désarroi auprès de l'Alliance pour la Confiance Numérique (ACN).

Qui va acheter les produits français d'OSINT si le commercial n'est pas en mesure de rassurer les clients sur l'absence de risques en cas d'utilisation raisonnable du produit ? C'est ce qui se passe aujourd'hui, et les clients vont se fournir à l'étranger; tous les utilisateurs d'OSINT non visés par un texte spécial ont l'impression qu'ils sont en infraction avec le droit français, alors que ce n'est même pas le cas dans un grand nombre de situations !

De cette insatisfaction est né un partenariat entre l'ACN et la Chaire « Souveraineté numérique et cybersécurité » de l'Institut des Hautes Études de Défense Nationale (IHEDN) Ce groupe a réuni les praticiens de plusieurs secteurs comme le régalien, les entreprises, le barreau et la recherche universitaire.

« Nous ne parlons pas d'OSINT mais de *recueil d'informations en sources ouvertes* »

Émilie Musso
Docteure en droit privé et sciences criminelles
Membre associée du laboratoire de recherche en droit Lab-LEX (UR 7480)
Responsable juridique Anozr Way

Michel Séjean
Professeur agrégé de droit privé et sciences criminelles, université Sorbonne Paris Nord

Bertrand Warusfel
Professeur à l'université Paris 8
Avocat, Feltesse Warusfel Pasquier & Associés

Comment avez-vous mené vos travaux ?

Nous avons fait de la recherche appliquée en droit. C'est un procédé de création par induction.

On part de situations factuelles, par exemple des cas d'usage d'une technologie, et on rapproche toutes ces études de cas pour faire émerger une règle. Autrement dit, on part du fait pour remonter vers le droit (induction) au lieu de partir de la règle générale pour l'appliquer aux faits (déduction).

Nous avons donc procédé par induction : certes, nous n'avons pas étudié chaque cas d'usage de l'OSINT - cela aurait été trop fastidieux - mais nous avons essayé de prendre du recul et de trouver un fil conducteur, une logique commune.

Cet exercice a permis de rédiger une proposition de ce que pourrait être un régime de droit commun applicable à l'OSINT.

Quel est le résultat de vos deux années de travaux ?

Nous avons proposé de créer un cadre de droit commun pour apporter une vraie sécurité juridique à toutes les personnes qui explorent les sources ouvertes sans être visées par un texte de droit spécial sur l'OSINT.

Notre proposition suit deux axes principaux.

Le premier vise à définir l'OSINT, à affirmer clairement que sa pratique est libre dans le respect des textes relatifs à la vie privée, aux données à caractère personnel, à la propriété intellectuelle et aux secrets protégés par la loi. Ce premier texte s'achève sur l'articulation de cette liberté de principe avec des textes spéciaux pouvant restreindre cette liberté par voie législative ou réglementaire.

Le second propose la création d'une infraction accompagnée d'un fait justificatif, comme il en existe déjà en droit pénal, qui vise à sanctionner les activités d'OSINT basées sur des informations rendues disponibles à la suite de la commission d'une infraction telle que le vol par exemple, sauf lorsque cette collecte est réalisée à des fins légitimes, notamment de recherche et de sécurité informatique.

Ce faisant, nous souhaitons apporter la sécurité juridique à cette activité, nécessaire pour l'accomplissement des missions de cybersécurité (recherche de vulnérabilités, tests d'intrusion, audits d'empreinte numérique, etc.). C'est le début d'une nouvelle conversation collective sur l'OSINT.

Nous espérons que les secteurs d'activité qui dépendent des sources ouvertes vont, ensuite, solliciter les circuits démocratiques afin de faire reconnaître leurs spécificités et d'obtenir un texte de droit spécial si cela est utile et juste. »

Actions dans le cadre du Sommet de l'IA – février 2025

Du 6 au 11 février 2025 s'est tenu à Paris le Sommet pour l'action sur l'IA, à cette occasion des milliers d'acteurs représentant une centaine de pays et appartenant au secteur de l'intelligence artificielle se sont réunis à Paris, au Grand Palais, afin de participer à ce Sommet international.
L'objectif de ce Sommet été de promouvoir une stratégie française et européenne en matière d'IA en mettant en avant le savoir-faire des acteurs de l'IA en Europe.

À l'issue de ce Sommet, 100 actions et engagements concrets ont été annoncés pour promouvoir une IA de confiance et accessible à tous.

Ces actions s'orientent autour de trois axes principaux :
• Donner à chacun les moyens de s'approprier la révolution de l'IA ;

• Promouvoir notre confiance dans une IA durable, respectueuse de l'environnement comme de la cohésion sociale et de nos démocraties ;

• Renforcer le système international de gouvernance de l'IA pour le rendre plus efficace et inclusif.

Parmi ces annonces, on retient particulièrement :
• L'annonce par le gouvernement de la création de l'Institut National pour l'Évaluation et la Sécurité de l'Intelligence Artificielle (INESIA) afin d'étudier scientifiquement les effets de cette technologie, y compris en termes de sécurité. Cet institut a pour mission de fédérer les grands acteurs nationaux spécialisés dans ce domaine et déjà existants.

• L'annonce par le Président de la République d'investissements à hauteur de 109 milliards d'euros en France par des entreprises privées dans l'IA au cours des prochaines années. Une grande partie sera dirigée vers la construction de *data centers*.

• La création d'une nouvelle fondation internationale sur l'IA d'intérêt général « *Current AI* » a également vu le jour, afin de réorganiser le paysage de l'IA générative en développant et en soutenant des initiatives qui servent l'intérêt public, notamment sur le sujet de la qualité de la donnée. Elle est portée par la France et réunit neuf pays, des entreprises et des organisations philanthropiques, notamment américaines.

• Une déclaration sur la gouvernance internationale de l'IA a été rendue publique. Celle-ci a été élaborée par un groupe de travail pendant plus de 7 mois réunissant 29 États, 6 organisations internationales, 7 entreprises de la tech et 10 organisations de la société civile. Son travail vise à identifier les points de consensus afin d'établir une cartographie des secteurs et des besoins de gouvernance en matière d'IA.

• Dans le cadre d'une IA inclusive et durable pour les peuples et la planète : 58 pays, dont la France, la Chine et l'Inde, ont signé une déclaration commune visant à promouvoir une IA ouverte, transparente, éthique et digne de confiance. En complément de cette déclaration, une coalition pour une IA environnementalement respectueuse (*Coalition for environmentally sustainable artificial intelligence*) a été lancée. Elle se compose d'États, d'organisations internationales, de chefs d'entreprise, d'académiques, d'artistes et de membres de la société civile.

Organisation par l'ACN des 1ères Rencontres de l'IA de Confiance (RIAC)

Dans le cadre du Sommet de l'IA en France de février 2025, l'ACN a organisé ses premières Rencontres de l'IA de Confiance (RIAC). Elles se sont tenues le 3 février 2025 au Campus Cyber.

Cet événement avait pour objectif d'explorer la notion d'IA de confiance afin de sensibiliser l'écosystème de l'IA et de contribuer à sa structuration, apportant ainsi une contribution positive au débat public en croisant les regards d'acteurs étatiques, industriels et universitaires autour de trois tables rondes.

Dans la droite ligne du Livre Blanc sur l'IA de confiance, publié par l'ACN en mars 2024, les débats étaient centrés sur les critères permettant de caractériser la confiance dans l'IA en explorant notamment les dimensions juridiques, techniques et éthiques nécessaires à cette confiance.

Cet évènement a notamment permis de générer un large consensus autour de la nécessité de mettre cette notion de confiance au cœur du déploiement de l'IA, et d'inciter les acteurs de cette dynamique à structurer cette démarche autour des travaux communs initiés par l'ACN, particulièrement par l'établissement d'une cartographie de ces acteurs, leur recensement dans l'Observatoire de la filière de la confiance numérique, l'établissement en cours d'une charte d'éthique de la filière, etc.

Livre blanc ACN « L'intelligence artificielle de confiance »

disponible en téléchargement sur :
urlr.me/Kr6S4J

6.3 LES TENDANCES TECHNOLOGIQUES

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

6.3.a. 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 (États-Unis) et Toshiba (Japon) dans les mémoires. Cependant aujourd'hui il existe des alternatives au développement de la loi de Moore, tel que le conditionnement avancé et l'intégration hétérogène sont vues comme des alternatives à la production de puces de plus en plus performantes pour un moindre coût d'investissement.

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. À 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 solutions 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.

À 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*.

3.Identités numériques
Fortement corrélée à la thématique de souveraineté de la donnée, la re-définition des identités numériques découle également de la transformation digitale et de la généralisation des démarches à distance. Le paysage actuel en France reste caractérisé par la coexistence de multiples identités numériques, hétérogènes par leur niveau de sécurité : identités fortes (carte SIM, carte bancaire, passeport), identités substantielles (Identité Numérique La Poste), et identités faibles, souvent délivrées par des acteurs non-européens (GAFAM). Cette fragmentation soulève des enjeux de protection des données personnelles et de maîtrise technologique.

L'alternative portée par les autorités européennes repose sur le déploiement d'une identité numérique forte, certifiée, unique et souveraine, associée à l'utilisateur, et à partir de laquelle celui-ci pourrait dériver des identités secondaires selon ses usages.

La filière industrielle française dispose des compétences nécessaires à cette ambition (éléments sécurisés, IAM, intégration, cryptographie, biométrie, PVID, etc.), et les initiatives en ce sens se multiplient : en France, autour de la Carte Nationale d'Identité Électronique (CNIe) et de FranceConnect; à l'échelle européenne, dans le cadre du règlement eIDAS2 et du portefeuille d'identité numérique européen (*European Digital Identity Wallet)*.

Le portefeuille européen d'identité numérique représente une avancée majeure dans la standardisation et la sécurisation de l'identité numérique au sein de l'Union européenne.

Expérimenté dans le cadre du projet POTENTIAL, piloté par le ministère de l'Intérieur français et réunissant 20 pays, ce portefeuille numérique vise à permettre à chaque citoyen européen d'accéder à des services publics et privés via une identité certifiée et interopérable. Les cas d'usage expérimentés couvrent notamment l'accès aux services publics, aux services bancaires ou télécoms, les prescriptions électroniques, le permis de conduire ou encore la signature électronique. Des briques techniques communes pour l'émission et la vérification des attestations sont en cours de déploiement, notamment dans un environnement mutualisé ouvert à l'écosystème et hébergé par l'ANTS.

Deux nouveaux projets européens, APTITUDE et WEBUILD, viendront compléter cette dynamique à partir de septembre 2025, respectivement sur les usages liés aux personnes physiques et aux personnes morales.

Au-delà de son volet technologique, le *Digital Wallet* soulève aussi des enjeux d'adoption, de confiance et d'inclusion numérique. Sa généralisation passera par une sensibilisation du grand public, la création d'écosystèmes de services intégrés et le respect des référentiels européens (notamment pour les services de vérification d'âge, comme prévu par la loi française de mai 2024).

À titre d'exemple, plusieurs acteurs français, tels que Docaposte, participent activement à ces initiatives, notamment au travers du projet POTENTIAL, en développant des briques d'émission et de vérification d'attestations, et en contribuant à la pédagogie autour de l'identité numérique et du portefeuille européen. Parallèlement, en France, Docaposte développe des solutions concrètes de vérification d'identité et de preuve d'âge en lien avec les exigences réglementaires françaises, notamment via la plateforme 18Connect.

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.

FOCUS RECHERCHE : AGENCES DE PROGRAMMES ET CYBERSÉCURITÉ

Selon une vision communément admise, le numérique évolue progressivement vers une généralisation du calcul et des communications, sous la forme d'un continuum où le calcul est universellement réparti. Un tel scénario a pour effet de conduire à une augmentation considérable de la surface d'attaque, et donc de la vulnérabilité de l'univers numérique dans son ensemble.

Par ailleurs, les évolutions géostratégiques de ces dernières années demandent que la France et l'Europe soient en mesure prendre des décisions indépendantes, sans ingérence extérieure.
Cela vaut bien entendu pour toute décision relative à l'univers numérique. La cybersécurité est un élément essentiel de la souveraineté numérique puisqu'elle vise précisément à protéger les infrastructures et les données contre les menaces extérieures.
La recherche alimente les futures technologies souveraines dans des domaines aussi variés que la cryptographie, l'évaluation, la supervision.
Citons quelques-uns des grands enjeux à saisir dès aujourd'hui pour assurer un rôle souverain dans les années à venir :

- **la maîtrise de l'évaluation et de la certification des systèmes numériques**, tant au niveau du matériel que des logiciels, y compris leurs interactions les conséquences mutuelles des perturbations de l'un sur l'autre ;

- **la confiance dans les protocoles de cryptage,** y compris et surtout concernant les algorithmes post-quantiques, aujourd'hui adoptés au niveau international mais dont la solidité reste encore à établir avec un fort degré de certitude ;

- **la confiance dans les procédés de vote électronique ;**

- **la capacité de finement contrôler ses données personnelles et industrielles en toute circonstance**, même dans des environnements envers lesquels la confiance est limitée.

Ces sujets, qui ne sont que des exemples, demandent encore des travaux de recherche, dont les résultats seront engageants dans les années à venir, aussi bien pour l'industrie nationale que pour les citoyens.

Dans la continuité des programmes PEPR, dont en particulier le PEPR cybersécurité, qui a été présenté dans l'édition 2024 de l'Observatoire ACN, l'État a décidé d'affecter aux Organismes nationaux de recherche une mission de prospective et de pilotage des actions stratégiques de recherche sur leur périmètre de compétence. Les Agences de programme ainsi créées à cet effet doivent proposer la suite des grands programmes de type PEPR, et pour cela identifier et cartographier les compétences françaises dans chacune des disciplines de leur domaine de compétence.

Ces agences ont été annoncées par le président de la République en décembre 2023 :

« chaque agence doit être de plus en plus stratège dans son domaine et participer à la définition de thématiques de recherche prioritaires, organiser la veille scientifique pour l'ensemble des chercheurs de son domaine de compétence, interagir avec les homologues européens internationaux et veiller au développement des infrastructures de recherche. Chaque ONR transformé en agence aura ainsi un vrai mandat et disposera des ressources pour piloter les programmes qui lui seront confiés »

Parmi les 7 agences créées, deux recouvrent le domaine de la cybersécurité :

- **agence ASIC du composant aux systèmes et infrastructures numériques**, opérée par le CEA, recouvrant en particulier l'évaluation du matériel et toutes les applications aux composants, infrastructures, micrologiciels et logiciels embarqués des technologies de conception, programmation, évaluation, détection et réponses aux attaques, ainsi que la sécurité des infrastructures ;

- **agence du numérique - algorithmes, logiciels et usages**, opérée par Inria, qui inclut un programme cybersécurité qui vise à produire des résultats de recherche et de l'innovation sur tout le spectre de la cybersécurité logicielle et à faire émerger et soutenir des opérations de transfert de technologies, de compétences et de connaissances depuis la recherche académique vers les cas d'usage et l'industrie.

Les programmes cybersécurité des agences ont ainsi pour rôle de proposer une vision de l'évolution du domaine de la cybersécurité, d'assurer la supervision scientifique et la cohérence des actions engagées dans le cadre du PEPR cybersécurité, de monter et d'opérer les futures programmes adossés à la stratégie nationale.

Pour plus d'information, vous pouvez contacter :

- pour l'agence ASIC :
  Géraud Canet • geraud.canet@cea.fr
- pour l'agence du numérique :
  Ludovic Mé • ludovic.me@inria.fr

6.3.b. Les innovations propres à la filière qui génèrent de nouveaux produits

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

1. Cryptographie

La cryptographie regroupe l'ensemble des procédés visant 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 œuvre 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.
C'est dans ce contexte notamment que plusieurs projets voit le jour comme le consortium RESQUE, incluant six entités françaises (Thales, TheGreenBow, CryptoExperts, CryptoNext Security, ANSSI et l'Inria avec six institutions académiques affiliées), s'engage dans un projet de trois ans pour développer une solution de cryptographie post-quantique.
Ce projet vise à sécuriser les communications et infrastructures contre les attaques potentielles des ordinateurs quantiques.
Financé par le gouvernement français et l'UE, avec un complément de Bpifrance, il se concentre sur la création d'un VPN hybride et d'un HSM haute performance post-quantiques.
Ces projets s'étendent au delà des frontières françaises comme le démontre le partenariat entre Thales et le principal opérateur mobile coréen SK Telecom pour le développement de la cryptographie post-quantique pour les réseaux 5G.

• **Chiffrement homomorphique.** L'essor du *cloud computing* a généré un champ de recherche très actif autour du chiffrement fonctionnel et du chiffrement homomorphique. Le chiffrement fonctionnel est un nouveau paradigme de chiffrement à clé publique permettant à la fois un contrôle d'accès à granularité fine et des calculs sélectifs sur des données chiffrées. Dans sa version la plus avancée, le chiffrement entièrement homomorphe (FHE) permet de réaliser des calculs sur des données chiffrées sans jamais les déchiffrer : une partie peut chiffrer des données, une autre – sans disposer de la clé – peut effectuer des traitements dessus, et seul le détenteur de la clé peut ensuite accéder au résultat en clair.
Ce champ est très prometteur et les premières applications industrielles émergent.
Iliadata s'inscrit dans cette dynamique : en combinant des technologies de calcul multipartite sécurisé (MPC) et de chiffrement homomorphe, elle propose des solutions de mutualisation de données confidentielles, permettant à plusieurs acteurs d'exploiter collectivement des données sans en compromettre la confidentialité.
Cette innovation a été récompensée par le Prix de la Recherche du Forum InCyber 2025, soulignant la pertinence croissante de ces technologies dans les environnements fortement régulés ou sensibles.

• **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.

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

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 ST Microelectronics.
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 États-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 États-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 États-Unis en la matière, qui menace les positions françaises à l'avenir y compris sur le secteur de la sécurité.

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 des transactions dans un registre répliqué et partagé entre les acteurs. Les informations sont, de fait, infalsifiables et non modifiables. La *blockchain* est donc 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 : certification des données, registres d'opérations financières ou contractuelles, suivi de chaînes logistiques complexes, stockage infalsifiable de données, automatisation de tâches sensibles mais aussi missions de sécurité civile ou intérieure et gestion du secret entre institutions. Associée à des portefeuilles (*wallets*) elle offre également des fonctions de vérifications des droits.

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. Dans le domaine privé, le même changement est nécessaire vers une plus grande capacité à collaborer et s'auto-réguler par filière industrielle ou économique.

Les acteurs français maîtrisent plusieurs des technologies clés du domaine de la *blockchain* (cryptographie, méthodes formelles, *wallets*,etc.). 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.

La Commission européenne finance plusieurs projets d'innovation dans les domaines de l'identité décentralisée, de l'énergie, de la traçabilité... en lien avec son intérêt pour les architectures fédérées (par exemple, GaiaX). Enfin, les écosystèmes allemand et anglais sont au moins comparables à l'écosystème français, et de nombreux petits pays en Europe de l'Est en particulier ou en Afrique voient en la blockchain comme une solution pour mettre en œuvre des services publics ou privés nativement digitaux.

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, par exemple, 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.

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

6.3.c. Transformation digitale & miniaturisation : Vers des offres globales de *Security as a Service*

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

En effet, au niveau mondial, la 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 digitale, conduisant à une croissance toujours plus importante de la part qu'occupent les logiciels dans les outils de sécurité. En particulier, les producteurs de produits physiques et électroniques – où les marges sont en moyenne plus basses qu'en cybersécurité – tentent progressivement de monter en gamme dans la chaine de valeur en développant des compétences dans le logiciel.
Ces derniers - à l'image de 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.

À titre illustratif, la grande entreprise espagnole Prosegur, l'un des *leaders* européens du gardiennage, a crée un fond d'investissement doté de 30 M€ pour investir dans la sécurité électronique et cyber. Depuis 2016, ce fond a racheté les entreprises Dognaedis, Innevis et Cipher, toutes spécialisées dans la cybersécurité et regroupées au sein de Prosegur sous la marque Cipher.

Securitas, autre *leader* européen de la sécurité privée, a racheté l'activité sécurité électronique de l'américain Stanley Security en Janvier 2022 et se développe sur ce segment.

Enfin, cette tendance se ressent également du côté des acheteurs de la filière. 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.

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

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

3. ...*open source*...

Certains acteurs proposent des approches clef-en-main avec systèmes propriétaires. Ces approches sont de moins en moins plébiscitées par les clients qui se retrouvent dépendants d'un unique acteur privé pour l'entretien et l'amélioration future des interfaces.

En conséquence, le développement de solutions *open source* se développe de plus en plus.

Dans le domaine particulier des systèmes nationaux de gestion d'identité (état civil) opérés par les états, 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 états 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 interoperable 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*).

4.... 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.

À PROPOS DE L'ACN

ACN
Alliance pour la confiance numérique

L'Alliance pour la Confiance Numérique (ACN) représente les entreprises (*leaders* mondiaux, PME/TPE, et ETI) du secteur de la confiance numérique et notamment celles de 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 2 499 entreprises réalisant en France 21,3 Milliards d'euros de chiffre d'affaires dans ce secteur en forte croissance (7,4% de croissance annuelle moyenne depuis 2016).

Les 130 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 Électriques, Électroniques et de Communication), est membre associé du Campus cyber et participe activement aux travaux des CSF (Comité Stratégique de Filière) des Industries de Sécurité et Solutions Numériques de Confiance.

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

Partenaires de l'ACN

Membres de l'ACN

Membres associés de l'ACN

À PROPOS DE DECISION ÉTUDES & CONSEIL

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 :

• Électronique (composants, équipements, systèmes)

• Aéronautique, défense, sécurité

• Électrique, énergies 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'Économie (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'Économie (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'Économie (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'Économie (DGE) et le SGDSN.

Pour plus d'informations
www.decision.eu

DECISION
ETUDES & CONSEIL

NOTES

Réalisation - Mise en page
Agence Verveine

ACN

English version available at :
www.confiance-numerique.fr

Partenariat
presse