2026

confiance-numerique.fr

Observatoire de la Filière de la Confiance Numérique

ACN
Alliance pour la confiance numérique

Inspirer Rassembler Renforcer Agir

ACN

Alliance pour la confiance numérique

Observatoire de la Filière de la Confiance Numérique 2026

Réalisation - Mise en page
Agence Verveine

achevé d'imprimer en mai 2026

SOMMAIRE

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

Grégory Wintrebert
Président de l'ACN

La publication de la 12e édition de l'Observatoire ACN intervient dans un contexte mondial et économique particulièrement tendu, où les crises géopolitiques, les disruptions commerciales et les menaces cybernétiques redessinent les contours de notre souveraineté. Ces turbulences, amplifiées par des pressions inflationnistes et des vulnérabilités structurelles, mettent à l'épreuve nos chaînes de valeur numériques et tendent à ralentir le rythme de croissance de la filière de la confiance numérique, qui demeure néanmoins très dynamique avec 5,4% de croissance en 2025.

Pour autant, cet environnement exigeant nous pousse à repenser nos modèles et à accélérer notre transition vers une autonomie renforcée. L'Observatoire ACN, avec ses analyses pointues et ses perspectives prospectives, offre un éclairage précieux pour guider nos décisions collectives dans cette période critique.

Réaffirmer la confiance numérique face aux défis actuels

Au cœur de cette dynamique se trouve la filière française de la confiance numérique, indispensable pour bâtir des sociétés résilientes et des économies performantes tout en renforçant notre souveraineté numérique. Notre filière, qui va de l'identité numérique, à la cybersécurité, en passant par l'IA de confiance, la *blockchain* et les infrastructures numériques de confiance, est en première ligne pour répondre à ces enjeux.

Elle représente en 2025 près de 35 milliards d'euros de chiffre d'affaires dans le monde dont 22,4 milliards d'euros en France et emploie plus de 170 000 salariés dans le monde dont 62 000 en France. Dans les années à venir, le déploiement effectif du portefeuille d'identité numérique européen pour les citoyens et les entreprises marquera une avancée décisive, tandis que les progrès générés par les réglementations françaises et européennes (Résilience, NIS2, Cyber Resilience Act, ...) contribueront à consolider notre cybersécurité et à renforcer notre filière. Par ailleurs, l'émergence d'un cadre juridique pour l'IA de confiance ouvrira de nouvelles voies à une innovation éthique, maîtrisée et inclusive, reposant sur des infrastructures numériques de confiance.

« ACN se positionne au centre de l'écosystème numérique national, en renforçant les liens avec les institutions publiques et les territoires »

Nos trois axes stratégiques : une feuille de route ambitieuse

Pour répondre à ces défis, l'ACN s'appuie sur trois axes stratégiques clairs. Tout d'abord, il s'agit de structurer la filière en optimisant les initiatives et en favorisant les collaborations. Cela signifie produire des analyses robustes, consolider nos données, clarifier les enjeux des marchés clés, accompagner les entreprises dans leurs démarches de conformité, et valoriser les savoir-faire français et européens. Cette mission s'incarne dans nos travaux, nos Observatoires successifs, et l'effort constant visant à donner à la filière un cadre lisible, cohérent et ambitieux.

Ensuite, il nous paraît essentiel de fédérer les acteurs autour d'une voix unie, tout en préservant leurs spécificités. La confiance numérique ne se construit jamais seule. Elle repose sur un dialogue permanent entre fournisseurs, utilisateurs, institutions, chercheurs et pouvoirs publics. Notre rôle est de créer ces passerelles, de renforcer la circulation des bonnes pratiques, d'animer des groupes de travail ouverts et exigeants, et de porter une voix collective capable d'influencer les feuilles de route nationales et européennes. Comme en témoignent nos initiatives récentes, cette dynamique de coopération s'affirme d'année en année.

Enfin, l'ACN se positionne au centre de l'écosystème numérique national, en renforçant les liens déjà étroits avec les institutions publiques et les territoires. Dans un contexte de consolidation réglementaire, de montée en puissance des exigences en matière de confiance numérique et de compétition technologique mondiale, nous sommes un point d'ancrage. Un acteur présent, écouté et force de proposition. Notre capacité à dialoguer avec les décideurs, à anticiper les mutations et à orienter les stratégies, publiques et privées, est au cœur de notre mission.

Ces piliers guident nos actions quotidiennes et amplifient notre impact collectif. Nous avons, par ailleurs, consacré un effort majeur à la formalisation de notre raison d'être, de nos missions et de nos valeurs fondamentales. Celles-ci se cristallisent autour de quatre verbes d'action : inspirer par des visions innovantes, rassembler les énergies vives de la filière, renforcer nos capacités collectives et agir de manière décisive pour des résultats tangibles. Cette charte claire oriente désormais toutes les initiatives de l'ACN.

Une transformation profonde pour servir la filière et le pays

Afin d'accompagner au mieux les mutations en cours, l'ACN change de dimension. Nous engageons une évolution profonde de nos services pour proposer à nos membres et à l'ensemble de la filière une valeur ajoutée accrue : outils d'analyse renforcés, accompagnement personnalisé, production de connaissances stratégiques, espaces d'échange dédiés, initiatives communes, ...

Surtout, en tant que syndicat professionnel représentant la filière, nous œuvrons à réinventer la relation entre entreprises et pouvoirs publics, en posant la confiance au centre de la relation et en proposant des modèles de partenariat innovants au service de la souveraineté numérique et de la résilience nationale. Cette ambition nous positionne comme un acteur pivot dans la construction d'un avenir technologique maîtrisé et nous serons force de propositions pour porter avec détermination les priorités des entreprises de notre filière auprès des candidats à la prochaine élection présidentielle.

Nous changeons d'ère. La confiance numérique se réinvente, s'élargit, se complexifie. L'ACN se transforme à son tour pour accompagner la filière dans cette mutation. Ensemble, nous allons renforcer notre capacité d'action, affirmer notre rôle dans l'écosystème et bâtir les fondations d'une filière toujours plus solide, plus unie et plus stratégique pour notre pays et l'Europe.

« La confiance numérique se réinvente, s'élargit, se complexifie »

LE MOT DE LA MINISTRE

Anne Le Hénanff

Ministre déléguée chargée
de l'Intelligence artificielle
et du Numérique

Dans un contexte géopolitique bousculé, le numérique apparait de manière encore plus criante comme une des conditions sine qua non de notre souveraineté, clé de la maitrise de notre destin.

J'ai fait de la souveraineté numérique le fil rouge de mon action. Celle-ci ne peut être ni un slogan ni une posture. Elle est une boussole, qui guide nos choix et conditionne notre capacité à décider par nous-mêmes. Être souverain, c'est d'abord regarder en face nos dépendances technologiques. Cette lucidité est indispensable : on ne transforme que ce que l'on comprend.

Sur la base de cette cartographie, nous devons faire émerger des solutions alternatives, avec une offre souveraine, française et européenne. Cela suppose de créer les conditions pour que ces solutions existent, notamment à l'échelle européenne.
Il s'agit aussi d'assumer une forme de préférence européenne, pour renforcer notre autonomie collective. Cela passe aussi au niveau national par la commande publique et la commande privée.

La souveraineté numérique ne se limite pas à une question industrielle ou technologique. Elle est indissociable de la défense de nos valeurs. Protéger les citoyens, en particulier les plus vulnérables, garantir une concurrence loyale et faire respecter nos règles face aux grandes plateformes sont des exigences fondamentales. Je refuse d'opposer innovation et régulation : il faut tenir une ligne d'équilibre, exigeante et responsable.
Au fond, la souveraineté numérique est une condition de notre puissance, de notre indépendance et de la vitalité de notre démocratie. Elle ne se décrète pas, elle se construit dans la durée.

La souveraineté numérique et l'innovation vont de pair. C'est en particulier vrai dans le domaine de l'intelligence artificielle. Le développement de l'intelligence artificielle est un défi majeur pour notre société : l'IA représente une opportunité majeure pour nos entreprises, nos laboratoires, nos collectivités, qui pourront tous gagner en productivité en automatisant certaines tâches, en libérant du temps aux salariés qui pourront se concentrer sur les tâches à forte valeur ajoutée.
Celles qui ne l'adoptent pas, au contraire, risquent d'être vite dépassées par leurs concurrentes.
C'est pourquoi nous agissons pour que toutes nos entreprises adoptent l'IA, avec un plan national : « Osez l'IA ».

« l'IA représente une opportunité majeure pour nos entreprises, nos laboratoires, nos collectivités »

Mais ce développement peut aussi inquiéter : les risques liés à l'intelligence sont nombreux. Le développement de l'IA peut avoir des conséquences néfastes sur le travail, sur l'environnement, sur la santé mentale.
C'est pourquoi nous agissons pour que nous ayons, en France et en Europe, des IA qui nous ressemblent, en accord avec nos valeurs, et qui ne mettent pas nos populations et notre planète en danger.

Si le progrès technologique est certes porteur d'opportunités, il doit aller de pair avec l'édiction d'une politique de sécurité numérique ambitieuse pour en contrer les risques et les dérives potentielles.

La cybersécurité est un défi que nous devons collectivement relever. Comme l'a très justement souligné la Revue nationale stratégique 2025, « le cyberespace est devenu un espace de compétition, de contestation et parfois même d'affrontement désinhibé, en miroir des tensions géopolitiques et des rivalités internationales ». Ce constat nous rappelle que la cybersécurité est devenue une condition sine qua non de notre liberté, de notre souveraineté et de notre autonomie stratégique.

Dans ce contexte, l'Etat a élaboré une feuille de route ambitieuse pour la Nation à travers la Stratégie nationale de cybersécurité 2026-2030, articulée autour de 5 axes pour consolider la cyber-résilience de la Nation et inscrire l'action de la France dans un cadre européen et international pour garantir la stabilité du cyberespace.
La prochaine étape en la matière sera l'adoption du projet de loi Résilience à l'Assemblée nationale, qui fixera pour la première fois des exigences de cybersécurité ambitieuses pour 15 000 entités essentielles et importantes en application de la directive européenne NIS 2.
Mais la parole de l'Etat ne saurait être crédible si celui-ci ne se fixe pas lui-même des ambitions fortes pour sa propre cybersécurité. C'est dans cet esprit que le Premier ministre a rendu publique, pour la première fois, la feuille de route interministérielle 2026-2027 sur les efforts prioritaires en matière de sécurité numérique de l'Etat.

La souveraineté numérique, c'est aussi s'assurer que nos concitoyens évoluent dans un espace numérique respectueux de notre droit et de notre cadre réglementaire. C'est une nécessité pour les plus vulnérables, notamment les mineurs, mais aussi pour la protection de nos modèles démocratiques.

Face aux risques désormais clairement établis que les réseaux sociaux font peser sur la santé mentale et physique des mineurs, ainsi que sur leur sécurité, je porte, aux niveaux national et européen, la mise en place d'une majorité numérique fixée à 15 ans, interdisant l'accès aux réseaux sociaux en dessous de cet âge.

En parallèle, j'ai chargé le Conseil de l'intelligence artificielle et du numérique d'organiser et de structurer des travaux scientifiques sur les risques émergents liés, d'une part, aux assistants conversationnels fondés sur l'intelligence artificielle générative et, d'autre part, aux jeux vidéo.

En prévision des échéances électorales de 2027, la France s'est dotée d'une Stratégie nationale de lutte contre les manipulations de l'information (2026-2030) dont l'un des objectifs est de renforcer la régulation des plateformes en ligne et des services d'intelligence artificielle générative au niveau européen, que je porterai au niveau européen dans les prochains mois sous l'impulsion du Président de la République.

Vous pouvez compter sur mon plein engagement pour faire du numérique un des leviers de l'excellence de notre pays.

« la cybersécurité est devenue une condition sine qua non de notre liberté, de notre souveraineté et de notre autonomie stratégique »

ÉLÉMENTS CLEFS

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 2026, couvrant le champ de la cybersécurité, de la sécurité numérique et de l'IA. Les principaux enseignements de l'édition 2026 portent sur l'évolution du chiffre d'affaires de la filière, le renforcement de sa projection à l'international, et l'identification des marchés qui demeurent les plus porteurs.

Chiffres clés 2025

22,4 Mds€
Confiance numérique

+4,2%
Croissance (hors IA)

+5,4%
Croissance (avec IA)

+2,4%
Sécurité numérique

+5%
Cybersécurité

+23,4%
IA de confiance

Levées de fonds M&A

#1 La confiance numérique reste une filière en croissance, mais le ralentissement engagé depuis 2023 se confirme en 2025

Après le point haut de 2022, la croissance du chiffre d'affaires ralentit progressivement, passant de 6,8 % en 2023 à 6,4 % en 2024, puis à 4,2 % en 2025. En intégrant l'intelligence artificielle, seul segment affichant une croissance à deux chiffres, la progression atteint toutefois 5,4 % en 2025.

Cette décélération s'inscrit dans un contexte global de ralentissement du marché, marqué par des tensions géopolitiques, une contrainte accrue sur les finances publiques et une pression croissante sur les budgets des organisations. Elle est également liée à des dynamiques opérationnelles, avec un allongement des cycles de décision, des tensions sur le marché du conseil et une intensification de la concurrence, se traduisant notamment par des guerres de prix sur certains segments.

Elle s'explique également par l'évolution contrastée des segments :

- **la sécurité numérique**, plus mature, reste sur une croissance modérée (+2,4 % en 2024 puis +2,4 % en 2025) ;
- **la cybersécurité** conserve un rôle moteur mais avec une dynamique moins homogène, les produits cyber restant bien orientés (+6,4 % en 2025) tandis que les services cyber ralentissent nettement (+3,4 % en 2025 après +10,6 % en 2024) ;
- **l'IA de confiance** apparaît comme le segment le plus dynamique, avec une croissance de 9,3 % en 2024 puis de 23,4 % en 2025.

Dans ce contexte, le développement du marché reste tiré par des enjeux structurants autour de l'intelligence artificielle, de la résilience et de la souveraineté. Parallèlement, l'écosystème poursuit sa consolidation, bien que les levées de fonds reculent (456 M€ pour 41 opérations en 2023, contre 352 M€ pour 27 opérations en 2024), traduisant un environnement d'investissement plus sélectif.

Ces évolutions témoignent d'une croissance qui demeure soutenue, mais désormais plus sélective, portée en priorité par les segments les plus différenciants.

Les principaux marchés de la filière :

18%
Secteur public

&

17%
Finances
Banque & Assurance

#2 Marchés porteurs : les relais de croissance se concentrent sur les segments où la sécurité est la moins arbitrable

Dans un contexte de ralentissement global, les marchés les plus porteurs restent ceux où les enjeux de sécurité, de souveraineté et de résilience sont les moins arbitrables.
Les principaux relais de croissance se situent ainsi dans la défense, l'espace, la sécurité, les grands ministères et organismes affiliés, ainsi que dans la banque et l'assurance.
Ces marchés continuent de soutenir la demande, car ils sont directement exposés à des exigences fortes de continuité d'activité, de conformité, de protection des données et de maîtrise des infrastructures critiques.
Cette polarisation de la demande bénéficie surtout aux acteurs les mieux positionnés sur des besoins critiques ou différenciants. Elle explique que, malgré le ralentissement agrégé de la filière, certaines PME et ETI continuent d'enregistrer des croissances à deux chiffres, en particulier lorsqu'elles sont présentes sur des offres à forte valeur ajoutée, adossées à des besoins souverains, réglementaires ou sectoriels difficiles à différer.
La croissance se concentre sur les segments les plus critiques, où la sécurité, la conformité et la souveraineté deviennent des critères d'achat dominants, limitant les arbitrages budgétaires et accentuant la polarisation au détriment des offres les plus standardisées et facilement substituables.

+3,25 Mds€
Chiffre d'affaires à l'international depuis 2022

6,9 Mds€
Chiffre d'affaires à l'export

31%
Du chiffre d'affaires Confiance

+5,4%/an
Chiffre d'affaires réalisé hors de France depuis 2022

#3 La filière française de la confiance numérique consolide sa projection à l'international

En 2025, la part du chiffre d'affaires réalisée à l'export atteint 31 %, soit 6,9 Md€, ce qui traduit une légère progression de l'ouverture internationale de la filière.
Plus largement, le chiffre d'affaires réalisé hors de France progresse en moyenne de 5,4 % par an entre 2022 et 2025, signe d'un ancrage croissant des acteurs français sur les marchés européens et mondiaux.
Le développement à l'échelle européenne est par ailleurs favorisé par l'adoption de cadres réglementaires structurants ces dernières années, notamment en matière d'intelligence artificielle, de solutions de confiance, de cybersécurité et de protection des données, contribuant à harmoniser les marchés et à créer des opportunités de déploiement pour les acteurs français.
Cette internationalisation repose à la fois sur :
• les exportations
• les stratégies de croissance externe
Les acquisitions menées par des entreprises françaises à l'étranger, en particulier en Europe, montrent que la filière ne se contente plus d'exporter depuis la France, mais cherche de plus en plus à bâtir une présence locale sur des marchés cibles.
Cette dynamique est particulièrement visible au Royaume-Uni et plus largement en Europe, où plusieurs groupes français ont procédé à des rachats ciblés afin d'élargir leur couverture géographique, leur base de clientèle et leurs expertises.
Si l'international s'impose de plus en plus comme un levier de développement, sa progression reste encore insuffisante face à l'intensité concurrentielle mondiale, ce qui en fait un impératif stratégique pour atteindre une taille critique.

Dans un contexte de croissance ralentie, la filière de la Confiance Numérique entre dans une phase de sélection et de polarisation :
• la croissance devient plus exigeante et se concentre sur les acteurs les plus différenciés ;
• la création de valeur se déplace vers des segments moins arbitrables, liés à la sécurité, à la conformité et à la souveraineté ;
• l'internationalisation s'impose comme un levier clé de compétitivité.

Dans ce cadre, l'impact de l'intelligence artificielle constitue un facteur structurant pour les années à venir. Son développement, notamment à travers les approches agentiques, est susceptible de transformer en profondeur certains segments, en particulier le conseil et les services.

Par ailleurs, l'essor de l'IA semble déjà rebattre les cartes en matière d'investissement. Il pourrait contribuer à une recomposition des priorités des acteurs et à un ralentissement temporaire des dynamiques de fusions-acquisitions, un phénomène qui restera à observer attentivement dans les prochains mois.

La filière atteint 34,7 Md€ de chiffre d'affaires en 2025, avec une croissance de +5,4 %, en ralentissement par rapport aux années précédentes mais toujours supérieure à celle de l'économie française. Elle génère 10,6 Md€ de valeur ajoutée et représente 113 600 emplois en France (auxquels s'ajoutent 61 300 à l'étranger), confirmant son positionnement sur des activités à forte intensité technologique et son rôle de contributeur significatif à l'emploi qualifié sur le territoire.

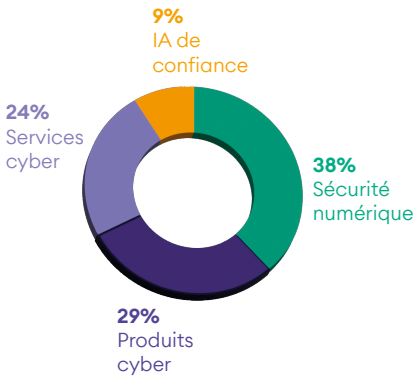
Fondamentaux 2025

CA Monde	**34.7 MDS €**
CA Hors de France	**12.3 MDS €**
CA France	**22.4 MDS €**
	dont export **6.8 MDS €**
Valeur ajoutée France	**10.6 MDS €**

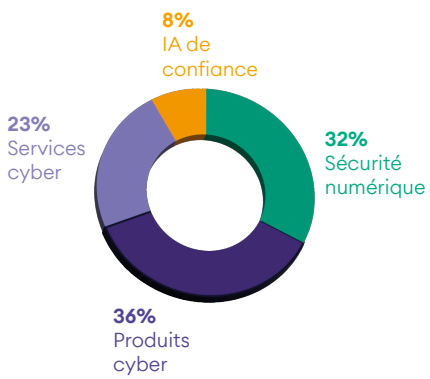
La structuration des segments révèle des logiques différenciées : la sécurité numérique domine en volume (38% du chiffre d'affaires), traduisant un marché étendu, tandis que les produits cyber représentent un nombre plus élevé d'entreprises (36 %), reflétant un écosystème plus fragmenté. Les services cyber occupent une place intermédiaire, notamment en matière d'effectifs (27 %), tandis que l'IA de confiance, encore limitée en poids (8 %), s'inscrit dans une dynamique de structuration progressive.

Les principaux segments de la confiance numérique en 2025

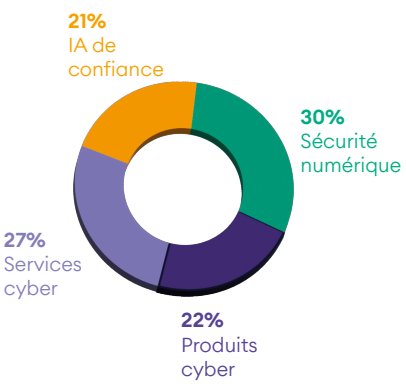
• Chiffre d'affaires



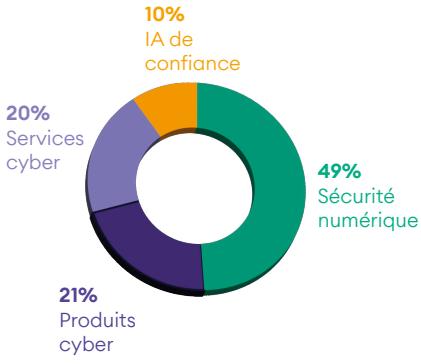
• Nombre d'entreprises



• Effectifs

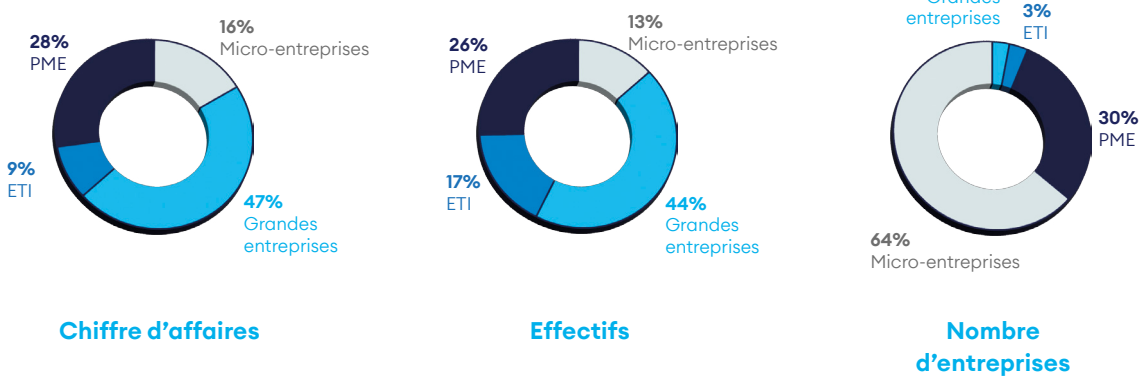


• Valeur ajoutée



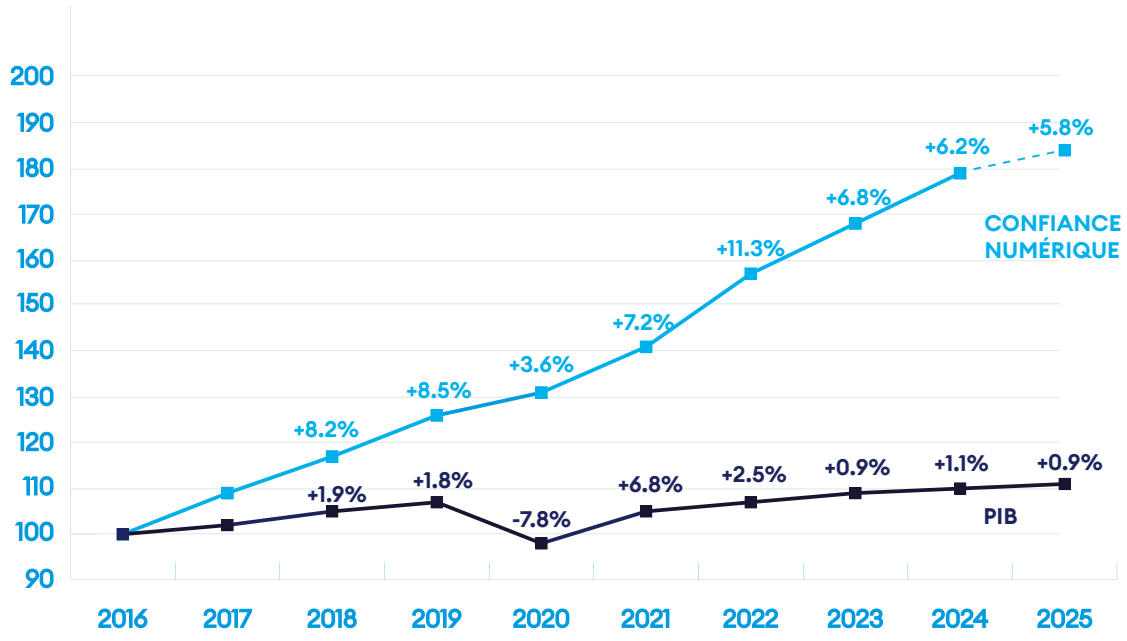
La filière se caractérise par une concentration du chiffre d'affaires au profit des grandes entreprises (47 %), tout en laissant une place significative aux PME (28 %) dans la création de valeur. Les effectifs sont répartis de façon quasi équivalente entre grandes entreprises (44 %) et acteurs intermédiaires (PME et ETI, 43 %). Enfin, les microentreprises représentent à elles seules 64 % des acteurs, tandis que les grandes entreprises et ETI restent peu nombreuses, traduisant une fragmentation du tissu économique

Répartition par taille d'entreprises 2025



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

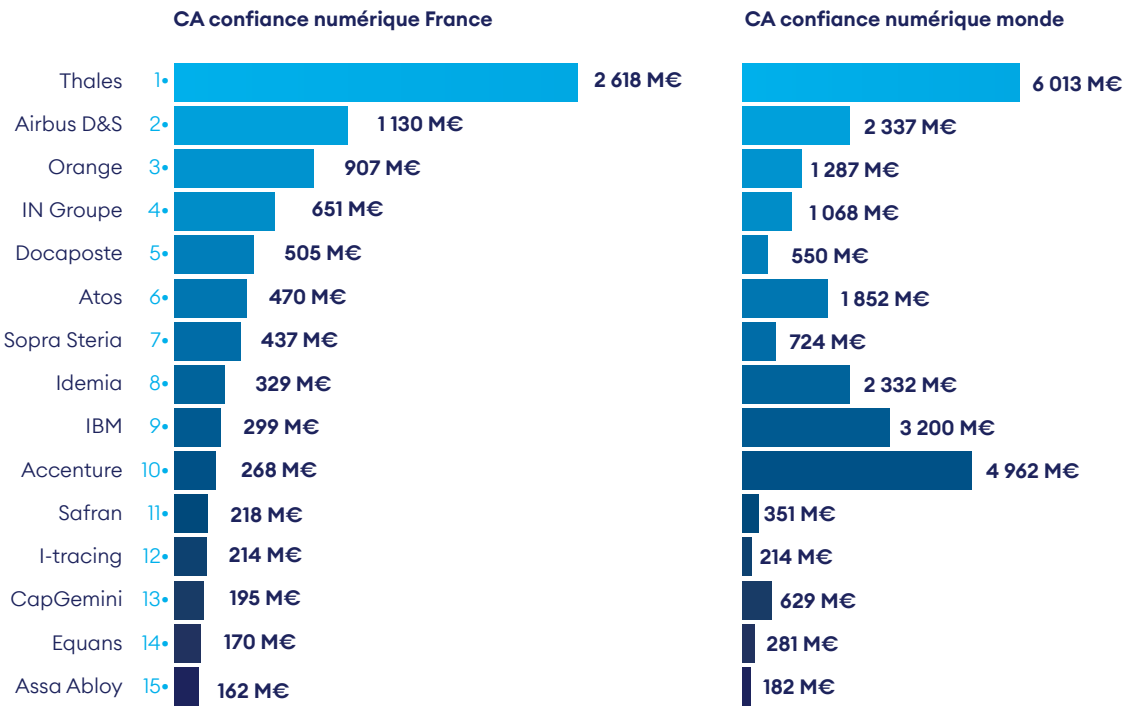
Croissance France comparée 2017- 2025



Base 100 en 2016

Croissance du PIB mesurée par l'INSEE, et par le FMI en 2025
Cette croissance ne prend pas en compte la croissance dans l'IA de confiance

Top 15 acteurs France 2025



*** Note :** l'édition 2026 de l'Observatoire introduit un élargissement du périmètre d'analyse avec l'ajout du segment IA de confiance en 2025. 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 2026 et 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 OneWelcome, S21sec, Excellium, Tesserent et Imperva.
• **Atos** comprend Idnomic, Ipsotek, Motiv ICT Security, Sec consult, In fidem, Paladion…
• **Orange Cyberdéfense** comprend SCRT, Telsys et ensec.
• **Sopra Steria** comprend CS Group, Tobania et Ordina.
• **Docaposte** comprend les activités de signature électronique d'IDEMIA, BoomkR et Thiqa…
• **IN Groupe** comprend l'activité eID de Nexi et IDEMIA Smart Identity
• **Chapvision / Flandrin technologies** comprend Deveryware, Bertin IT, Vcsys, Elektrob et Geotrend

Top 1-10 acteurs France

THALES · AIRBUS DEFENCE & SPACE · Atos · DOCAPOSTE · IBM · IDEMIA · IN GROUPE · orange · sopra steria · accenture

Top 11-20 acteurs France

CA confiance numérique France compris entre 135 M€ et 220 M€

EQUANS · Capgemini · CHAPSVISION DATA MAKE SENSE · i-TRACING CYBERSECURITY · SAFRAN · WORLDLINE

ASSA ABLOY · exaprobe | econocom · FORTINET

Top 21-50 acteurs France

CA confiance numérique France compris entre 60 M€ et 130 M€

SPIE · WAVESTONE · SFR · CROSSCALL · squad · NAVAL GROUP · odrive · CHEOPS TECHNOLOGY · The Cloud Customized For You ! · ANTEMETA · Stordata · Sogetrel · Ledger · Almond · nxo · cogelec · tessi · ALTEN

Deloitte. · EY · Linxens · SIEMENS APIXIT · CGI · Palantir · pwc · cisco · NOKIA · TREND MICRO

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

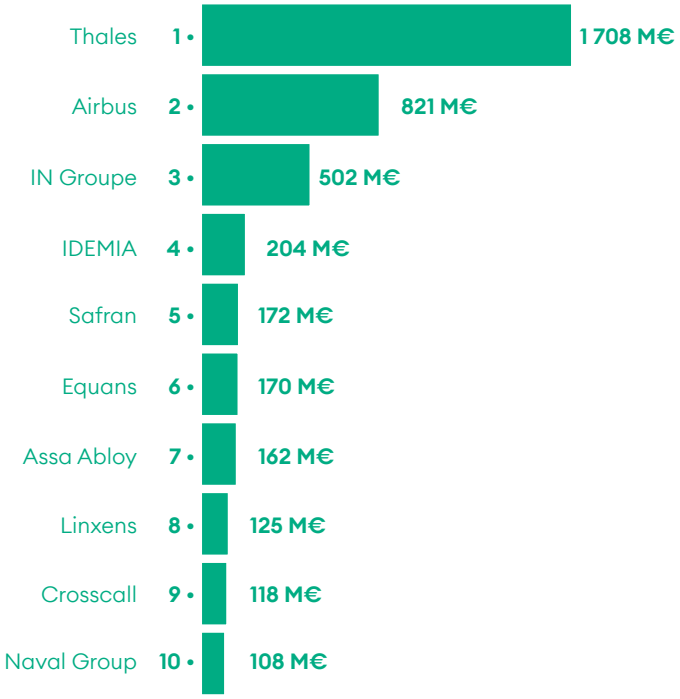
Parmi les acteurs situés entre la 10ème et la 20ème position et réalisant un CA confiance numérique supérieur à 135M€ depuis la France en 2024, on trouve des acteurs français tels que Cap Gemini, Nomios et I-Tracing (services cyber), Worldline (sécurité des paiements), Safran (dont IA spécifique), et 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 2024-2025
+2.4%

• Chiffre d'affaires
8 559 M€

• Emplois
34 462

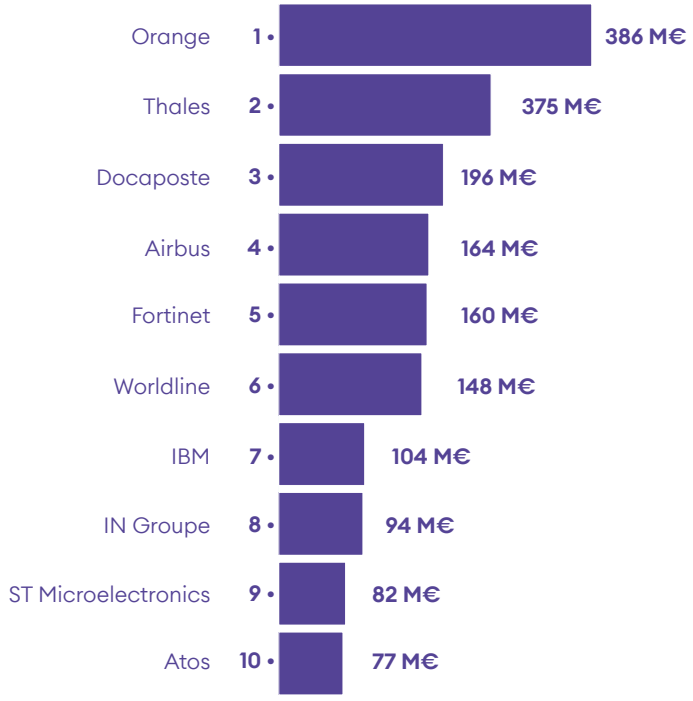
• Nombre d'entreprises
1 772

• Valeur ajoutée
3 438 M€

	Chiffre d'affaires M€	Emplois	Nombre d'entreprises	Valeur ajoutée M€
Systèmes et contrôle d'accès électronique	1 866	6 928	333	695
Identification et authentification des personnes	2 458	9 562	509	966
Observation et détection large zone	572	2 246	191	305
Traçage et localisation	670	2 685	224	252
Communications sécurisées	1 729	6 806	315	652
Commande, contrôle et aide à la décision	793	3 346	275	367
Renseignement et collecte d'informations	471	2 888	234	201

FOCUS

Segment Produits et solutions de cybersécurité



• Croissance 2024-2025
+6.4%

• Chiffre d'affaires
6 502 M€

• Emplois
25 433

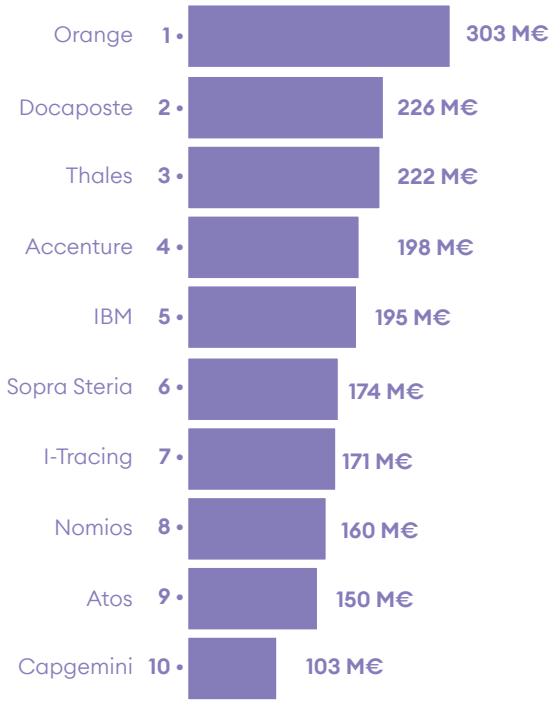
• Nombre d'entreprises
749

• Valeur ajoutée
3 817 M€

	Chiffre d'affaires M€	Emplois	Nombre d'entreprises	Valeur ajoutée M€
Gouvernance cyber	1 169	5 843	233	670
Gestion des identités et des accès	948	3 071	214	604
Sécurité des données	1 974	7 178	356	1 190
Sécurité des applications	440	1 599	177	304
Sécurité des infrastructures numériques	1 581	6 281	360	897
Sécurité des produits et équipements	390	1 480	161	152

FOCUS

Segment Services de cybersécurité



• Croissance 2024-2025
+3.4%

• Chiffre d'affaires
5 407 M€

• Emplois
30 335

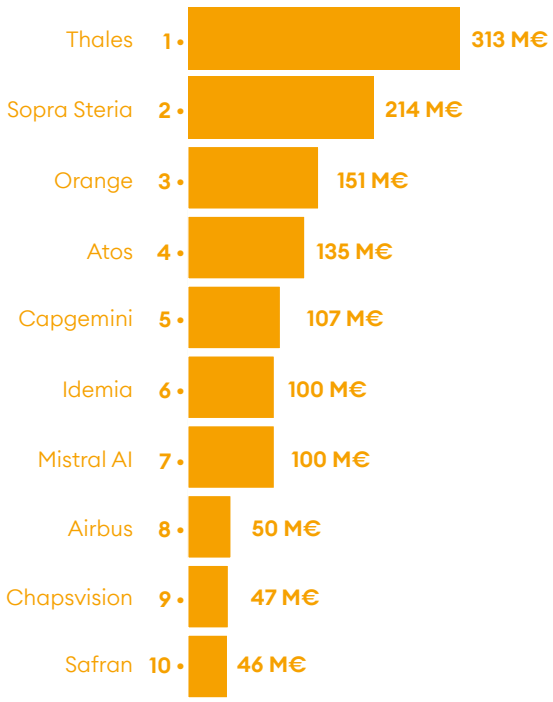
• Nombre d'entreprises
730

• Valeur ajoutée
2 499 M€

	Chiffre d'affaires M€	Emplois	Nombre d'entreprises	Valeur ajoutée M€
Audit, planning et conseil cyber	2 366	13 711	684	971
Mise en oeuvre cyber	1 742	10 348	477	755
Sécurisation de l'infogérance et exploitation	1 179	5 202	367	701
Formation en cybersécurité	120	107	207	72

FOCUS

Segment IA de confiance



• Croissance 2024-2025
+23.4%

• Chiffre d'affaires
1 957 M€

• Emplois
23 339

• Nombre d'entreprises
379

• Valeur ajoutée
900 M€

	Chiffre d'affaires M€	Emplois	Nombre d'entreprises	Valeur ajoutée M€
IA à usage général	437	3080	144	201
IA spécifique	1521	14 126	310	699

1. CONFIANCE NUMÉRIQUE

1.1 CYBERSÉCURITÉ, SÉCURITÉ NUMÉRIQUE ET IA DE CONFIANCE : UN TRIPTYQUE TECHNOLOGIQUE COMPLÉMENTAIRE

La confiance numérique est la garante du progrès numérique. Au fil des années, 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 :

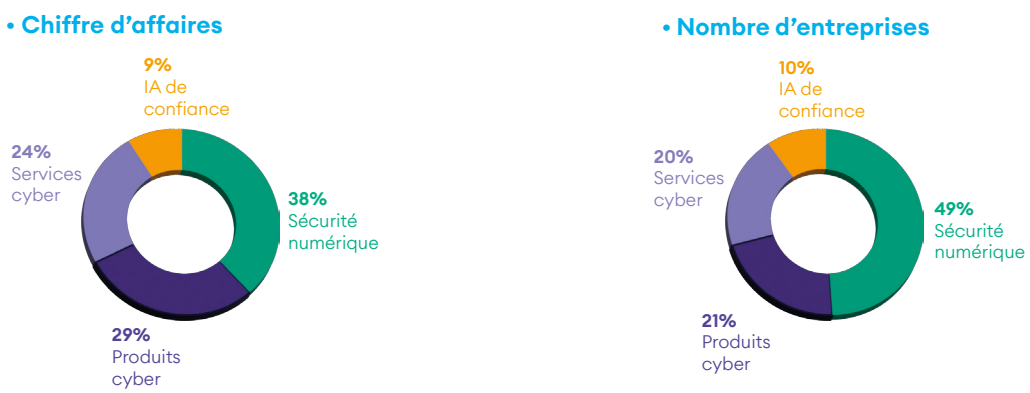
• **La Cybersécurité** proprement dite, qui correspond à la sécurisation «interne» des systèmes numériques. La cybersécurité regroupe deux types d'activités souvent associées dans la pratique, les services (conseil, conception, mise en place, exploitation, formation), et les logiciels et solutions, destinés 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 oeuvre 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 2025

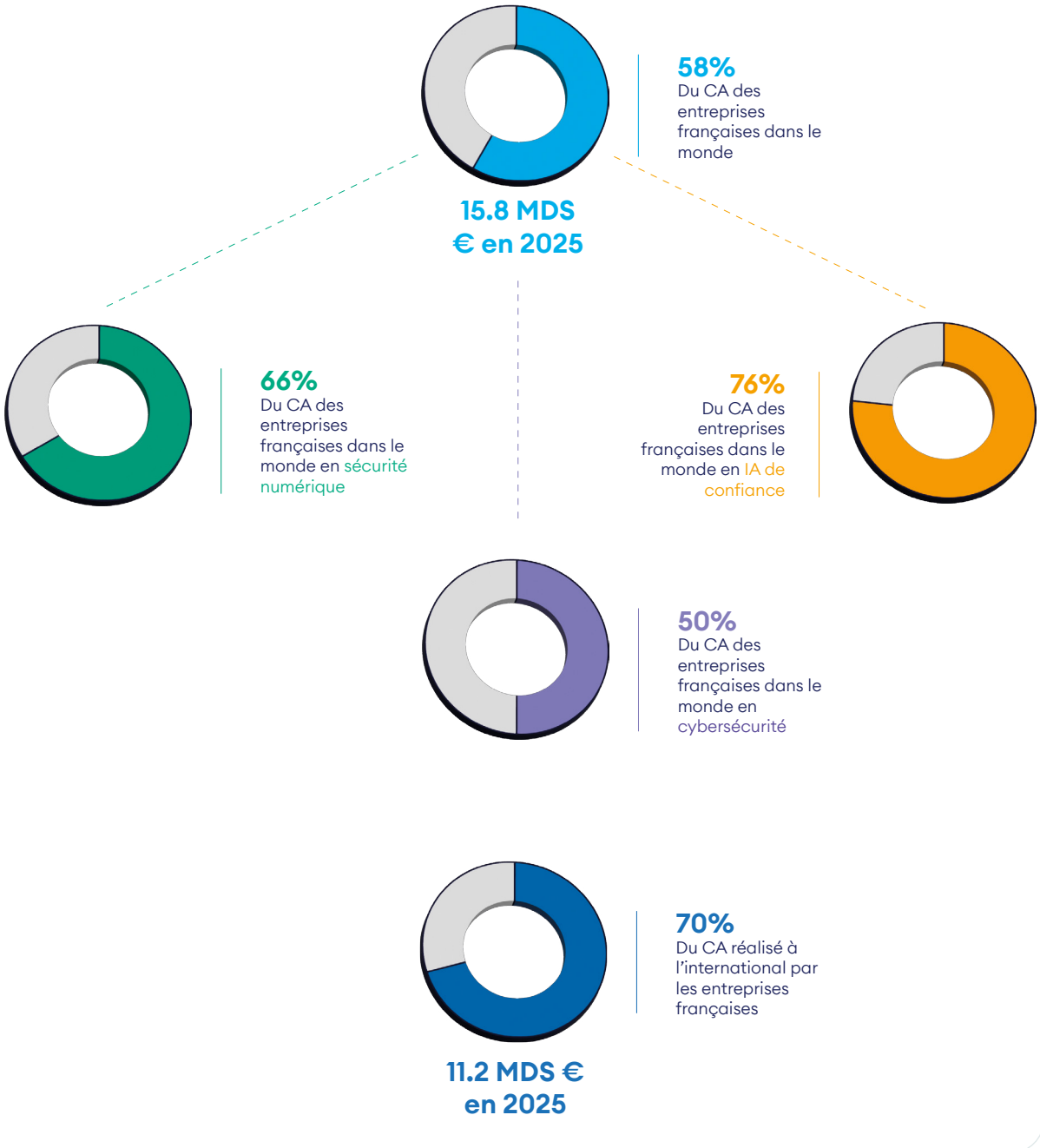


L'ACN est au coeur de la filière

Parmi les adhérents de l'ACN, on trouve :

• **10 grandes entreprises ou ETI, parmi lesquelles les 9 *leaders* français de la confiance numérique.**
• Mais aussi **76 PME, TPE et *startups* innovantes adhérents directs** et **plus de 200 PME du secteur** via les écosystèmes de ses membres partenaires partenaires (SPAC, GICAT, Bretagne Next, etc).

Les membres de l'ACN représentent



1.2 LA RAISON D'ÊTRE, LES MISSIONS ET LES VALEURS DE L'ACN

« Pour maîtriser notre avenir numérique, l'Alliance pour la Confiance Numérique inspire, rassemble, renforce, agit au service des entreprises et de la société. »

L'Alliance pour la Confiance Numérique est un syndicat professionnel qui représente les entreprises françaises de la confiance numérique et se structure autour de l'identité numérique, la cybersécurité, l'intelligence artificielle de confiance, la blockchain et les infrastructures de confiance. Les missions de l'ACN s'articulent autour de cinq axes stratégiques.

- **Inspirer et éclairer les décisions publiques** : l'ACN s'attache à porter une vision stratégique de la confiance numérique au service de la souveraineté et de l'intérêt général. À ce titre, elle représente la filière auprès des pouvoirs publics en France et en Europe, tout en contribuant aux débats législatifs et réglementaires nationaux et européens.

- **Être force de proposition pour la filière** : l'ACN nourrit les débats publics par l'analyse, l'innovation et l'anticipation. Elle produit des travaux de référence, tels que des feuilles de route, des livres blancs ou des positions communes, et formule des propositions concrètes sur les lois, règlements et politiques publiques.

- **Agir pour le développement et l'impact de la filière** : l'ACN conduit des actions collectives au service des membres et de la filière, le soutien à l'émergence de solutions françaises de confiance numérique, ainsi que l'accompagnement des démarches opérationnelles à impact réel.

- **Renforcer la souveraineté et la compétitivité de la filière** : l'ACN œuvre pour accroître la compétitivité et l'influence de la filière française, tout en promouvant un numérique de confiance, durable et responsable.

- **Rassembler et la structurer l'écosystème** : l'ACN fédère les acteurs autour d'une vision et d'objectifs communs, en structurant la dynamique sectorielle et en coordonnant les initiatives, tout en favorisant la coopération entre entreprises, institutions, académies et partenaires européens.

Les valeurs de l'ACN reposent sur cinq piliers fondamentaux :

- **Le collectif** est au cœur de l'ADN de l'ACN. L'ACN croit à la force de l'intelligence collective, à la diversité des points de vue et à la mise en commun des expertises. Cette valeur se traduit par la fédération des acteurs de la filière, la construction de positions partagées et la recherche de l'intérêt commun au-delà des intérêts individuels.

- **La responsabilité** constitue une autre valeur clé de l'ACN. Cette responsabilité implique une approche éthique, durable et souveraine des technologies : maîtrise des dépendances, respect des cadres réglementaires, protection des données, et prise en compte des conséquences à long terme des choix technologiques. Être responsable, c'est anticiper, orienter et assumer les décisions prises au service de l'intérêt général.

- **La confiance** est un prérequis à toute coopération durable. L'ACN s'engage à créer un cadre de dialogue transparent, loyal et exigeant entre ses membres, ses partenaires et les institutions. Cette confiance repose sur la crédibilité des positions défendues, la rigueur des travaux menés et la constance des engagements, afin de bâtir des relations solides et pérennes.

- **La coopération** va au-delà de la simple mise en réseau, l'ACN favorise les dynamiques de travail concrètes entre acteurs publics et privés, grandes entreprises, PME, start-up, monde académique et institutionnel. Cette valeur se traduit par la volonté de co-construire des solutions, de mutualiser les efforts et de dépasser les logiques de silos pour renforcer collectivement la filière numérique.

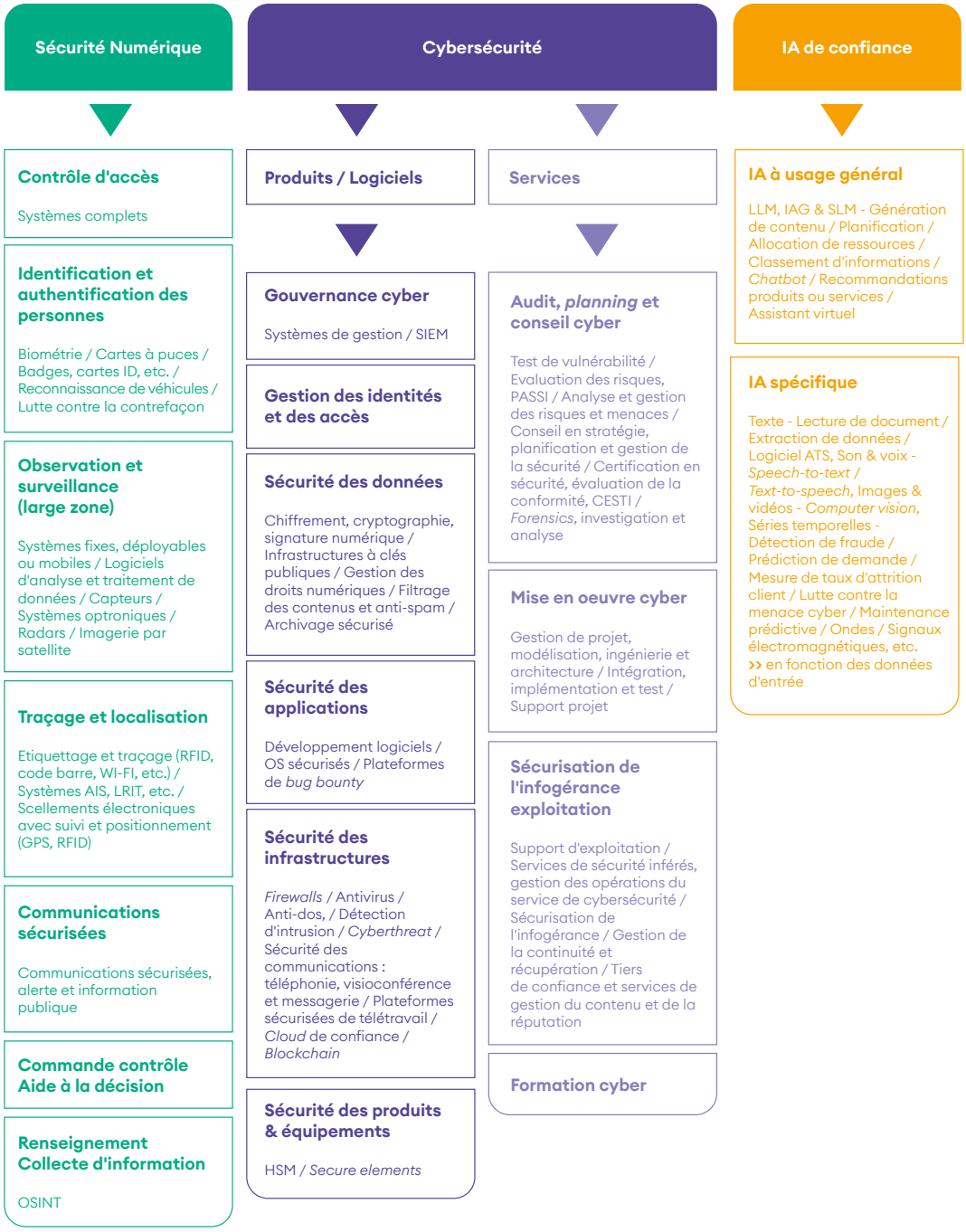
- **L'action** est au cœur de l'identité et de la crédibilité de l'ACN. Elle traduit la volonté de passer de la vision à la mise en œuvre, et de transformer les travaux collectifs en résultats concrets et utiles pour la filière. Cette valeur s'incarne dans des actions opérationnelles, le développement des marchés, la structuration des offres, le soutien aux acteurs et la contribution à la souveraineté numérique. Pour l'ACN, agir signifie s'engager de manière responsable, avec exigence, pragmatisme et sens du long terme, afin que chaque action renforce durablement la confiance, la compétitivité et l'autonomie stratégique de l'écosystème numérique français.

1.3 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**, correspondant 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



1.4 MÉTHODOLOGIE

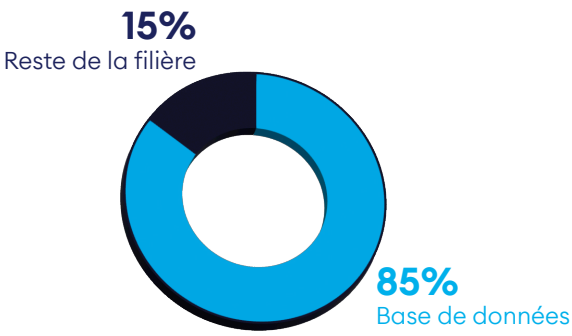
L'objectif de l'Observatoire de la filière de la confiance numérique est à la fois de définir le périmètre de la filière et d'en évaluer le poids économique et les caractéristiques.

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 1010 entreprises parmi les 2 573 que compte la filière de la confiance numérique.
Cette base de données prend en compte :

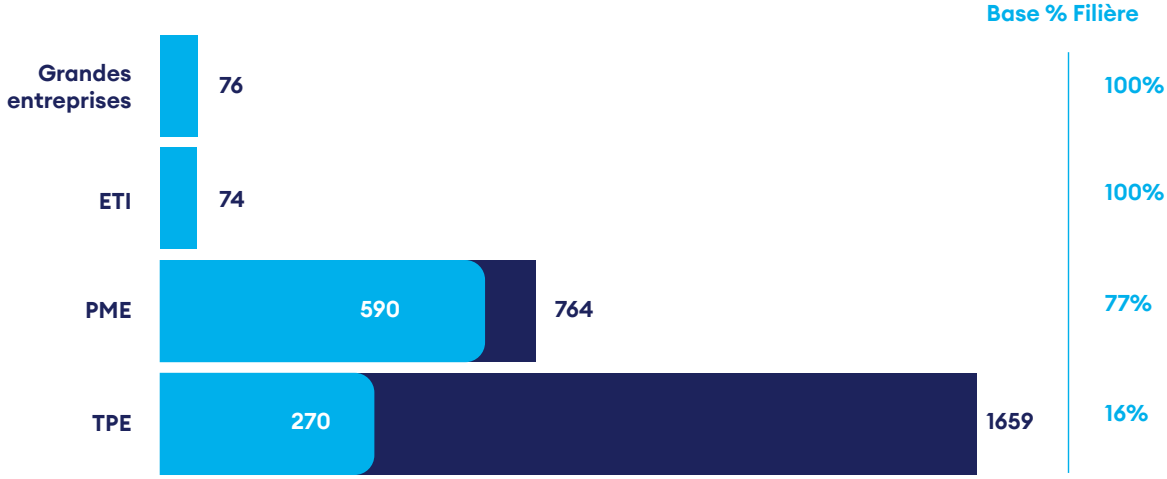
- La totalité des grandes entreprises de la filière (76/76) ;
- La totalité des entreprises de tailles intermédiaires (ETI) de la filière (72/72) ;
- La majorité des petites et moyennes entreprises (PME) de la filière (590/764) ;
- Les très petites entreprises (TPE) et *startups* les plus remarquables et innovantes (270/1659).

Ainsi, bien que seul 39% des entreprises de la filière soient prises en compte dans la base de données, celle-ci est représentative de 85% du chiffre d'affaires total de la filière de confiance numérique France.

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 2015-2025 :** 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 2026, les membres ayant répondu au questionnaire représentent 12% 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 2025 et en fonction de la nouvelle segmentation des acteurs. Les chiffres 2024 actualisés sont présentés dans les sections suivantes.

2. UNE FILIÈRE IMPORTANTE ET DYNAMIQUE

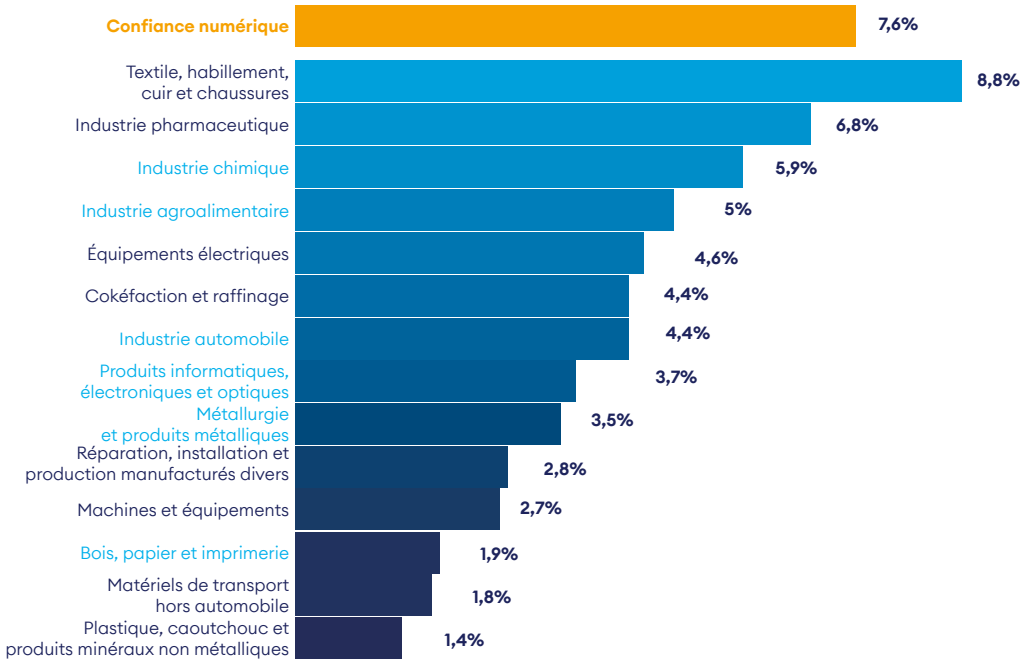
2.1 L'UNE DES INDUSTRIES FRANÇAISES QUI BÉNÉFICIENT DE LA CROISSANCE LA PLUS FORTE SUR LA PÉRIODE 2016-2024

Sur la période 2016-2024, la confiance numérique est la filière industrielle française qui bénéficie du plus fort taux de croissance, avec 7,4% par 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 textile et de l'habillement, l'industrie pharmaceutique, l'industrie chimique, et l'industrie agroalimentaire. 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 12ème filière industrielle française sur 15 en valeur ajoutée en dépassant à la fois la filière de l'équipement électrique.

Croissance annuelle moyenne des filières françaises sur la période 2016-2024



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 2024

2.2 LA FILIÈRE INDUSTRIELLE 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 48% (valeur ajoutée / chiffre d'affaires) en 2023. 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 la plus élevée, devant les produits informatiques, électroniques et optiques à 39%. 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.

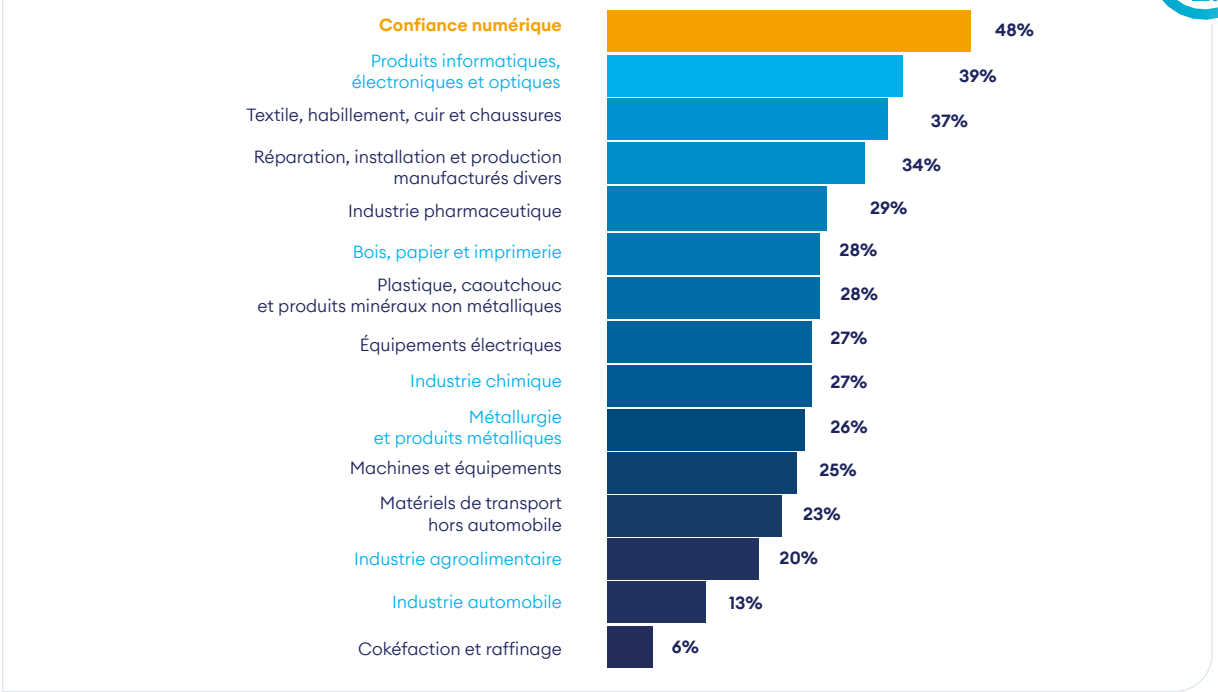
Ce phénomène s'explique principalement par trois facteurs :

1. **Le pourcentage de l'activité dédiée aux services est relativement élevé dans la filière française de confiance numérique** (24% en 2025), 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, alors même qu'en ce qui concerne l'industrie électronique française dans son ensemble, une grande partie des étapes de production en amont de la chaine de valeur est réalisée en Asie, **ce phénomène ne s'applique que peu au segment de la confiance numérique qui maintient autant que faire se peut toutes les étapes de la production en France en raison de sa proximité avec les secteurs régaliens.** D'autres filières françaises se concentrent plus fortement sur des activités d'intégration en amont de la chaîne de valeur et sur des activités d'ingénierie pure (*design*, développement, etc.). 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).

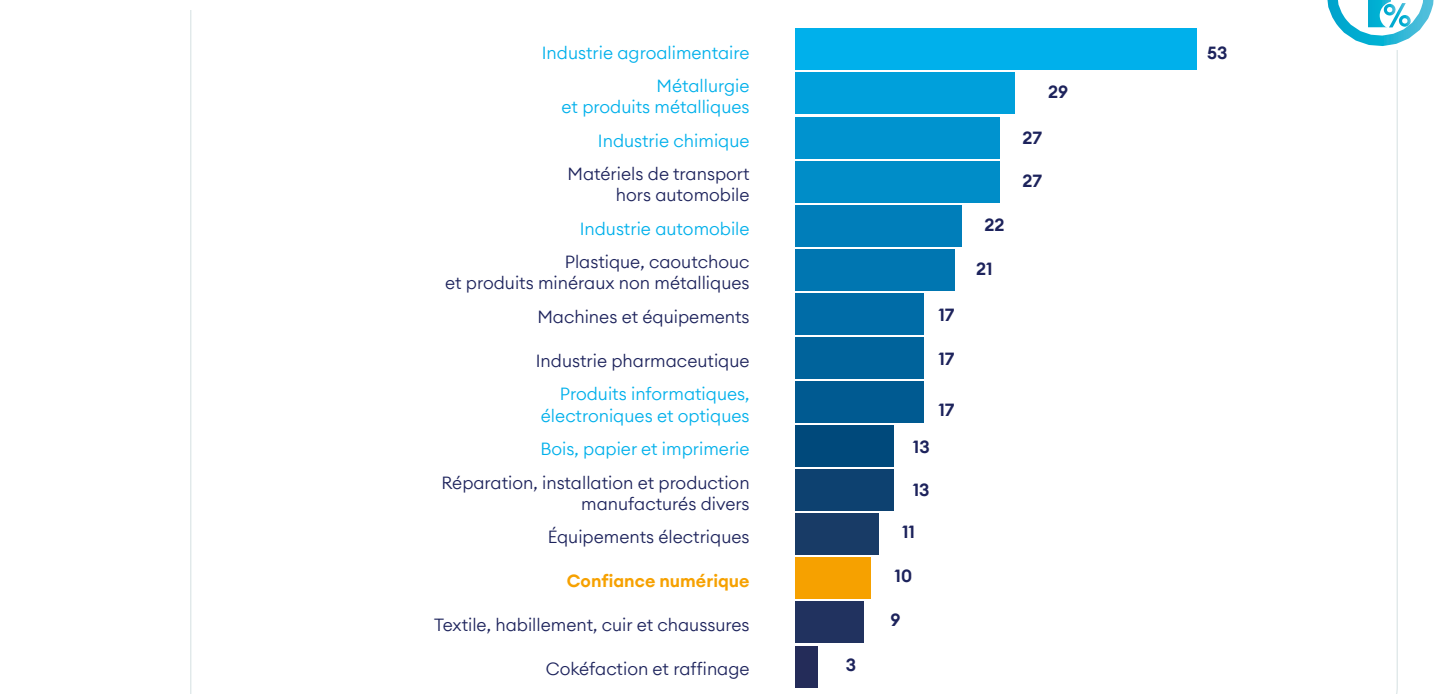
Taux de valeur ajoutée (VA/CA) des filières françaises en 2023



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 se trouve entre la filière du textile et de l'habillement, et celle des équipements électriques. En termes d'emploi, elle dépasse largement la filière de cokéfaction et se rapproche de l'industrie pharmaceutique.

Valeurs ajoutées des filières françaises en 2023 (MDS €)



Emplois des filières françaises en 2023 (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 73% du chiffre d'affaires de la confiance numérique en France, soit 16,3 milliards d'euros en 2025. Autrement dit, les acteurs étrangers de la filière réalisent 27% du chiffre d'affaires de la filière en France, soit environ 6 milliards d'euros en 2025. 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'est pas 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 2025 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 (1.1 % par an de croissance du PIB français sur la période 2018-2025), 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 :

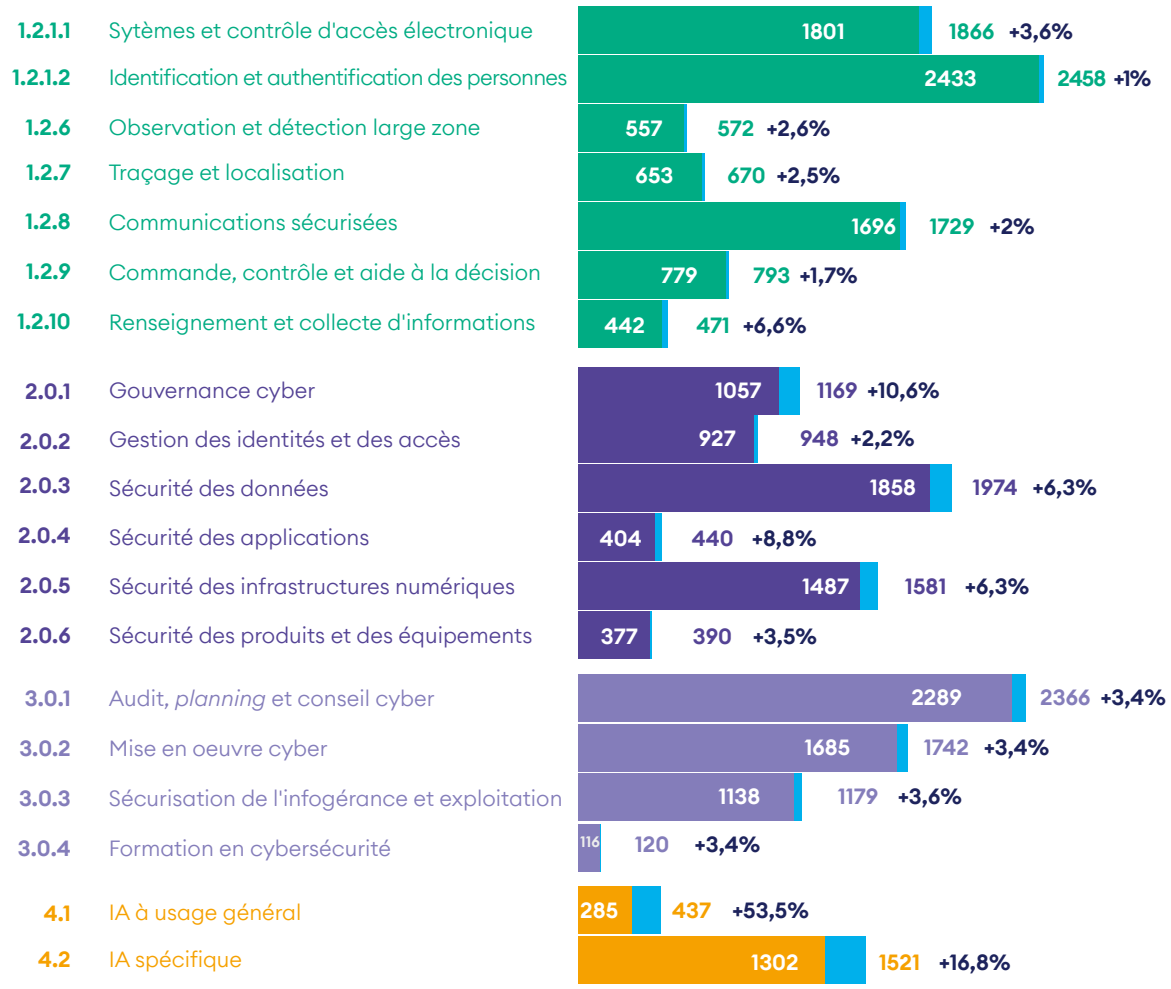
- Le **potentiel de croissance** est durablement supérieur à celui de toutes les autres industries françaises ;
- La confiance numérique est déjà de **taille significative ;**
- Les acteurs français sont à la pointe en matière de **compétences et de R&D ;**
- Ce secteur est essentiel à la **souveraineté 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 • 22,425 Mds € en 2025

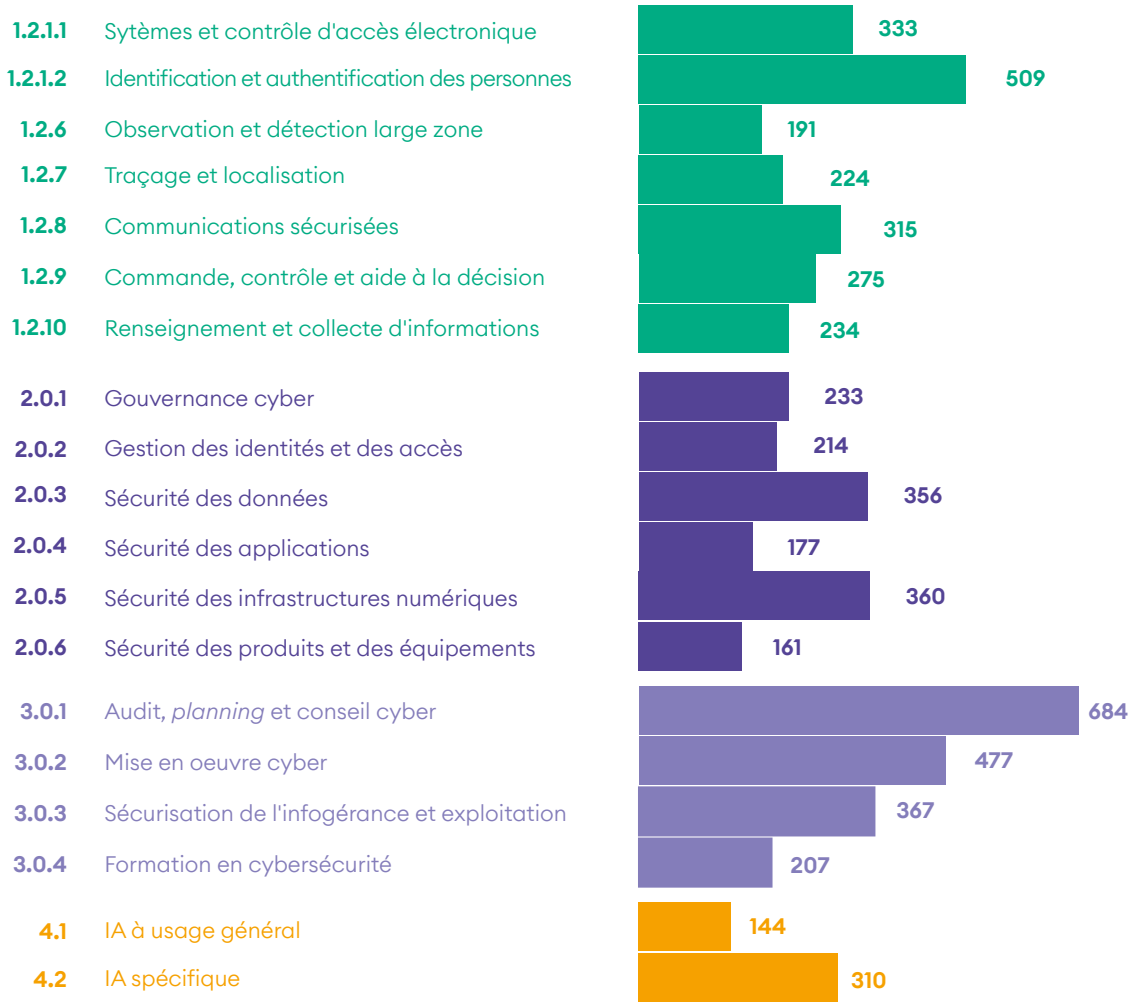


Sécurité numérique	Produits de cybersécurité	Services de cybersécurité	IA de confiance
8 559 M€ de CA	**6 512 M€** de CA	**5 459 M€** de CA	**1 957 M€** de CA
+2,4% en 2025	+6,4% en 2025	+3,4% en 2025	+23,4% en 2025

22 425 M€ de CA
de confiance numérique en France
+5,4% en 2025

Source : DECISION Etudes & Conseil

3.2 NOMBRE D'ENTREPRISES

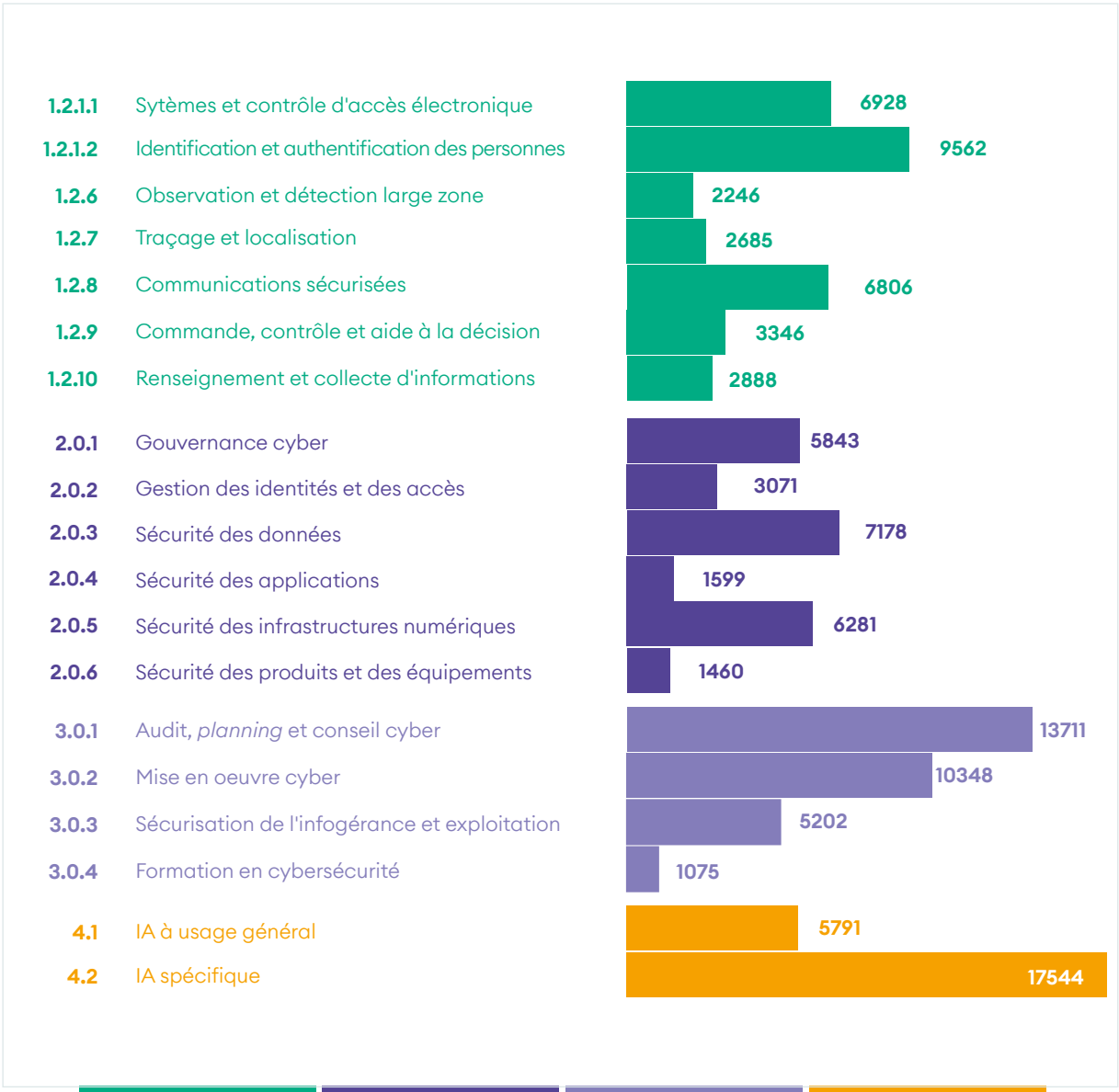


Sécurité numérique	Produits de cybersécurité	Services de cybersécurité	IA de confiance
1 772 entreprises	**749** entreprises	**730** entreprises	**379** entreprises

2 572 entreprises
de confiance numérique en France

Source : DECISION Etudes & Conseil

3.3 EMPLOIS

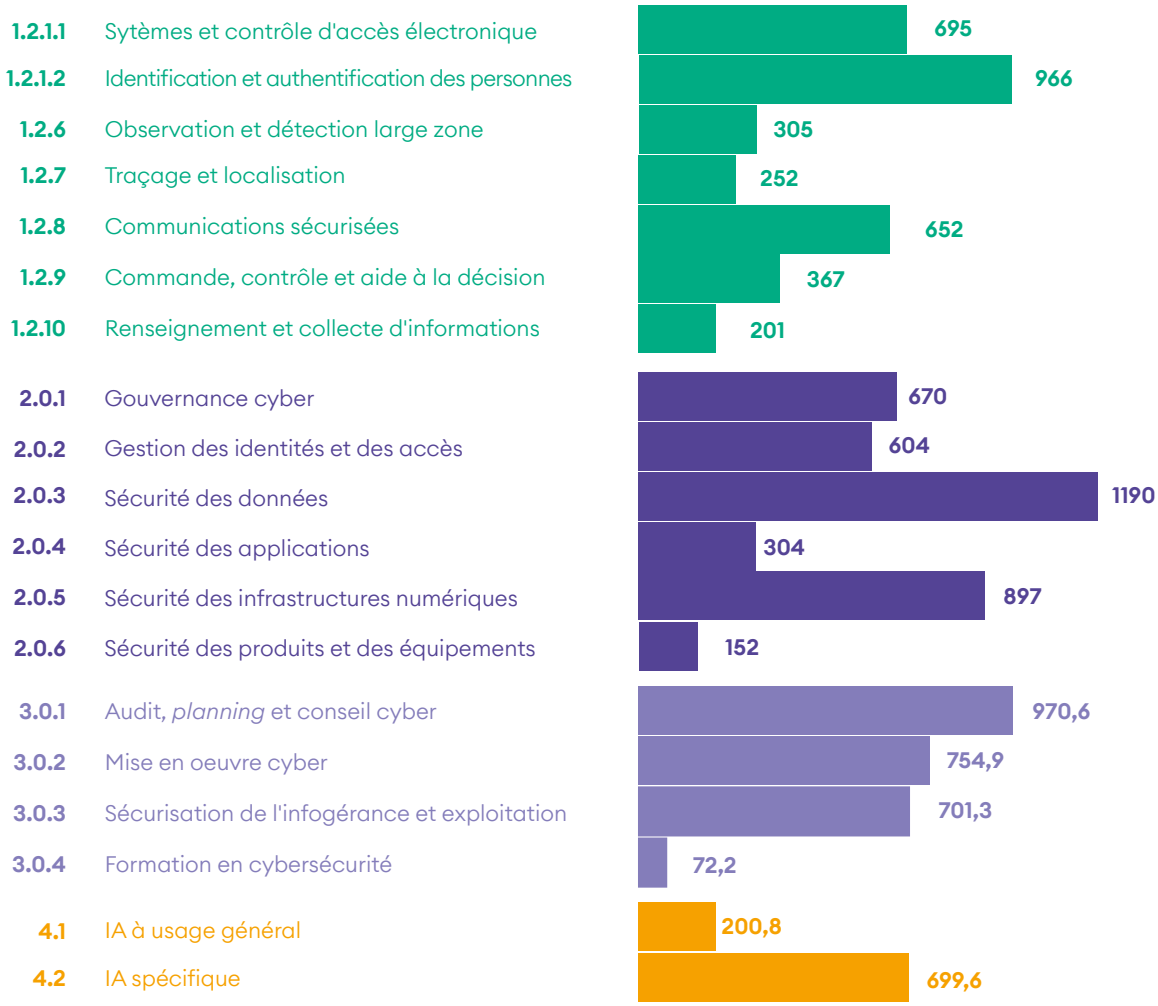


Sécurité numérique	Produits de cybersécurité	Services de cybersécurité	IA de confiance
34 462 emplois	**25 433** emplois	**30 335** emplois	**23 339** emplois

113 600 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
3 438 M€	**3 817 M€**	**2 499 M€**	**900 M€**
de valeur ajoutée	de valeur ajoutée	de valeur ajoutée	de valeur ajoutée

10 654 M€ de valeur ajoutée
de confiance numérique en France

Source : DECISION Etudes & Conseil

3.5 LES MOUVEMENTS DE FUSION - ACQUISITION

Entre janvier 2024 et mars 2026, 33 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 15 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 33 opérations :

- 16 concernent des rachats d'entreprises françaises par d'autres entreprises françaises (49 %) ;
- 9 correspondent à des acquisitions d'entreprises étrangères par des entreprises françaises (27 %);
- 8 impliquent le rachat d'entreprises françaises par des entreprises étrangères (24 %).

La grande majorité des sociétés rachetées sont des PME (73 %), 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.

Les années 2024 et 2025 se distinguent par un volume de transactions plus faible (14 à 15 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.

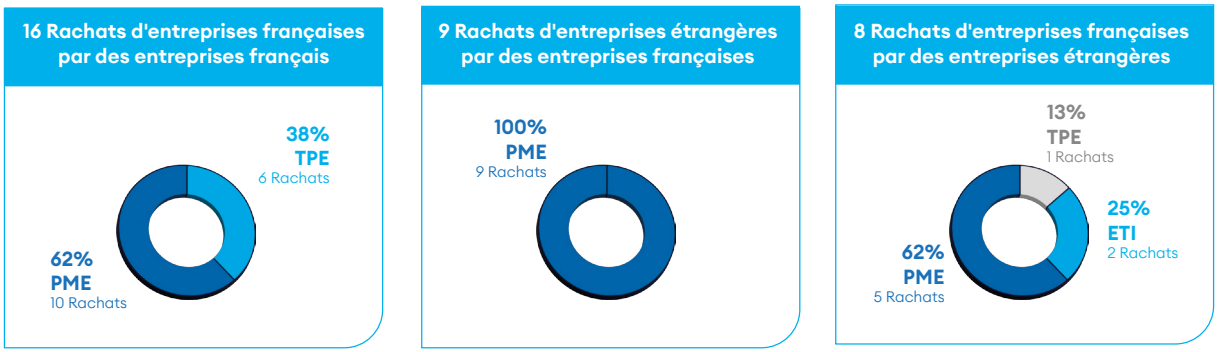
Sur la période récente, les flux de fusions-acquisitions entre la France et l'étranger tendent à davantage s'équilibrer.

Alors que la période 2017-2020 avait été marquée par une nette domination des rachats d'entreprises françaises par des capitaux étrangers, cette asymétrie apparaît aujourd'hui moins prononcée, sous l'effet d'une intensification des acquisitions menées par des acteurs français en Europe et à l'international.

Les États-Unis conservent néanmoins une place centrale dans les opérations impliquant des entreprises françaises de la cybersécurité.

Cela s'illustre notamment par le rachat d'Expert Lines par Neverhack, société française passée sous contrôle majoritaire du fonds américain Carlyle fin 2023, ainsi que par les acquisitions de PingCastle par Netwrix et de Secure-IC par Cadence.
S'y ajoutent les opérations menées par Hornetsecurity sur Vade Security puis Altospam.

Les 33 mouvements de rachats sont résumés dans le diagramme en page suivante.



Bilan : rachats d'entreprises sur la période 2024-2026

1• Les principales acquisitions depuis 2024 par les entreprises françaises

Airbus Defence and Space renforce sa stratégie de souveraineté cyber avec l'acquisition annoncée d'Ultra Cyber

En mars 2026, Airbus Defence and Space a annoncé la signature d'un accord définitif en vue d'acquérir Ultra Cyber Ltd auprès du groupe Cobham Ultra. Cette opération s'inscrit dans une stratégie plus large visant à maintenir Airbus en tant qu'acteur européen de premier plan dans la cybersécurité multi-souveraine, tout en consolidant sa position de partenaire de confiance du Royaume-Uni et de ses alliés.

Avec plus de 200 salariés, principalement basés à Maidenhead, Ultra Cyber apporte à Airbus des capacités cyber souveraines complémentaires de celles déjà développées au Royaume-Uni, notamment à Newport, au Pays de Galles.

L'opération permet également de renforcer le portefeuille cyber de bout en bout du groupe, tout en y ajoutant des compétences spécialisées dans les liaisons de données aéroportées, en lien avec les activités militaires d'Airbus.

Après l'acquisition d'Infodas en Allemagne en 2024, cette nouvelle étape confirme la volonté d'Airbus de structurer une activité cyber paneuropéenne couvrant plusieurs marchés nationaux clés.

Il convient toutefois de noter que la finalisation de l'opération reste soumise aux autorisations réglementaires d'usage et n'est attendue qu'au second semestre 2026.

IN Groupe finalise le rachat stratégique d'IDEMIA Smart Identity et se positionne dans le top 5 de la filière

Après l'ouverture de négociations exclusives en septembre 2024, IN Groupe a finalisé le 1er juillet 2025 l'acquisition d'IDEMIA Smart Identity.

Cette opération constitue un changement d'échelle majeur pour le groupe, qui vise désormais près d'un milliard d'euros de chiffre d'affaires et environ 4 000 collaborateurs à l'échelle mondiale.

Elle renforce simultanément ses positions dans l'identité physique, l'identité numérique et les

services de confiance, tout en élargissant son empreinte internationale.
Au-delà de la taille critique atteinte, l'opération consolide aussi des capacités technologiques clés dans les titres sécurisés, les logiciels et les solutions d'identité, dans un contexte où les enjeux de souveraineté, de cybersécurité et de conformité réglementaire se renforcent.

Orange Cyberdefense consolide sa présence européenne avec l'acquisition ciblée d'ensec en Suisse

Avec l'acquisition d'ensec, finalisée en juillet 2025, Orange Cyberdefense a poursuivi une logique de renforcement géographique et opérationnel sur un marché européen stratégique.

Cette opération permet à la filiale cyber d'Orange d'acquérir un acteur suisse reconnu dans le conseil, l'intégration de sécurité et les services de sécurité managés, tout en renforçant sa présence dans un pays caractérisé par une forte demande locale, des exigences réglementaires élevées et une sensibilité accrue aux enjeux de confiance numérique.

L'intégration d'environ 40 experts supplémentaires porte à près de 140 le nombre de spécialistes d'Orange Cyberdefense en Suisse.

Ekinops renforce son positionnement européen dans le SASE (Secure Access service Edge)

Ekinops a engagé en 2025 et 2026 une stratégie de croissance externe pour se positionner comme un acteur européen de référence sur le marché de la cybersécurité des réseaux.

Le rachat d'Olfeo, finalisé fin mai 2025, a permis au groupe d'intégrer un éditeur français spécialisé dans le SSE (Security Service Edge).
Cette opération a renforcé les capacités d'Ekinops dans la sécurisation des accès *web* et *cloud*, tout en l'installant sur les segments en forte croissance du SSE et du SASE.
Dans le prolongement de cette première acquisition, Ekinops a annoncé en mars 2026 le rachat de Chimere, spécialiste français du ZTNA (Zero Trust Network Access) universel.

Cette seconde opération complète le portefeuille technologique du groupe et accélère l'exécution de son plan stratégique visant à proposer une offre intégrée combinant SD-WAN, SSE et ZTNA. À travers ces deux acquisitions, Ekinops cherche ainsi à construire une offre européenne souveraine de cybersécurité des accès, capable de répondre aux besoins croissants des entreprises et des opérateurs en matière de connectivité sécurisée, de conformité et de déploiement simplifié.

Le Royaume-Uni apparaît comme le marché étranger le plus attractif pour les acquéreurs français

Les opérations recensées montrent une attractivité particulière du Royaume-Uni pour les entreprises françaises. Depuis 2024, cinq acquisitions de cibles britanniques ou implantées au Royaume-Uni ont été engagées : Bridewell par I-Tracing, Dionach par Nomios, MetaCompliance par Keensight Capital, Intragen par Nomios, ainsi que l'acquisition d'Ultra Cyber annoncée par Airbus Defence and Space en mars 2026.

Ces opérations portent sur des expertises variées et complémentaires, allant du conseil stratégique en cybersécurité à la gestion des identités, en passant par le *pentest*, la sensibilisation au risque humain et les capacités cyber souveraines liées à la défense.

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

Les capitaux américains demeurent au cœur des opérations impliquant des entreprises françaises

Les acteurs américains restent très présents dans les rachats d'entreprises françaises de la filière. Parmi les exemples les plus marquants figurent l'acquisition d'Expert Lines par Neverhack, groupe français passé sous contrôle majoritaire de Carlyle, celle de PingCastle par Netwrix et celle de Secure-IC par Cadence.

Ces opérations concernent des segments variés mais stratégiques, allant des services cyber à l'audit de sécurité des environnements Active Directory, en passant par la cybersécurité embarquée et les IP de sécurité.

Le rachat de Vade Security par Hornetsecurity en 2024, puis celui d'Altospam par ce même groupe en 2025, ont d'abord renforcé l'ancrage français de Hornetsecurity dans la sécurisation des emails.

Mais l'opération a pris une dimension supplémentaire avec le rachat de Hornetsecurity par Proofpoint, finalisé en décembre 2025.

Ce point est d'autant plus notable que Vade avait auparavant été engagée dans un contentieux important avec Proofpoint aux États-Unis sur des questions de propriété intellectuelle et de secrets d'affaires.

CGI rachète Apside et renforce sa base technologique et sectorielle en France

L'acquisition d'Apside par le canadien CGI, finalisée en août 2025, illustre également l'intérêt d'acteurs étrangers de grande taille pour des entreprises françaises disposant d'une masse critique et d'expertises technologiques différenciantes.

Avec plus de 2 500 collaborateurs, dont 2 200 en France, Apside permet à CGI de consolider sa présence sur le marché français et de renforcer ses capacités dans plusieurs domaines stratégiques, parmi lesquels les données, l'intelligence artificielle, le *cloud* et la cybersécurité.

3.6 UN RALENTISSEMENT DES INVESTISSEMENTS EN 2024 QUI SE CONFIRME EN 2025

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.

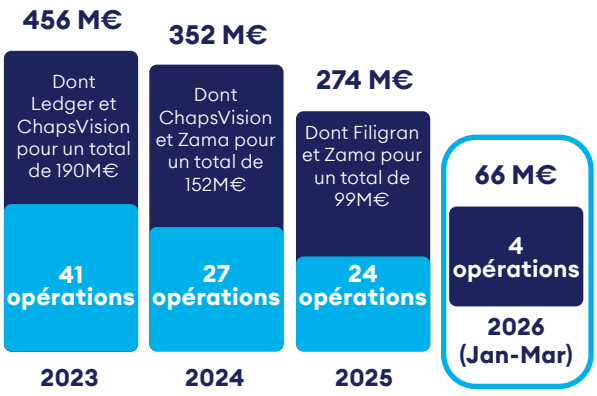
Après le pic observé en 2023, les levées de fonds des *startups* françaises de la confiance numérique ont ralenti sur les deux années dernières années. Le montant total levé est passé de 456 M€ pour 41 opérations en 2023 à 352 M€ pour 27 opérations en 2024, puis à 274 M€ pour 24 opérations en 2025. La contraction observée en 2024 s'est donc prolongée en 2025. Le début de l'année 2026 reste encore trop partiel pour dégager une tendance de fond, avec 66 M€ levés sur 4 opérations entre janvier et mars, mais il montre que des tickets significatifs continuent d'être réalisés.

Cette dynamique reste en outre portée par quelques opérations structurantes. En 2023, Ledger et ChapsVision concentraient à elles seules 190 M€, soit un peu plus de 40 % des montants levés. En 2024, ChapsVision et Zama représentaient 152 M€ sur 352 M€, soit plus de 43 % du total. En 2025, la concentration demeure élevée, avec Filigran et Zama totalisant 99 M€ sur 274 M€. Autrement dit, malgré le reflux du nombre d'opérations, l'écosystème français continue de faire émerger chaque année plusieurs tours de table de taille significative. Le baromètre 2026 de Tikehau Capital confirme cette résilience, tout en montrant un léger tassement français en 2025. Le baromètre recense 22 levées en France pour 221,6 M€ en 2025, avec un ticket moyen d'environ 10,1 M€, contre 25 levées en 2024. Il souligne aussi que la France demeure un acteur majeur en Europe, se classant troisième en montants levés comme en nombre d'opérations en 2025.

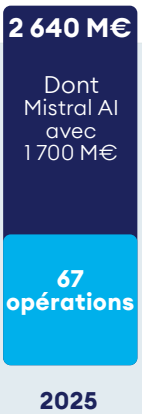
Ce positionnement doit être lu dans un contexte européen redevenu plus porteur pour la cyber. Selon Tikehau, le nombre de levées en cybersécurité en Europe a progressé de 34% entre 2024 et 2025, tandis que les montants levés ont augmenté de 83%, à rebours de la tendance observée tous secteurs confondus. Autrement dit, la France évolue dans un marché européen redevenu dynamique, mais où la concurrence entre écosystèmes nationaux s'est renforcée, notamment avec le retour en force du Royaume-Uni et la bonne tenue d'autres marchés.

Enfin, l'année 2025 a aussi confirmé la capacité de l'écosystème français à faire émerger des champions technologiques visibles à l'échelle mondiale. Le baromètre Tikehau cite notamment Zama parmi les nouvelles licornes mondiales de la cybersécurité en 2025.

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 en 2025 des niveaux très supérieurs à ceux observés dans la cybersécurité. Les entreprises françaises de l'IA ont levé 2,64 milliards d'euros à travers 67 opérations, dont 1,7 milliard d'euros pour Mistral AI à elle seule. Rapportés aux 274 M€ levés dans la confiance numérique sur 24 opérations la même année, ces montants placent l'IA à un niveau près de dix fois supérieur en valeur et près de trois fois supérieur en nombre d'opérations ; la seule opération Mistral représente en outre près des deux tiers des montants levés dans l'IA.
Ce différentiel ne remet pas en cause l'importance stratégique de la cybersécurité, mais illustre l'attractivité exceptionnelle de l'IA auprès des investisseurs, dans un contexte où ce segment concentre une part très importante des anticipations de croissance et de transformation technologique.

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

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	Filigran		2025	50
2	Zama	**ACN**	2025	49
3	Riot		2025	27.7
4	Sekoia	**ACN**	2025	26
5	Gatewatcher		2025	25
6	Dfns		2025	15.5
7	Qevlar AI		2025	13
8	Memority		2025	13
9	Evertrust		2025	10
10	BforAI		2025	9
11	Kerys		2025	6.2
12	CYGO		2025	5
13	Dastra		2025	4.3
14	Tremau		2025	3
15	Nucleon		2025	3
16	Plakar		2025	2.6
17	MokN		2025	2.6
18	Aleph		2025	2
19	Galink		2025	1.6
20	Skyld		2025	1.5
21	Akidaia		2025	1.3
22	Dream On Technology		2025	1.3
23	Avanoo		2025	1
24	Vaultys	**ACN**	2025	0.6
	Total ACN			**76**

Janvier à avril 2026

	Entreprise	Syndicat	Année	Montant (M€)
1	Riot		2026	25.5
2	Sekoia.io	**ACN**	2026	20
3	Cryptio		2026	15
4	CyGo Entrepreneurs		2026	5,4

POINT DE VUE

BAROMÈTRE DE L'INVESTISSEMENT EUROPÉEN EN CYBERSÉCURITÉ

7ème édition – Mars 2026

TIKEHAU CAPITAL

François Lavaste

Executive Director

Comme chaque année, Tikehau Capital a publié, en partenariat avec le Forum InCyber, la **7ème édition** de son baromètre cyber. Il est devenu une vraie référence et couvre l'ensemble des opérations de financement et de M&A de l'année **2025**, en France, en Europe, en Israël et aux USA.

Première tendance majeure de 2025 : au niveau global, le financement de la cybersécurité continue de croitre **avec 15,6 Md€ en montants levés pour 866 opérations**, soit **+29% en montants et +26% en nombre d'opérations.** L'année 2025 atteint ainsi un record historique en termes de nombre de levées et la seconde enregistrée après le pic de 2021, en termes de montants levés.

En 2025, **l'Europe augmente ses parts du marché global**, à la fois en termes de montants levés, passant de 9% en 2024 à 12% en 2025 ; et en termes de nombre d'opérations, passant de 25% en 2024 à 26% en 2025.

En **Europe**, le secteur de la cybersécurité surperforme clairement le secteur tech de manière générale : alors que les levées tous secteurs confondus sont en léger recul, la **cybersécurité bondit de 83 % en montants levés** atteignant 1.9 Md€ en 2025 **et de 34 % en volume** avec 226 opérations - un **record**- portée par des tours plus matures et par une consolidation principalement intra-européenne.

En **France, l'activité d'investissement en cyber se maintient à un niveau élevé avec 22 levées (vs. 25 en 2024) en nombre d'opérations**, mais le montant levé baisse à 221 M€ (vs. 342 M€ en 2024) ainsi que la taille du ticket moyen qui passe à 10,1 M€ (vs. 14 M€ en 2024). En 2025 Tikehau Capital a soutenu par exemple la société Memority en lui apportant 13 M€ et annoncé une prise de participation majoritaire dans Intersec.

En conclusion, le bilan global de l'année 2025 est très positif, en particulier au niveau global et européen. Il devient de plus en plus clair que les enjeux dans les domaines cyber et IA ne sont plus seulement français mais européens. La France continue cependant d'être bien positionnée, avec l'annonce de sa première licorne cyber (Zama, spécialiste de la cryptographie open-source). L'année 2026 devrait confirmer l'ancrage de la **cybersécurité comme pilier durable de l'innovation et de l'indépendance stratégique européenne.**

Les principales tendances de l'investissement en cybersécurité révélées par la **7ème édition du baromètre publié par Tikehau Capital**

disponible en téléchargement sur : urlr.me/7wmBGU

3. Les chiffres clefs de la filière
Observatoire ACN de la filière de la confiance numérique 2026

3.7 CONSOLIDATION DES PME ET DYNAMIQUES DE STRUCTURATION DE L'ÉCOSYSTÈME DES STARTUPS

1• La montée en maturité des PME de la 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 17,6 Mds € de chiffre d'affaires en 2025.

Cependant, un **écosystème de PME spécialisées dans la confiance numérique** a émergé à partir des années 1990 et consolide aujourd'hui sa présence. 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 2,8 et 3,9 Mds € en 2025 (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

17,6 Mds € en 2025

Emergence d'un fort écosystème de PME

2,8 à 3,9 Mds € en 2025

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).

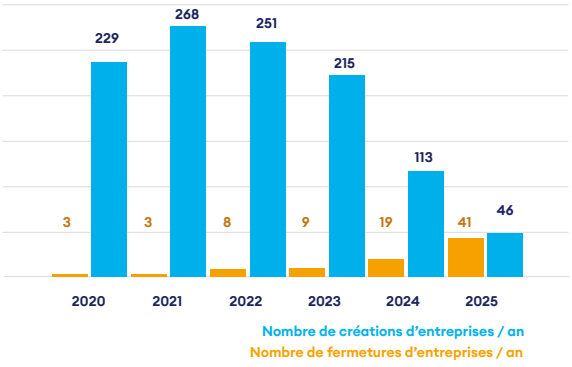
2• Les évolutions récentes de l'écosystème *startup* : créations, fermetures et procédures collectives

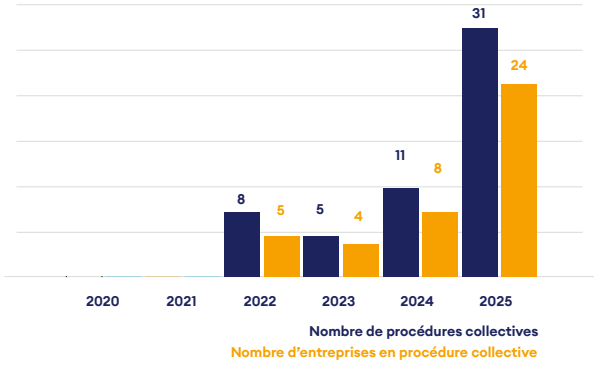
La dynamique des *startups* s'inscrit dans une trajectoire en plusieurs temps. Les années 2020 et 2021 correspondent encore au contexte de la crise sanitaire et à ses effets sur l'activité économique. L'année 2022 marque la sortie de crise, dans un contexte où la confiance numérique connaît, avec 2023, ses plus fortes croissances. Cette séquence se traduit par un volume de créations particulièrement élevé entre 2020 et 2023, avec 229 créations en 2020, 268 en 2021, 251 en 2022 et 215 en 2023. À partir de 2024, le rythme ralentit, tout en restant encore soutenu (113 créations), avant de reculer plus nettement en 2025 (46 créations). Au total, 1 129 entreprises ont été créées sur la période observée.

En parallèle, les fermetures d'entreprises restent limitées jusqu'en 2023, avec 3 fermetures en 2020, 3 en 2021, 8 en 2022 et 9 en 2023. La situation change à partir de 2024, avec 19 fermetures, puis s'accentue nettement en 2025, année où 41 fermetures sont recensées. Au total, 98 entreprises ont fermé sur la période observée. Cette évolution suggère qu'après une phase de forte expansion du tissu entrepreneurial, l'écosystème entre dans une phase plus sélective, dans laquelle toutes les entreprises créées au cours des années de forte croissance ne parviennent pas à stabiliser leur trajectoire.

Les procédures collectives confirment cette évolution. Aucun cas n'est observé en 2020 et 2021, puis 8 procédures collectives sont recensées en 2022, 5 en 2023, 11 en 2024 et 31 en 2025. Au total, 66 procédures collectives ont été identifiées, concernant 35 entreprises distinctes. L'écart entre le nombre total de procédures et le nombre d'entreprises concernées montre que certaines *startups* ont connu plusieurs événements successifs, signe de difficultés prolongées plutôt que ponctuelles. La progression rapide du nombre d'entreprises concernées, de 5 en 2022 à 24 en 2025, souligne l'extension du phénomène à une part croissante du tissu entrepreneurial.

Pris ensemble, les indicateurs de création, de fermeture et de procédure collective montrent donc une trajectoire en deux temps. La période 2020-2023 correspond à une phase de forte expansion entrepreneuriale, d'abord dans un contexte de crise puis dans celui du rebond post-crise et de la forte dynamique du marché de la confiance numérique. À partir de 2024, et plus nettement encore en 2025, l'écosystème bascule vers une phase de rationalisation, marquée par un ralentissement des créations et une montée visible des difficultés économiques.





3• Les formes de partenariat au sein de cet écosystème

À partir du sondage et des entretiens réalisés auprès des acteurs, il ressort que les *startups* cyber françaises s'inscrivent dans un écosystème où les relations avec les groupes établis jouent un rôle important, mais selon des modalités diverses. D'après les réponses au sondage, des partenariats avec de grandes entreprises sont en place pour une partie des *startups* interrogées, ils prennent d'abord la forme de relations commerciales, et ils sont globalement perçus comme positifs. Sur les 7 réponses exploitables, 3 *startups* déclarent avoir des partenariats en cours avec de grandes entreprises, principalement sous la forme de contrats commerciaux et, dans un cas, d'intégration technologique. Lorsqu'ils existent, ces partenariats sont jugés utiles, avec une note moyenne de 8,25/10 sur les réponses renseignées.

Les entretiens confirment que, sur le marché cyber français, les groupes établis interviennent auprès des *startups* selon plusieurs logiques complémentaires. Une première logique est celle de l'incubation et du *mentoring*. C'est le cas de Thales. Le groupe est partenaire cybersécurité de STATION F et a structuré depuis plusieurs années un programme dédié aux *startups* cyber, avec le dispositif Cyber@Station F, conçu pour accompagner des jeunes pousses sur des sujets de confiance numérique et de cybersécurité.

Une deuxième logique est celle de la co-innovation technologique, dans laquelle la *startup* apporte une brique spécialisée et le groupe établi apporte la capacité d'industrialisation, accès au client et crédibilité. C'est ce que montrent plusieurs cas évoqués en entretien. Chez Thales, cette logique apparaît à la fois dans les coopérations mises en avant lors de l'European Cyber Week, où le groupe a présenté des démonstrateurs cyber en lien avec des *startups* comme OverSOC, et dans le partenariat stratégique annoncé en 2025 avec Sekoia.io, destiné à intégrer la plateforme AI SOC de Sekoia dans les services managés de Thales, notamment dans des environnements de confiance comme S3NS. Les entretiens réalisés suggèrent qu'au-delà de la seule innovation technologique, ce type de coopération répond aussi à un enjeu de réduction du risque perçu par les clients finaux, en particulier dans les secteurs à cycles longs comme la défense ou le nucléaire, où la pérennité du fournisseur constitue un critère décisif.

Les entretiens soulignent qu'il est difficile pour une *startup* cyber française d'être retenue par les grands groupes, ceux-ci ayant souvent tendance à privilégier des fournisseurs internationaux déjà bien référencés. Dans ce contexte, la mise en avant d'une technologie performante, d'une architecture ouverte et d'un coût plus compétitif apparaît comme un levier de différenciation. Cette lecture est cohérente avec le positionnement public de Sekoia.io, qui met l'accent sur l'ouverture de sa plateforme, ses nombreuses intégrations et son ancrage dans la French Tech 120, tout en valorisant une approche européenne et souveraine de la détection et de la réponse.

Une troisième logique observée est celle de l'intégration commerciale et opérationnelle de technologies de *startups* dans l'offre de groupes cyber déjà installés. Almond constitue ici un cas intéressant. D'une part, Board of Cyber est présentée publiquement comme une solution développée pendant trois ans au sein de la *startup-studio* d'Almond D'autre part, Almond a noué des partenariats avec plusieurs startups spécialisées, notamment Memority sur les enjeux IAM et Qevlar AI pour l'intégration d'outils d'IA dans son SOC. Dans le cas de Qevlar AI, les communications publiques mettent en avant des gains opérationnels concrets, avec une automatisation d'une large part du traitement des alertes et une réduction sensible du temps de remédiation.

Le cas de Sopra Steria met en évidence une logique de corporate venture et de structuration d'un écosystème d'innovation. Le groupe dispose d'une entité dédiée, Sopra Steria Ventures, qui se présente explicitement comme un outil d'investissement et de partenariats stratégiques avec des *startups*, avec l'objectif de transformer leurs technologies en offres de marché concrètes.

Le sondage suggère par ailleurs que les startups cyber françaises ne se développent pas uniquement par le marché, mais aussi par leur insertion dans des dispositifs de recherche et de soutien public. Sur les 7 réponses recueillies, 4 *startups* déclarent participer à des projets de R&D coopératifs français ou européens, principalement via France 2030 et, dans un cas, via un pôle de compétitivité / projet labellisé. En parallèle, l'accès aux aides publiques apparaît très répandu dans l'échantillon : les 7 répondants citent au moins un dispositif, en particulier le CIR, France 2030 et Bpifrance.

FOCUS

LE FINANCEMENT PUBLIC DES PROJETS INNOVANTS DE LA FILIÈRE - F.INITIATIVES

Le Crédit d'Impôt Recherche « CIR », codifié à l'article 244 quater B du CGI, a été créé en 1983. C'est un mécanisme d'incitation fiscale qui a pour objectif de développer l'effort de recherche scientifique et technique des entreprises.
Le CIR est déclaratif : contrairement à une subvention, le système de contrôle est aléatoire, et se fait a posteriori de la déclaration. Le délai de reprise par l'Administration fiscale est de trois ans.

Le CIR permet le financement des activités de recherche et développement (« R&D ») et des activités d'innovation des entreprises déclarant de l'IS.

L'article 49 septies F de l'annexe III du CGI donne la définition d'une opération de recherche scientifique ou technique pouvant être éligible au CIR. La doctrine est venue préciser que les cinq critères définis dans le manuel de Frascati devaient également être remplis. Peu importe le secteur ou la taille, toutes les entreprises peuvent bénéficier du CIR.

En revanche, le Crédit d'impôt innovation (CII) est réservé aux PME - au sens communautaires - qui ne sont pas en difficultés. Attention, le CII concerne les prototypes ou installations pilotes d'un produit nouveau là où le CIR vise la prise en compte d'une opération de recherche scientifique ou technique.

En tant que « crédit d'impôt », en cas de montant de CIR supérieur au montant de l'impôt, le déclarant bénéficie d'une créance qui pourra faire l'objet d'un remboursement par l'Etat. Soit le déclarant est par exemple une PME, et il peut en obtenir le remboursement anticipé. Soit ce n'est pas le cas, et il doit imputer sur son IS son CIR avant, le cas échéant, d'en demander le reliquat après une période de trois ans.

Taux du CIR : 30 % du montant des dépenses éligibles (imputées notamment des subventions) jusqu'à 100M€ ; 5 % au delà

Taux du CII* : 20% du montant des dépenses éligibles, plafonné à 400 000 euros par an

*en France Métropolitaine

Les dépenses qui rentrent dans l'assiette du CIR

les dépenses de personnel

les dépenses de fonctionnement

les dépenses externalisées – communément appelés dépenses de sous-traitance

les dotations aux amortissements

les dépenses de normalisation

La réforme du CIR – Loi de finances 2025

Depuis la loi de finances 2025, les frais de brevets, les frais de veille technologiques, les dépenses de jeunes docteurs sont supprimés. Les frais de fonctionnement passent de 43% à 40%.

💡 Le saviez-vous ?

Le député Philippe Latombe a proposé dans un amendement déposé lors de la loi de finances 2026, un amendement afin de créer un CIR digital. Avec un taux bonifié à 40 % pour les secteurs définis annuellement par décret : IA, quantique, cybersécurité, *blockchain*, biotechnologies numériques, cet amendement a été déclaré irrecevable et n'a donc pas pu faire l'objet d'une étude en séance publique.

En parallèle, ont été déposés, à l'Assemblée nationale puis au Sénat, un amendement visant à étendre les dépenses éligibles au CIR aux dépenses afférentes à la location de temps de calcul sur les GPU et les CPU affectés aux opérations de rechercher par les entreprises d'intelligence artificielle.

Pour en savoir plus sur le CIR, téléchargez le livre blanc de F. Initiatives « Crédit d'impôt recherche - 1983 – 2023, Retour sur 40 années de financements » ainsi que son addendum sur les conséquences de la loi de finances 2025.

En matière de subventions :

- **Il faut faire une veille constante** pour regarder les appels à projets existants.
- **Le financeur** partage son cahier des charges.
- **Le projet ne doit pas avoir encore débuté** pour pouvoir solliciter l'aide.
- **Vous pouvez choisir de déposer seul votre projet, ou bien, dans le cadre d'un projet collaboratif** – c'est-à-dire que vous allez signer un contrat de consortium, vous allez prévoir la répartition des tâches, le partage des droits de propriété intellectuelle des résultats obtenus dans le cadre du projet, le régime de publication/ diffusion des résultats etc. en nommant un coordinateur, en charge de porter le projet vis-à-vis du financeur.

L'appel à projet « Pionniers de l'intelligence artificielle » a pour objectif de soutenir des projets de R&D à fort potentiel d'impact sur l'économie et qui contribuent à la souveraineté nationale grâce à des innovations de rupture en intelligence artificielle.

Son financement a été découpé en trois phases :

- **phase de financement des dépenses de faisabilité technique de la solution envisagée**, qui se base sur la technologie de rupture ;
- **phase relative à des développements** plus ambitieux ;
- et enfin une dernière **phase pour financer l'application des travaux réalisés sur un cas d'usage prometteur** sur le plan économique et la concrétisation d'un prospect pour l'industrialisation et la commercialisation de la solution développée.

POINT DE VUE

POINT DE VUE DE ABBAS DJOBO

F. INITIATIVES

Abbas Djobo

Président de F.initiatives

En tant que président de F. Initiatives, société spécialisée dans le financement de l'innovation, quels sont vos conseils aux sociétés déclarantes ?

« Tout d'abord garder en tête le fait que nous parlons d'argent public : un investissement de l'Etat, donc de chacun d'entre nous, avec pour objectif d'inciter à la réalisation d'opérations de R&D et d'innovation et ainsi augmenter la compétitivité de notre pays. Qui dit argent public dit possibilité, voir nécessité, de contrôle.
Pensez à anticiper ce contrôle et à récolter rigoureusement les éléments justificatifs en amont et au fur et à mesure de la réalisation des opérations de recherche ; assurez-vous de structurer ces opérations avant leur lancement et durant les travaux ; une attention particulière est à porter au suivant des temps des chercheurs. »

La particularité de notre filière est que nous n'avons pas de code APEC ou NAF permettant de nous identifier. Qui peut réclamer un financement public ?

« C'est ici que réside toute la puissance du Crédit d'Impôt Recherche : nous parlons d'une aide indirecte dont l'objectif est de soutenir les activités de R&D et d'innovation : pour atteindre cet objectif, les pouvoirs ont compris que la recherche se niche dans tous les secteurs d'activités et peut être menée par tout type d'entreprise. Ce support public revêt probablement une importance plus grande et utile dans les secteurs ou les activités de recherche sont les moins évidentes ou les moins développées ; ainsi, le CIR concerne tous les secteurs confondus et ceci des PME, *startups* aux Grands Groupes ; seul le projet de recherche, son éligibilité et ses éléments de justification comptent. Je ne saurai suffisamment souligner l'importance de la matérialité : être à tout moment en mesure d'établir la réalité de ses travaux. »

Quelle documentation est nécessaire pour réaliser une déclaration de CIR ?

« En plus des obligations déclaratives (Cerfa 2069) il est important de regrouper l'ensemble de ses documents dans un dossier justificatif : une description détaillée, sans pour autant être extensive, est nécessaire ; l'objectif ici est de décrire ses travaux, démontrer leur éligibilité (les travaux réalisés au-delà de l'état de l'art) et y rajouter tout éléments de nature à établir leur réalité et importance. Même si elle n'est pas obligatoire, je conseille d'utiliser ou de s'inspirer de la trame proposée par le ministère de la Recherche dans son guide annuel. »

« Déclarer un projet de CIR ne s'improvise pas. La matérialité est la pierre angulaire d'une déclaration assumée ».

Est-ce que votre société utilise également l'intelligence artificielle pour réaliser ses prestations ?

« Comme vous le savez, l'IA ne remplacera jamais l'humain, et ne réalisera pas non plus les travaux de recherche à votre place...en tout cas pas dans le cadre du CIR. L'IA est un outil d'une remarquable efficacité pour vous aider à structurer et formaliser vos travaux. F.initiatives a été assez visionnaire sur ce sujet en créant son propre laboratoire de recherche interne il y a plusieurs années : nos chercheurs, auteurs de publications internationaux, ont ainsi pu créer plusieurs outils d'aide à nos consultants et à nos clients. Neophi, une superbe aide à la réalisation de revue de littérature scientifique, en est un exemple parfait. L'ensemble de ces développements est encadré par notre certification à la norme Iso 42001 pour assurer transparence, sécurité et évidemment une éthique stricte. »

Pour terminer, un mot de conclusion ?

« Faire une déclaration de CIR ne s'improvise pas. La matérialité est la pierre angulaire d'une déclaration assumée. Je rajouterais que le CIR ne soit pas être une fin en soit, un objectif ; ce qui compte avant tout, c'est bien votre stratégie de recherche, votre projet et l'impact que vous pourrez leur donner sur votre entreprise et sur votre métier. Le CIR vous accompagnera dans cette ambition. »

NeoPhi

Pour découvrir NEOPHI, imaginé par des chercheurs, pour des chercheurs !

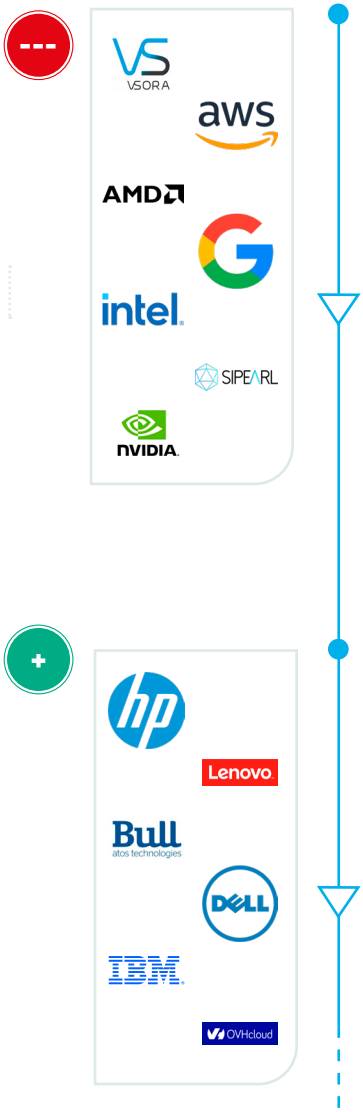
https://www.neophi.ai/fr

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 revient sur l'essor de l'IA agentique appliquée à la cybersécurité, qui constitue l'une des évolutions récentes les plus notables de la filière de l'IA 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

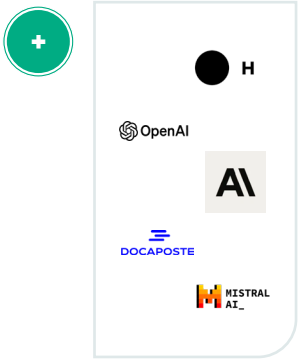
La production d'intelligence artificielle repose en amont sur les fabricants de processeurs spécialisés - GPU, NPU, ASIC... - nécessaires à l'entraînement et à l'inférence des modèles.
Ce segment est dominé par des entreprises américaines comme NVIDIA, AMD, ou encore Intel. Ces entreprises, souvent *fabless*, 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

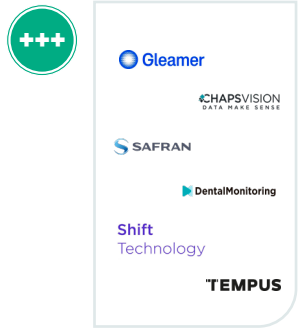
Le segment des équipements matériels - serveurs haute performance (HPC) et supercalculateurs - est dominé par les acteurs américains et chinois comme HP, Dell, IBM, ou encore Lenovo. Ces acteurs s'approvisionnent en processeurs auprès des fabricants pour assembler des solutions d'infrastructure adaptées 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

IA à usage général



IA spécifique



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. À côté de ces offres d'infrastructure, certains acteurs français développent également des plateformes permettant d'industrialiser les usages d'IA dans des environnements souverains. C'est le cas de Sopra Steria avec Innerdata, présentée comme une plateforme d'opérations d'apprentissage automatique (MLOps) et de *data*/IA destinée à accompagner le passage à l'échelle des stratégies d'intelligence artificielle, y compris dans des environnements de confiance.

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 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.

• **IAssist'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'agisse 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 éthiques 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 explicitement le critère de nationalité des entreprises.
Sont donc considérées comme faisant partie de cette production de confiance les solutions conçues par des acteurs français.

Malgré l'engouement médiatique et financier suscité par l'IA générative -notamment depuis l'émergence des LLM comme GPT, Claude ou des modèles open source comme ceux de Mistral AI- l'IA spécifique représente 78% du chiffre d'affaires généré depuis la France en 2025 (1,5 Mds €), contre seulement 22% pour l'IA générative (437 M €).

Cet écart entre visibilité et réalité économique continue de s'observer dans les levées de fonds.

En 2025, l'IA générative et les modèles généralistes ont de nouveau capté les montants les plus visibles, avec en particulier Mistral AI (1,7 Md€), mais aussi des acteurs positionnés sur des briques applicatives de génération ou de traitement de contenus, comme Moments Lab (24 M€), Aive (12 M€), Arcads AI (14 M€) ou encore PyannoteAI (8,1 M€).
Dans le même temps, les entreprises relevant d'une IA plus spécifique, intégrée à des usages métiers précis, ont confirmé leur dynamisme à travers une multiplication d'opérations de taille intermédiaire dans des secteurs variés.

C'est notamment le cas de BforeAI (9 M€) et Qevlar AI (13 M€) dans la cybersécurité, de DeepIP (15 M€) dans la propriété intellectuelle, de Veesion (38 M€) dans la computer vision appliquée au retail, ou encore de Nabla (65 M€) et SeqOne (20 M€) dans la santé. Ainsi, au-delà de quelques méga-levées très médiatisées, l'année 2025 confirme surtout l'élargissement du marché français de l'IA à un ensemble d'acteurs spécialisés, positionnés sur des cas d'usage sectoriels et des fonctions métier de plus en plus diversifiés.

Au-delà, le segment de l'IA de confiance reste globalement immature en 2025, avec un chiffre d'affaires moyen par employé bien plus faible que dans les autres segments de la confiance numérique (84 000 €).

4.4 L'ESSOR DE L'IA AGENTIQUE APPLIQUÉE À LA CYBERSÉCURITÉ

L'une des tendances récentes les plus marquantes au sein de la filière de l'IA de confiance réside dans l'essor de l'IA agentique appliquée à la cybersécurité. Par IA agentique, on entend ici des systèmes capables d'enchaîner, sous supervision humaine, plusieurs étapes d'analyse, d'investigation, de décision et d'exécution au sein d'un même processus opérationnel. Cette évolution marque un changement important : il ne s'agit plus seulement d'utiliser l'IA pour assister ponctuellement un analyste ou générer du contenu, mais pour automatiser de bout en bout certaines tâches critiques de détection, de qualification et de réponse aux incidents.

Cette dynamique se matérialise déjà chez plusieurs acteurs de la filière. Sopra Steria a ainsi introduit en février 2026 des fonctions de *workflow* agentique dans sa plateforme IAKA, afin d'orchestrer des agents IA capables d'enchaîner plusieurs étapes d'analyse et de production dans des processus complexes, tout en restant intégrés aux systèmes métiers existants et sous contrôle des opérateurs. Sekoia.io, de son côté, positionne sa plateforme AI-SOC sur l'automatisation de la détection et de la réponse, et a explicitement indiqué en 2025 vouloir accélérer ses investissements dans l'agent-based AI ; l'entreprise souligne d'ailleurs qu'une part significative des menaces détectées par sa plateforme l'a déjà été automatiquement grâce à ses technologies d'IA et de *cyber threat intelligence*.

Almond illustre également cette évolution à travers son partenariat avec Qevlar AI, qui vise à industrialiser l'investigation automatisée des incidents cyber au sein du SOC et à réduire fortement les temps de remédiation sur une grande partie des alertes traitées.

L'essor de l'IA agentique dans la cybersécurité ne concerne pas seulement les grands intégrateurs et les ESN, mais aussi les éditeurs spécialisés. WALLIX a renforcé en 2025 sa stratégie IA par l'acquisition de la *startup* française Malizen, spécialisée dans l'analyse de données de cybersécurité par intelligence artificielle.

À l'échelle européenne, la levée de fonds de 10 millions d'euros réalisée par Equixly en décembre 2025 confirme également l'intérêt des investisseurs pour des solutions d'agentic AI appliquées à la sécurité offensive et au test automatisé de la sécurité des API.

La création de valeur ne se situe plus uniquement dans les infrastructures d'hébergement ou dans les modèles généralistes, mais de plus en plus dans des briques logicielles capables d'automatiser des opérations cyber complexes sur des données sensibles et contextualisées.

Dans cette perspective, l'IA agentique apparaît comme un prolongement naturel de l'IA spécifique de confiance. Elle repose moins sur l'accès aux plus grands volumes de données généralistes que sur la capacité à mobiliser des données métier, de l'expertise, des scénarios opérationnels et des environnements sécurisés. Pour la filière française, l'enjeu stratégique est donc moins de rivaliser frontalement avec les *hyperscalers* sur l'ensemble de la chaîne de valeur de l'IA générative que de structurer des offres verticales, souveraines et intégrées, capables de *combiner expertise cyber*, automatisation avancée, supervision humaine et exigences élevées de confiance.

POINT DE VUE

L'ALIGNEMENT, GAGE DE CONFIANCE DANS LES SYSTÈMES D'IA

Vanina Paoli-Gagin

Sénatrice de l'Aube (Grand Est)

Chaque révolution technologique charrie son lot de peurs, de fantasmes et de résistances. Lorsque apparurent les premiers avions, certains affirmaient que le corps humain ne supporterait jamais une telle vitesse. Ces prédictions nous rappellent pourtant une constante : face à l'innovation, les inquiétudes légitimes côtoient toujours les intérêts établis, les asymétries d'information et les réflexes de protection.

L'intelligence artificielle (IA) ne fait pas exception. Elle suscite un immense espoir, mais aussi une inquiétude profonde, qui n'a rien d'irrationnel.

L'IA transforme déjà notre rapport au travail, à la connaissance, à l'information, à la décision, à la création. Elle recompose les rapports de puissance politique et économique, brouille les repères entre assistance, automatisation et délégation, floute les frontières entre le rêve et la réalité. Elle crée de nouvelles opportunités, mais aussi de nouvelles vulnérabilités, en ce qu'elle transforme profondément le rapport des humains au monde.

La mauvaise réponse serait de choisir entre deux postures également stériles : le refus de principe ou l'adhésion aveugle.

Sans doute la bonne question est-elle ailleurs : à quelles conditions pouvons-nous et sommes-nous prêts à faire confiance à l'IA ?

Cette confiance, métal rare de notre siècle, ne se construit ni par le marketing, ni par l'incantation, ou la seule promesse d'un progrès économique futur. Elle repose sur une exigence existentielle : l'alignement des systèmes d'IA.

Un système d'IA est aligné lorsque son comportement effectif demeure conforme aux intentions humaines, aux limites qui lui sont fixées et aux valeurs que nous jugeons légitimes.
Cette définition très concrète pose une question simple : comment s'assurer qu'un système, capable de s'autonomiser, toujours plus puissant et diffusé, continue de faire ce que nous attendons réellement de lui ?

Un système n'est pas digne de confiance seulement parce qu'il fonctionne dans une démonstration ou dans un cadre expérimental. Il l'est si nous sommes capables de vérifier qu'il demeure fiable, maîtrisable et robuste dans des conditions réelles, au contact d'environnements ouverts et sensibles, sous la contrainte et face à l'imprévu.

Cela suppose de rendre les systèmes compréhensibles, contrôlables et gouvernables grâce à des méthodes d'évaluation, des capacités de vérification, des standards, des dispositifs d'audit, des chaînes de responsabilité.

« L'alignement, ce n'est pas seulement éviter le crash, c'est aussi porter un enjeu mêlant souveraineté, compétitivité et modèle de société, voire d'humanité »

Cet enjeu devient décisif à mesure que l'IA s'installe dans les secteurs où la défaillance n'est pas acceptable : défense, infrastructures critiques, santé, finance, éducation, services publics.
Pour filer la métaphore aérienne, il ne s'agit pas de limiter arbitrairement la vitesse de l'avion, mais de faire en sorte que le pilote garde un avion fiable et la maîtrise de sa trajectoire pour conduire les voyageurs à bon port.

C'est je crois dans cet esprit que le Premier ministre m'a confié, fin février, une mission parlementaire sur l'alignement des systèmes d'IA. L'objectif en est clair : cartographier les acteurs concernés, recenser les initiatives existantes, évaluer les conditions techniques, économiques, institutionnelles et éthiques d'un alignement effectif, et identifier les leviers permettant à la France et à l'Europe de se positionner sur ce sujet stratégique.

Car l'alignement, ce n'est pas seulement éviter le crash, c'est aussi porter un enjeu mêlant souveraineté, compétitivité et modèle de société, voire d'humanité.

Pour que l'IA soit adoptée largement, utilement et durablement, nous devons être capables de démontrer qu'elle reste compatible avec nos principes démocratiques, nos exigences de sécurité et notre conception de la responsabilité, y compris environnementale. Si nous voulons peser dans la structuration des standards internationaux qui tirent les marchés, adoptons une posture dynamique en faisant de l'alignement un champ d'excellence et un levier de compétitivité pour la France et l'Europe.

À mesure que cette mission avance, j'ai l'intime conviction qu'il nous faut bâtir une véritable filière industrielle de l'alignement, embarquant chercheurs, industriels, acteurs publics, évaluateurs et normalisateurs, jusqu'aux utilisateurs finaux.

L'IA n'attendra pas que nous ayons fini d'en débattre. La question est donc simple : voulons-nous seulement accompagner le mouvement, pour le subir in fine, ou voulons-nous en être le moteur en arrêtant les finalités, en fixant les règles et les garanties que nous voulons ?

La confiance numérique de demain ne se gagnera pas contre l'IA, mais avec notre aptitude, dans un contexte où l'intrication réalité/fiction sera de plus en plus étroite, à en faire une technologie alignée.

5. POINT SUR LA MENACE INFORMATIQUE

5.1 PANORAMA ANSSI DE LA CYBERMENACE 2025

Le Panorama de la cybermenace 2025 publié par l'ANSSI dresse un état des lieux rigoureux d'une cybermenace qui reste élevée, diversifiée et systémique en France et en Europe.

Panorama ANSSI de la cybermenace 2025

disponible en téléchargement sur :
urlr.me/SDbxBj

L'année 2025 se caractérise par une complexification des attaques, un brouillage croissant des frontières entre acteurs étatiques et cybercriminels, ainsi qu'une sophistication accrue des techniques offensives. L'ANSSI a traité 3 586 événements de sécurité en 2025, soit une diminution de 18 % par rapport à 2024, en partie attribuable au pic exceptionnel de signalements lié aux Jeux Olympiques de Paris. Malgré cette baisse, le nombre d'incidents confirmés reste stable à 1 366, avec une concentration marquée dans quatre secteurs : l'éducation et la recherche (34 %), les ministères et collectivités territoriales (24 %), la santé (10 %) et les télécommunications (9 %).

Sur le plan des motivations, les attaques à finalité financière, notamment par rançongiciel, demeurent dominantes avec 128 compromissions recensées en 2025, contre 141 en 2024. Les PME, TPE et ETI restent les principales cibles, mais les établissements de santé voient leur part augmenter à 8 %, tandis que les établissements scolaires primaires et secondaires ont été particulièrement touchés. Une tendance préoccupante est l'adoption de rançongiciels par des acteurs étatiques, notamment nord-coréens et chinois, brouillant davantage la frontière entre cybercriminalité et espionnage. Parallèlement, les exfiltrations de données sans chiffrement progressent significativement, avec 196 incidents recensés en 2025 contre 130 en 2024, souvent attribués à des groupes exploitant des vulnérabilités *zero-day*, comme celle affectant Oracle E-Business Suite. L'utilisation d'*infostealers* comme vecteur d'intrusion initiale s'intensifie également.

L'espionnage stratégique mené par des acteurs étatiques, en particulier russes et chinois, reste une menace majeure. Les modes opératoires (MOA) tels que Laundry Bear (Russie), RedDelta/ Mustang Panda (Chine) et Salt Typhoon ciblent prioritairement les entités diplomatiques, gouvernementales, les infrastructures critiques et les secteurs de la défense. Ces acteurs exploitent des vulnérabilités logicielles et des techniques d'ingénierie sociale avancées, comme le SIM-swapping ou le MFA Fatigue, pour accéder à des informations sensibles. Parallèlement, les opérations de déstabilisation, notamment les attaques par déni de service (DDoS) et les tentatives de sabotage d'infrastructures critiques, se multiplient. En France, des hacktivistes pro-russes ciblent des micro-installations industrielles exposées sur Internet, bien que les impacts physiques restent limités.

L'innovation dans les capacités offensives est un marqueur fort de 2025. Les attaquants détournent massivement des outils légitimes, tels que les services cloud (Google Drive) ou les plateformes de développement (Pipedream), pour contourner les détections et réduire leurs coûts opérationnels.

L'intelligence artificielle générative est également instrumentalisée pour automatiser des campagnes de *phishing* personnalisées ou polluer les données d'entraînement des modèles.

Les techniques d'ingénierie sociale se diversifient, avec des campagnes incitant les victimes à exécuter elles-mêmes des commandes malveillantes, ou des attaques vocales usurpant des autorités de confiance. L'ANSSI note une collaboration accrue entre acteurs malveillants, qu'il s'agisse de partage d'outils, comme la réutilisation de vulnérabilités exploitées ou de sous-traitance de phases d'attaque via des courtiers en accès initiaux. Cette interpénétration entre écosystèmes criminels et étatiques complexifie l'imputation des attaques, d'autant que des fuites de données internes révèlent des liens personnels entre cybercriminels et services de renseignement, sans pour autant prouver une coordination systématique.

Cependant, les vulnérabilités techniques restent le vecteur d'intrusion le plus exploité, avec un ciblage récurrent des équipements de bordure, tels que les pares-feux, les VPN et les solutions SharePoint, ainsi que des failles jour-zéro. Les incidents traités par l'ANSSI illustrent des lacunes persistantes en gestion des correctifs : en 2025, plus de 6 200 actifs français étaient encore vulnérables à des failles critiques publiées depuis 2023. Les attaques via la chaîne d'approvisionnement se généralisent, touchant aussi bien les sous-traitants industriels de la Base Industrielle et Technologique de Défense (BITD) que les prestataires *cloud*, dont la compromission peut impacter des centaines de clients. Le secteur éducatif, souvent peu sécurisé, et les environnements mobiles, via l'exploitation de vulnérabilités iOS/Android, sont des points d'entrée fréquents.

Face à ce constat, l'ANSSI insiste sur l'importance de la résilience collective, renforcée par la transposition de la directive NIS2 et le Cyber Resilience Act, qui imposeront, très prochainement, des obligations de sécurité accrues pour les opérateurs critiques. La complexité des environnements numériques et la volatilité des menaces, avec une durée de vie moyenne d'un groupe de rançongiciel estimée à 262 jours, exigent une veille permanente et une adaptation continue des défenses. Les recommandations de l'ANSSI, telles que la réalisation d'audits globaux des systèmes d'information, le cloisonnement des usages professionnels et personnels, ou la sécurisation des accès VPN, soulignent un impératif : la cybersécurité doit désormais être abordée comme un enjeu stratégique intégrant les dimensions humaines, juridiques et géopolitiques.

34 %
des incidents cyber en 2025 concernent le secteur de l'éducation et de la recherche.

48 %
des victimes d'attaque par rançongiciel concernent les PME/TPE/ETI soit une augmentation de 11%.

18 %
d'augmentation de la publication de vulnérabilités par an depuis 2020.

5.2 REGARDS CROISÉS DES EXPERTS DU SECTEUR

RED ALERT LABS

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. »

YesWeHack

Aïmad BERADY
Chief Product Officer

Cachez-moi ces « vulnérabilités » que je ne saurais traiter !

« L'industrie cyber subit une dérive alarmante : l'amoncellement d'événements de sécurité qualifiés de « vulnérabilités » sature les backlogs. Noyées sous les alertes de scanners automatisés dénués de contexte, les équipes s'épuisent sur des pseudo-incidents au détriment des failles réellement impactantes. Cette course à l'exhaustivité crée un faux-semblant de sécurité. Pour retrouver une réelle résilience, il est nécessaire de séparer le bruit du signal en préservant l'humain au cœur du dispositif. L'expert cyber, augmenté par l'IA au besoin, reste le seul capable d'appréhender le contexte métier, de prouver l'exploitabilité et de qualifier le risque réel. L'enjeu n'est plus de corriger aveuglément, mais de collecter, de se focaliser et de neutraliser uniquement ce qui menace l'organisation »

THALES
Building a future we can all trust

Christophe BIANCO
VP Cybersecurity Services

En 2026, la cybersécurité devient une condition de confiance à échelle mondiale.

« L'essor de l'IA intensifie les menaces : automatisation des attaques, phishing ciblé et modèles d'IA visés. Les organisations répliquent avec une cybersécurité augmentée grâce à l'IA, des SOC plus résilients voire semi-autonomes et une surveillance IT/OT intégrée. Les campagnes hybrides mêlant États et cybercriminels se multiplient, tandis que la protection des chaînes d'approvisionnement et des environnements OT reste critique. Le risque quantique et le « Harvest Now, Decrypt Later » imposent une cybersécurité agile, soutenue par NIS2, DORA et le Cyber Resilience Act. 2026 est une année charnière : la cybersécurité n'est plus un simple bouclier mais un avantage compétitif et une condition de confiance à l'échelle mondiale. »

v6Protect

Florian BOMBARD
Président

L'IA : nouveau carburant des cybermenaces

« L'IA a ouvert de nouvelles portes aux attaquants : nul besoin de coder, il suffit d'instruire un modèle pour concevoir et lancer une attaque. Les offensives gagnent en furtivité, en précision et en impact, mettant en échec les défenses conventionnelles. Deux tendances s'imposent en 2025/2026. D'abord, les bots mutent et s'adaptent : le trafic des bots IA a bondi de 300 % depuis juillet 2024, tandis que les attaques DDoS progressent de 94 %. Ensuite, les cybercriminels ciblent massivement les API et les LLM, devenus le nouvel eldorado pour monétiser les données critiques. Face à cette menace augmentée, les entreprises doivent impérativement cartographier et réduire leur surface d'attaque, et s'appuyer sur l'analyse comportementale pour protéger leurs services numériques. »

iDAKTO

Yann BOUAN
Chief Strategy Officer

La gouvernance des identités, enjeu systémique de la cybersécurité

« Derrière les incidents les plus significatifs de 2025, une même mécanique : l'attaquant n'a pas forcé l'entrée, facteur d'authentification insuffisant, périmètre prestataire mal délimité, données personnelles surstockées ; autant de fragilités structurelles qui précèdent toute défaillance technique. La surface d'exposition d'une organisation se mesure à l'ensemble des identités qu'elle administre, ou néglige d'administrer. Réduire les données collectées au strict nécessaire et maîtriser chaque accès dans la chaîne constituent les deux décisions de sécurité les plus structurante. »

Phragma.

Frédéric CERCLET
Gérant

Identité numérique : mieux protéger nos données

« Les fuites de données sont devenues quotidiennes, touchant tous les secteurs d'activité. Le constat est alarmant : chaque français aurait ses données dans au moins une base compromise et revendue. Malgré le RGPD, la protection des données confiées à des tiers demeure un échec. Les conséquences sont bien réelles : usurpations d'identité et phishing ciblé en hausse, auxquels s'ajoutent des deepfakes rendant les arnaques toujours plus difficiles à détecter. Le wallet d'identité numérique prévu par eIDAS v2 vise à réduire ces fuites : chaque citoyen ne partagera que les informations strictement nécessaires. Une avancée prometteuse, à condition de l'accompagner d'une sensibilisation et d'un écosystème public-privé solide. Un beau défi pour les industriels et prestataires d'audit du numérique ! »

iliadata

Julia CHAULET
CEO & cofondatrice

Repenser la confiance numérique à l'ère des menaces systémiques

« Les fuites massives de données et les tensions géopolitiques actuelles révèlent une réalité : la confiance dans les infrastructures numériques n'est plus acquise. Dans ce contexte, les modèles de sécurité classiques atteignent leurs limites, alors même que les organisations doivent concilier protection des données et autonomie technologique. Il devient nécessaire de repenser en profondeur qui contrôle, traite et protège la donnée, en intégrant un fait désormais incontournable : la perte de maîtrise sur les infrastructures. Dans ce cadre, la cryptographie s'impose comme un levier stratégique, en apportant des garanties techniques robustes. »

François DERUTY
Chief Intelligence Officer

La CTI : boussole stratégique dans un cyberespace fragmenté

« En 2025-2026, l'instabilité géopolitique redessine la menace. Nous observons une hybridation inédite : les opérations étatiques de sabotage ou d'espionnage s'inspirent des tactiques cybercriminelles, et inversement. Face à des adversaires qui mutualisent leurs infrastructures, la défense purement réactive est aveugle. C'est ici que la Cyber Threat Intelligence (CTI) devient vitale. Elle n'est plus un luxe, mais le moteur de l'anticipation. En décryptant les modes opératoires et en contextualisant la menace, la CTI permet aux organisations d'adapter dynamiquement leur posture. Face au brouillard géopolitique actuel, intégrer nativement le renseignement au cœur des opérations de sécurité est la seule voie pour transformer l'incertitude en véritable résilience cyber. »

Alexandre DIEULANGARD
Co-fondateur
et Directeur Général

Ni panique, ni déni : l'IA exige une lecture calibrée du risque

« En 2025 et 2026, l'intelligence artificielle (IA) s'est confirmée comme un multiplicateur opérationnel pour les acteurs de la menace : ingénierie sociale plus crédible, fraude mieux contextualisée, indices de détection plus discrets. L'effet est réel, mais progressif, loin des scénarios de rupture qui saturent le débat public. Or c'est précisément cet écart entre réalité et perception qui constitue le risque décisionnel le plus concret. Les discours oscillent entre surestimation des capacités offensives et confiance excessive dans les garde-fous existants, deux biais qui conduisent à des arbitrages inadaptés. Les organisations les plus résilientes sont celles qui maintiennent une lecture factuelle et proportionnée : l'IA amplifie des attaques connues, elle ne les réinvente pas. »

Sébastien FAUX
CEO

Cybersécurité et IA : pourquoi les organisations peinent à suivre, selon l'ANSSI

« Le Panorama de la cybermenace 2025 de l'ANSSI est clair : la menace reste élevée, touche tous les acteurs et brouille les frontières entre cybercriminalité et actions étatiques. Mais ce qui change profondément, c'est le rôle de l'IA. Les attaquants exploitent désormais l'IA générative pour créer des phishings plus crédibles, produire des scripts malveillants ou cloner des voix lors d'attaques de vishing. Résultat : des attaquants peu qualifiés peuvent désormais mener des opérations plus sophistiquées. Dans ce contexte, se dire "sécurisé" ne suffit plus. Face au renforcement des exigences réglementaires, notamment NIS2 et le CRA, l'évaluation indépendante permet d'objectiver les mesures réellement en place, d'identifier les angles morts et d'apporter des preuves concrètes de conformité. »

Fanch FRANCIS
CEO

Ce que vous ne voyez pas vous compromet déjà

« En 2026, la menace informatique ne se distingue plus par sa sophistication mais par sa capacité à exploiter les angles morts. En effet, une part croissante des infrastructures reste invisible : systèmes non agentables, environnements hybrides, etc. Tant que la sécurité reposera sur une vision partielle et déclarative, elle restera contournable. Deux priorités pour 2026 : obtenir une visibilité exhaustive et en temps réel des communications entre systèmes, y compris là où aucun agent ni log fiable n'existe est une priorité. Cartographier en continu les actifs (dépendances et comportements) pour détecter les écarts exploitables. Sans cette base factuelle, chaque nouvel outil ajoute du bruit, pas du contrôle. »

Ramzi KHECHAIMIA
Directeur général
Co-fondateur

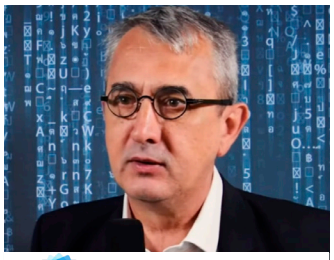
Cybersécurité 2026 : l'heure de la souveraineté opérationnelle

« En 2026, la cybermenace est automatisée, coordonnée, systémique. L'IA permet désormais d'exploiter les failles des organisations en temps réel, d'infiltrer leurs chaînes d'approvisionnement et leurs partenaires. Chaque maillon est devenu critique. NIS2, DORA, CRA imposent un niveau d'exigence inédit, sans dicter les moyens d'y répondre. Face à ce contexte, la question de la souveraineté opérationnelle s'est imposée comme une priorité concrète. Le SOC souverain s'affirme comme une réponse structurante : garder le contrôle sur la détection, réduire les délais de réaction et préserver l'autonomie décisionnelle. L'automatisation y joue un rôle central, mais c'est l'expertise humaine qui reste déterminante dans les arbitrages les plus sensibles. »

Fabien LECOQ
CEO Business Line
Cyber Groupe

Cybersécurité : la force, par la sérénité

« L'année 2025 a confirmé une intensification de la menace cyber visant les organisations européennes. En 2026, celle-ci s'inscrit durablement au cœur des chaînes de valeur numériques et des écosystèmes critiques. Les acteurs étatiques privilégient des stratégies de pré-positionnement dans les infrastructures critiques, tandis que la cybercriminalité poursuit son industrialisation. L'IA amplifie ces dynamiques en automatisant les attaques et en renforçant l'ingénierie sociale à grande échelle. Dans ce contexte, la frontière entre espionnage, influence et cybercrime s'estompe. Pour les organisations européennes, l'enjeu sera moins d'empêcher toute intrusion que de détecter, comprendre et contenir les opérations adverses afin de préserver durablement la confiance numérique. »



Philippe LOUDENOT
Directeur stratégie
cybersécurité

Menace cyber 2025-2026 : des fuites silencieuses et pernicieuses

« La menace la plus sournoise n'est pas toujours le hacker génial, mais l'habitude : une grande majorité des fuites provient d'échanges mal ou non sécurisés – liens de partage publics, pièces jointes non chiffrées, paramètres cloud mal configurés, et flux collaboratifs non contrôlés. Ces failles sont rapides, souvent automatisées, et amplifient l'impact d'une erreur humaine. Face à cette réalité, la réponse n'est pas la panique mais la simplicité et des solutions de confiance – pour que la sécurité redevienne un réflexe, pas une option. »

Philippe LUC
CEO et Cofondateur

La gestion du risque humain au cœur de la cybersécurité en 2026

« En 2025, l'ingénierie sociale a changé d'échelle, portée par l'automatisation par IA et l'exploitation massive de données volées : ANOZR WAY a identifié plus de 2,6 milliards de données compromises. Dans le même temps, les études convergent : la formation générique et les campagnes de phishing ne suffisent plus à réduire le risque humain. 2026 marque l'entrée dans une phase d'industrialisation de la gestion des risques cyber humains. Le risque humain ne relève plus de la sensibilisation mais s'intègre au cœur des métiers – gestion des identités, détection des vulnérabilités comportementales, assurance des particuliers. Pour ANOZR WAY, cela se traduit déjà par une forte accélération des demandes d'interopérabilité et de partenariats pour répondre à de nouveaux cas d'usage à grande échelle. »

Patricia MOUY
Responsable du programme cybersécurité du CEA-List

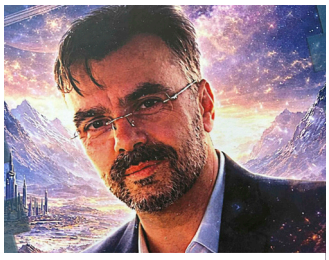
Anticiper les menaces par la recherche

« Face à l'essor continu du numérique, à l'élargissement de la surface d'attaque et à la complexité croissante des menaces, une réponse uniquement réactive ne suffit plus. Il devient essentiel d'adopter une démarche de recherche proactive, capable d'anticiper les évolutions technologiques comme les stratégies des attaquants. Dans ce contexte, l'innovation s'impose comme une condition de souveraineté, qu'il s'agisse de cryptographie post-quantique, d'IA de confiance ou de sécurité des systèmes embarqués et distribués. Les travaux du CEA-List s'inscrivent pleinement dans cette dynamique, en lien étroit avec les besoins industriels et les menaces émergentes : anticiper pour garder un longueur d'avance. »

Marc OLIVIER
CEO de HIAsecure

Face à l'IA et au post-quantique, remettre l'humain dans la boucle

« L'IA générative, les agents autonomes et, demain, le risque post-quantique, remettent en cause les fondements de l'authentification classique. Quand les attaques savent imiter, contourner, automatiser et exploiter à grande échelle, la sécurité ne peut plus reposer uniquement sur des identifiants, des codes ou des secrets réutilisables. Le véritable enjeu devient la preuve d'une action humaine consciente et contextualisée. Dans les environnements sensibles, cette évolution est décisive : il faut des mécanismes capables de conjuguer cybersécurité, souveraineté, traçabilité et résistance aux nouvelles menaces. L'avenir de la confiance numérique passera par des modèles qui valident l'intention, pas seulement l'identité. »



Dr. Florin PAUN
Cofondateur

Tous Xvaluators ! : la cybersecurité du futur sera basée sur des données qualifiées ou ne sera pas !

« Dans le contexte actuel de prolifération des données fausses ou biaisées (plus de 60% de l'IA) une nouvelle typologie IA en sciences cognitives (complémentaire des approches connectives et symboliques) découverte par le fondateur de la deeptech francaise Xvaluator (brevet obtenu en 2019) et reconnue par la communauté scientifique internationale pour avoir complété le Paradoxe de Condorcet et le théorème d'Arrow (y compris en Springer Encyclopedia) permet (comme IA embarquée) la réduction des flux des données fausses, la diminution de l'empreinte écologique et l'augmentation de la pertinence des résultats de tous les outils et usages IA. Cette innovation francaise générique et souveraine permet la prise de décision efficace en consensus et l'évolution du business model du numérique de la polarisation actuelle vers des approches «Tiers-inclus» basées sur la pertinence des données qualifiées et qualifiables dans des processus hautement collaboratifs et démocratiques. »

Valérie DE SAINT PÈRE
Présidente et cofondatrice

Face à l'industrialisation de la menace, former autrement les talents cyber

« À l'heure où l'IA offensive, l'agentique et l'automatisation redéfinissent la menace, la cybersécurité change d'échelle : attaquer devient industriel, se défendre doit le devenir aussi. Dans ce contexte, l'École 2600 fait évoluer en profondeur ses modèles pédagogiques et forme des profils capables d'opérer avec et contre ces technologies. Cela implique d'anticiper les métiers amenés à disparaître, d'intégrer la maîtrise de l'IA dans les parcours et de préparer à des usages malveillants plus sophistiqués. Fidèle à son ADN, l'école privilégie une approche fondée sur les fondamentaux – comprendre avant d'utiliser – pour ne pas réduire l'IA à un simple levier de productivité mais d'en faire un champ à maîtriser pour mieux défendre. Former vite ne suffit plus, il faut former juste et en avance. »

Cyrille VIGNON
CEO

Combattre l'IA par l'IA : la souveraineté comme impératif

« L'IA générative a contribué à industrialiser la production de malwares : des variants sont créés en quelques heures, rendant les signatures traditionnelles obsolètes. Face à cette accélération, les défenses doivent elles aussi évoluer. L'analyse comportementale du code, comprendre ce qu'un programme fait plutôt que ce à quoi il ressemble, devient une nécessité pour détecter les menaces inconnues avant qu'elles ne frappent. Mais l'IA défensive ne suffit pas : encore faut-il en maîtriser les fondations. Aujourd'hui, il y a un enjeu stratégique : garantir la souveraineté de nos outils de détection. Contrôler ses données, ses algorithmes et ses infrastructures d'analyse n'est plus une option, c'est un impératif pour l'écosystème cyber européen. »

Romain WALLER
Directeur Général

Face à la menace cyber 2026, la souveraineté des données comme pilier stratégique

« En 2026, la menace informatique atteint un niveau sans précédent : attaques étatiques, cybercriminalité industrialisée et exploitation massive des failles humaines comme techniques, exposent chaque organisation, quelle que soit sa taille. Dans ce contexte, la souveraineté des données devient un enjeu stratégique majeur. Elle garantit non seulement la maîtrise de l'information, mais aussi la capacité à protéger des actifs critiques face à des risques de plus en plus sophistiqués. Le recours à des solutions de confiance, souveraines, conçues selon les plus hauts standards de sécurité, est indispensable. Les solutions ERCOM répondent à cette exigence en assurant confidentialité, intégrité et contrôle. C'est un choix de résilience, de conformité et d'indépendance numérique. »

FOCUS

BAROMÈTRE DOCAPOSTE-CYBLEX DE LA CYBERSÉCURITÉ 2025

DOCAPOSTE

Smara Lungu

Directrice stratégie, marketing, communication et relations institutionnelles

« Le décalage se creuse entre perception et réalité du risque cyber : 2/3 des organisations déclarent avoir subi une attaque, tandis que 2/3 en minimisent encore la portée. La troisième édition de notre baromètre de la cybersécurité, co-réalisé par Docaposte avec Cyblex Consulting, le confirme. Si les mesures de base progressent, des fragilités persistent en matière de gouvernance : priorisation des actifs critiques, organisation de la réponse à incident, capacité à décider sous contrainte. Dans un contexte d'incertitude réglementaire, la capacité de décision s'affaiblit. Les attaques – *phishing* (38%), rançongiciel (28 %), perte de données (17 %) – exploitent ces failles. Le cyber devient un enjeu direct de continuité d'activité, dont la banalisation nourrit une illusion de maîtrise. »

Baromètre de la cybersécurité 2025 Docaposte-Cyblex

disponible en téléchargement sur : urlr.me/nZYEG2

DOCAPOSTE CYBLEX Consulting

Baromètre de la cybersécurité 2025

Le Baromètre de la cybersécurité, co-réalisé par Docaposte et Cyblex Consulting, permet de mesurer année après année l'évolution de la maturité cyber des entreprises et des organisations publiques.

- **1/3 des entreprises a subi une cyberattaque en 2025, comme en 2024.**

Les cyberattaques les plus courantes :

38 % Phishing

28 % Ransomware

17 % Vol/Perte de données

Leurs conséquences :

24 % Blocage des systèmes d'informations

21 % Vol et/ou perte de données

13 % Arrêt de la production

- **50 % des organisations ont maitrisé les attaques sans impact**

Les protections mises en place

89 % Gestion renforcée des mots de passe

85 % Mise à jour régulière des logiciels

81% Sauvegarde externalisée et régulière des données

+55 % des budgets cybersécurité sont en hausse (notamment dans le secteur public)

3/4 des entreprises pensent faire suffisamment d'efforts pour se protéger

env. **1/2** des entreprises privilégie des solutions packagées

1/3 des répondants connaissent et appliquent le guide de l'ANSSI

La souveraineté, essentielle dans le secteur public

55% des acteurs publics considèrent l'usage des systèmes souverains comme très important

VS

37 % des entreprises privées

6. LES TENDANCES DE MARCHÉ

6.1 LES TENDANCES GÉNÉRALES

1• La croissance de la filière française

Après le net point haut observé en 2022, la croissance de la filière française de la confiance numérique ralentit pour la troisième année consécutive. Elle s'établit à 5,4 % en 2025, après 6,4 % en 2024 et 6,8 % en 2023, tout en demeurant nettement supérieure à celle du PIB français (0,9% en 2025). Ce ralentissement ne remet pas en cause la dynamique structurelle du secteur, mais il confirme l'entrée dans une phase de croissance plus modérée, dans un environnement de demande moins porteur qu'au sortir de la période 2021-2022.

Cette évolution est d'abord liée au tassement des segments historiques. La sécurité numérique progresse de nouveau de seulement 2,4 % en 2025, comme en 2024, ce qui traduit le léger ralentissement des grands projets d'identité, de biométrie et de contrôle d'accès qui avaient fortement soutenu l'activité en 2022.
La cybersécurité continue de croître, mais de façon moins homogène : les produits cyber conservent une trajectoire relativement solide (+6,4 % en 2025 après +7,8 % en 2024), tandis que les services cyber ralentissent beaucoup plus nettement (+3,4 % en 2025 après +10,6 % en 2024). Ce décrochage montre que la conjoncture plus molle qui affectait déjà les services IT classiques touche désormais aussi les activités de services cyber.

Dans ce contexte, les marchés les plus porteurs restent ceux où la contrainte de sécurité demeure la moins arbitrable : défense, espace, sécurité, grands ministères et organismes affiliés, ainsi que banque et assurance. En parallèle, certaines PME et ETI continuent d'afficher des croissances à deux chiffres, ce qui montre que le ralentissement observé au niveau agrégé ne touche pas uniformément l'ensemble de l'écosystème et que les acteurs les mieux positionnés sur des besoins critiques ou différenciants continuent de gagner des parts de marché.

Les résultats de Thales illustrent bien cette phase de tassement chez certains grands acteurs historiques. En 2025, le segment Cyber & Digital du groupe reculait de 0,9 % en organique, la baisse étant notamment liée au processus d'intégration commerciale d'Imperva. Dans le même temps, les chiffres publiés par Thales montrent une légère progression de l'identité numérique à périmètre constant, ce qui confirme que les moteurs traditionnels de croissance restent présents, mais à un niveau plus modéré qu'auparavant.

À l'inverse, l'IA de confiance apparaît désormais comme le segment le plus porteur de la filière : après une croissance déjà élevée de 9,3 % en 2024, elle accélère fortement à 23,4 % en 2025. Cette dynamique contraste nettement avec le ralentissement des segments plus traditionnels et confirme que l'IA de confiance constitue aujourd'hui un des principaux moteurs d'expansion de la confiance numérique en France, même si son poids économique demeure encore inférieur à celui de la cybersécurité et de la sécurité numérique.

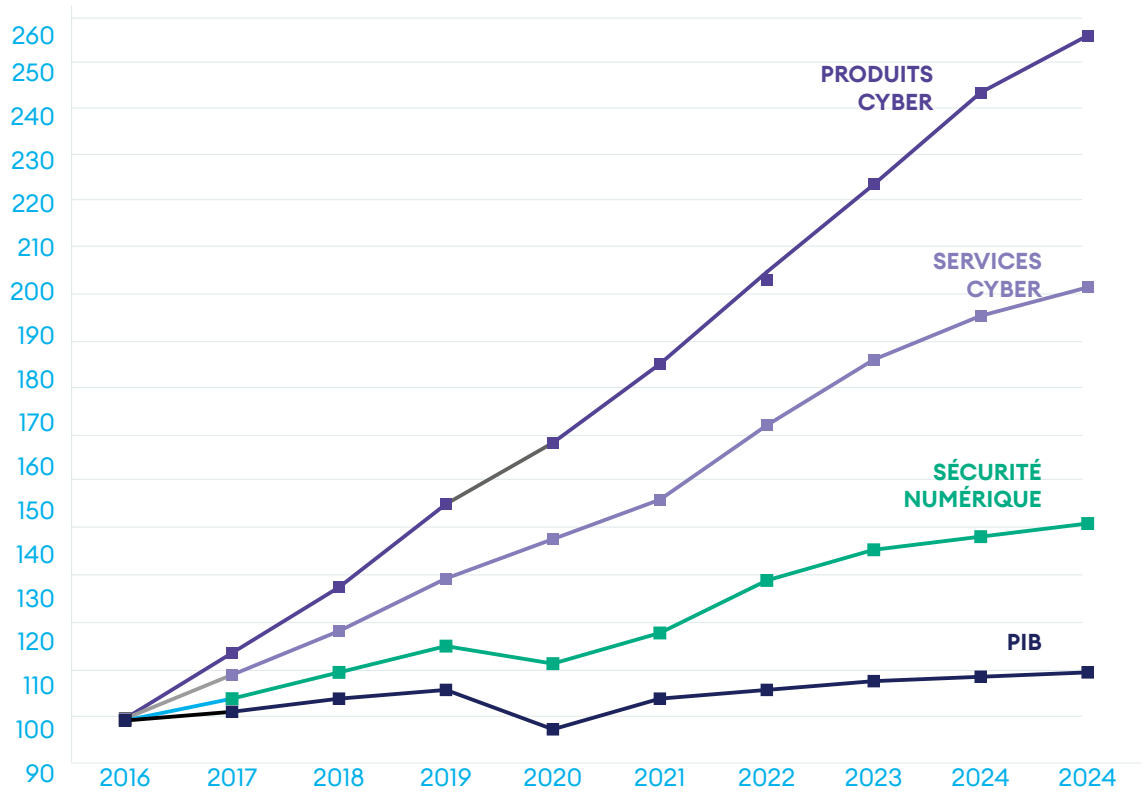
« Le rythme de croissance global de la filière se stabilise en 2025, autour de 5% »

Croissance France comparée 2017-2025

Croissance							
Segments	2019	2020	2021	2022	2023	2024	2025
Confiance numérique	8,5%	3,6%	7,3%	11,3%	6,8%	6,4%	5,4%
Produits cyber	14,0%	10,9%	8,8%	12,6%	9,0%	7,2%	6,4%
Services cyber	10,3%	5,8%	8,9%	10,3%	9,4%	10,6%	3,4%
Sécurité numérique	4,8%	-1,7%	5,2%	11,0%	3,8%	2,4%	2,4%
IA de confiance						9,3%	23,4%
PIB	1,8%	-7,8%	6,8%	2,5%	0,9%	1,1%	0,9%

Le graphique ci-dessus montre l'évolution comparée de la croissance des trois principaux segments de la filière confiance numérique et du PIB sur la période 2017-2025.

Source: INSEE



Source : DECISION Etudes & Conseil

2• Les marchés de la filière

Les marchés en 2025

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 (6,8 Mds € en 2025), les deux tiers restants provenant du secteur privé (13,7 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.

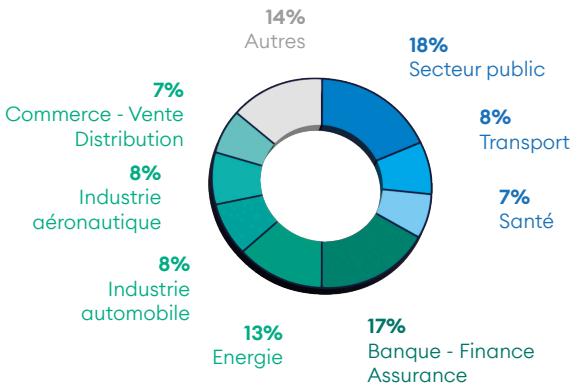
L'émergence d'un marché des PME/TPE et des petites collectivités territoriales

La série de diagrammes ci-contre montre la segmentation du marché français de la filière selon le type d'entreprise fournisseur de solutions de confiance (grande entreprise versus TPE / PME).

On observe que l'Etat, les Opérateurs d'Importance Vitale (OIV) et les grandes entreprises (hors OIV) représentent plus de 75% du marché des grandes entreprises de la filière, et 80% de leurs perspectives de croissance pour les années à venir.

Ces grandes entreprises fournisseurs de solutions de confiance représentent 57% du chiffre d'affaires de la filière en France en 2025 (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 : Etat, OIV et grands comptes privés.

Principaux marchés de la filière en 2025



Source : DECISION Etudes & Conseil, questionnaire renseigné par les entreprises de la filière en de 2022 à 2026.
Réponse en % des répondants pondérés par leur poids dans la filière.
L'échantillon représente 12% de la filière en chiffre d'affaires.

À contrario, l'État et les OIV ne représentent que 30% du marché des PME et TPE de la filière. Ce sont les grandes entreprises (31%), les PME / TPE (15%) et les collectivités locales (23%) 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 :

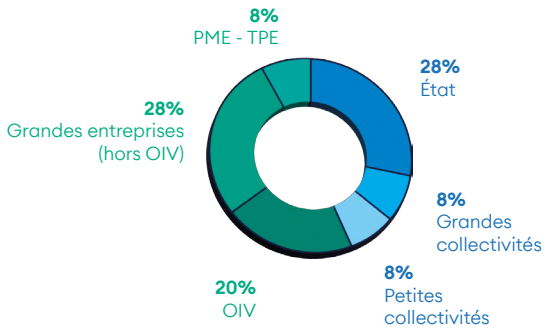
• **Celui des collectivités locales**, y compris les petites collectivités locales. Par extrapolation, on peut estimer le marché des petites collectivités locales à 3,9 milliards d'euros en 2025.
• Mais surtout, **le développement du marché associé au besoin de produits et services de confiance de la part des PME et TPE françaises**. Par extrapolation, on peut estimer ce marché à 2,3 milliards d'euros en 2025. Ce marché se caractérise par des offres dédiées : offres standardisées, déploiement rapide, faible coût, souvent sans support *hardware*...

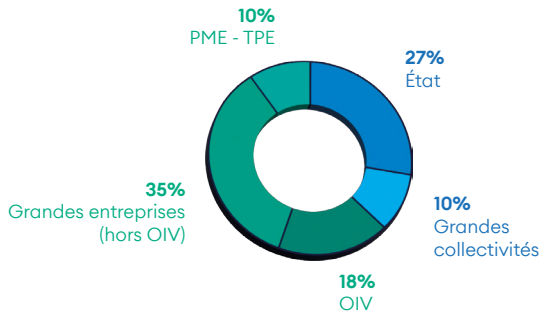
Le développement de ce marché des PME et TPE françaises a été ralenti en 2020 par la crise du COVID. En effet, les PME et TPE françaises ont été plus affectées par les restrictions associées au COVID que les grands clients traditionnels de la filière de la confiance numérique (État, OIV, grandes entreprises)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

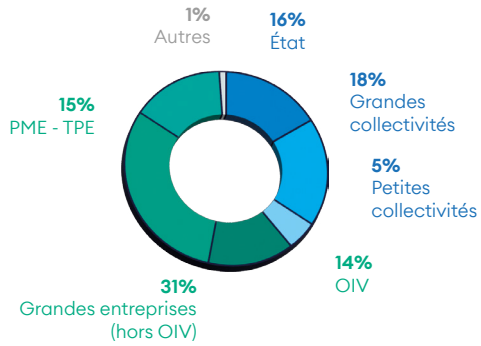
Enfin, bien qu'encore négligeables, on observe l'apparition de marchés de sécurisation des associations ou encore des particuliers.

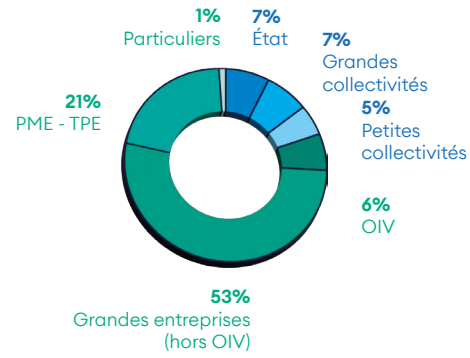
Grandes entreprises





TPE - PME





Source : DECISION Etudes & Conseil, questionnaire renseigné par les entreprises de la filière en de 2022 à 2026.
Réponses en % des répondants pondérés par leur poids dans la filière.
L'échantillon représente 12% de la filière en chiffre d'affaires.

FOCUS

STRUCTURER L'ÉCOSYSTÈME POUR PASSER À L'ÉCHELLE – LE RÔLE DU CAMPUS CYBER

CAMPUS CYBER

Joffrey Célestin-Urbain

Président du Campus Cyber

La cybersécurité est-elle devenue un nouvel enjeu de puissance ?

«La cybersécurité a clairement changé de nature ces dernières années. Longtemps considérée comme un sujet technique relevant de la protection des systèmes d'information, elle s'impose désormais comme un enjeu stratégique pour les Etats, les entreprises et les citoyens.

La transformation numérique des économies, l'augmentation des cyberattaques et l'émergence de technologies structurantes comme l'intelligence artificielle ou l'informatique quantique ont profondément modifié le paysage des risques numériques. Dans le même temps, les rivalités technologiques entre grandes puissances replacent les infrastructures numériques au cœur des enjeux de sécurité économique et d'autonomie stratégique.

Dans ce contexte, la cybersécurité dépasse la seule protection des systèmes. Elle participe directement à la résilience des sociétés, à la sécurité économique et à la capacité des États à maîtriser leurs technologies. Elle constitue désormais un pilier de la souveraineté numérique.
Le Campus Cyber s'inscrit dans cette dynamique, en étant le relais de la stratégie nationale cyber et en contribuant à sa mise en œuvre opérationnelle.»

Farida Poulain

Directrice générale du Campus cyber

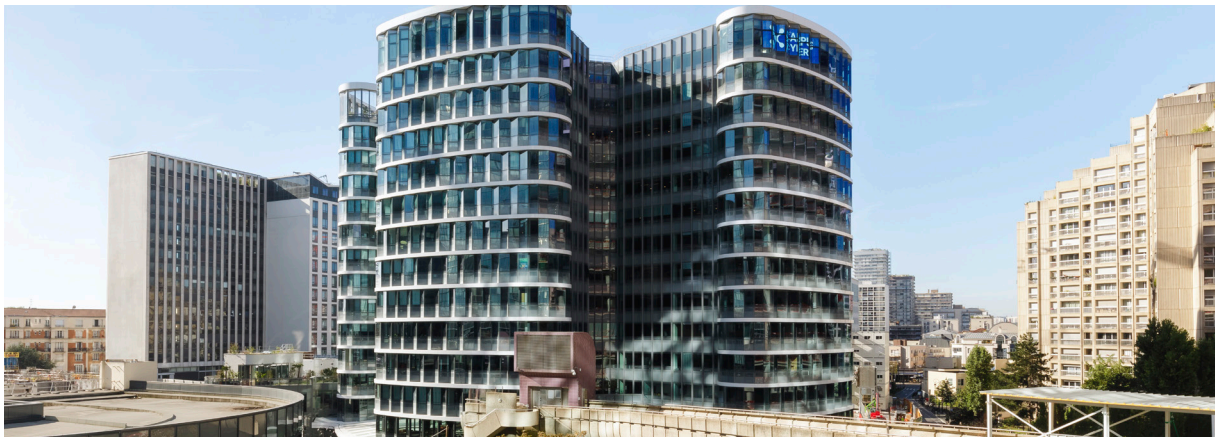
Justement, quelle est la vision que vous portez sur le secteur ?

«Au Campus Cyber, nous voyons un écosystème cyber européen riche mais encore fragmenté. Des startups innovantes, des centres de recherche reconnus et des entreprises technologiques de premier plan développent des solutions de cybersécurité parmi les plus avancées.
Pourtant, un paradoxe persiste. Les talents existent. Les technologies aussi. Mais les entreprises européennes peinent encore à atteindre la taille critique qui leur permettrait de rivaliser pleinement avec les grands acteurs internationaux.

Les cadres réglementaires, les pratiques d'achat et les dynamiques industrielles restent largement organisés à l'échelle nationale. Cette fragmentation limite les effets d'échelle et ralentit l'émergence d'acteurs capables de s'imposer sur la scène internationale.

À cela s'ajoute une difficulté d'accès aux grands donneurs d'ordre. De nombreuses entreprises, notamment les startups et PME, peinent à transformer leur capacité d'innovation en déploiement à grande échelle.

Dans un secteur où les investissements en recherche et développement sont considérables, la rapidité d'accès au marché devient un facteur décisif de compétitivité.»



Quel est le rôle que le Campus Cyber entend jouer dans ce contexte ?

«Aujourd'hui, l'enjeu n'est plus seulement d'innover, mais d'organiser concrètement les condi-tions du passage à l'échelle. C'est précisément pour répondre à ce défi que se déploie la feuille de route 2026-2028 du Campus Cyber. Le Campus Cyber n'a pas vocation à se substituer aux acteurs existants.

Il les met en capacité de travailler ensemble, de monter des projets, de tester des solutions, de se connecter au marché et d'aller plus vite.
Son rôle est d'organiser les coopérations, de connecter plus efficacement l'offre et la demande, et de faire émerger des dispositifs utiles, à la fois pour le marché et pour la résilience.**»**

Le Campus Cyber est donc un acteur au service de l'écosystème ?

«C'est exactement ça ! Le Campus rassemble les forces publiques et privées de la cybersécurité française et réunit aujourd'hui 250 entités membres, dont 190 entités résidentes, couvrant l'ensemble de la chaîne de valeur : entreprises, acteurs publics, centres de recherche, organismes de formation, startups et associations. Cet écosystème comprend notamment 110 entreprises membres, 23 organismes de formation et écoles, 5 organismes de recherche et 7 acteurs institutionnels.

Après une première phase consacrée à la structuration du lieu et de sa communauté, le Campus entre dans une nouvelle étape de son développement. Sa stratégie 2026-2028 marque un tournant : passer d'un lieu de rassemblement à un acteur structurant, capable d'organiser l'action collective et d'accélérer des projets concrets.

Cette évolution répond directement au besoin de transformer un écosystème riche en dynamique opérationnelle. Elle se traduit par un positionnement renforcé comme plateforme servicielle.

Concrètement, le Campus propose des dispositifs opérationnels pour accompagner les acteurs : mise en relation, montage de projets, accès à des terrains d'expérimentation et connexion aux marchés.**»**

Pouvez-vous nous en donner quelques exemples ?

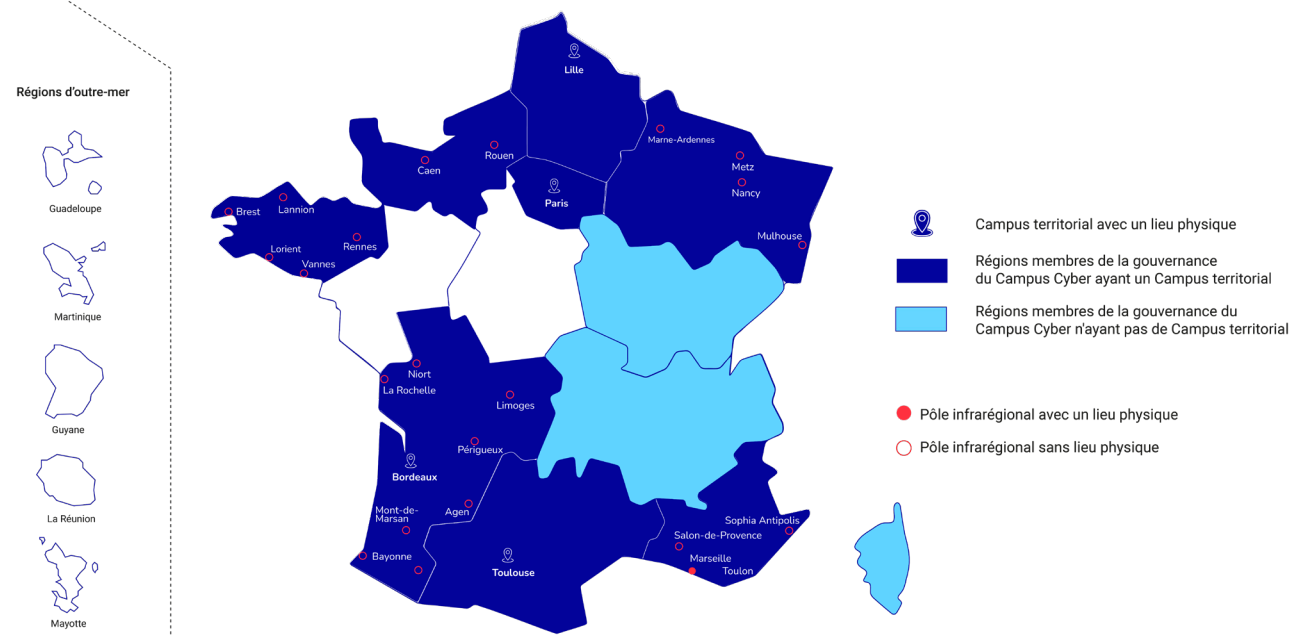
«Un premier *game changer* sera le plateau technique mutualisé. Il permettra de tester des solutions, d'expérimenter en conditions réelles et de valider des technologies avant leur déploiement. Nous préfigurons aussi une forge à croissance qui vise ainsi à accompagner les *startups* et PME cyber dans leur développement, en facilitant leur accès à des donneurs d'ordre, à des investisseurs, à des partenaires industriels et, lorsque c'est pertinent, à des partenaires européens.
Le Campus joue également un rôle clé dans la structuration de la demande, en facilitant la mise en relation entre offreurs de solutions et acheteurs, grands groupes, administrations et collectivités afin de favoriser leur déploiement à grande échelle, notamment dans un contexte de montée en puissance des exigences réglementaires liées à la directive NIS2. Cette dynamique se traduit notamment par le développement d'une plateforme de services NIS2, visant à orienter les organisations concernées, qualifier leurs besoins et fluidifier leur accès aux solutions adaptées.

Dans cette logique de structuration et de diffusion à grande échelle, le Campus Cyber s'appuie fortement sur la richesse du tissu associatif français en cybersécurité, dont les initiatives portées notamment dans le cadre de l'ACN contribuent activement à la sensibilisation, à la formation et à la diffusion des bonnes pratiques.**»**

Quand on parle de passage à l'échelle, on pense forcément à l'international et, d'abord à l'Europe ?

«En effet, et c'est une grande partie de nos activités. Nous développons une logique E2E, Ecosystem to Ecosystem qui se traduit par des coopérations concrètes avec d'autres écosystèmes cyber : partenariats, montage de projets, collaboration entre acteurs et accès au marché. Le Campus porte une ambition : créer les conditions pour que les acteurs européens collaborent et se développent. Elle ne peut toutefois se concrétiser pleinement sans un ancrage territorial fort. C'est tout le rôle du réseau des Campus Cyber territoriaux, qui permettent de déployer cette dynamique au plus près des acteurs économiques et publics, et d'en assurer la traduction opérationnelle sur l'ensemble du territoire.**»**

FOCUS PRÉSENTATION GÉNÉRALE DU RÉSEAU DES CAMPUS CYBER TERRITORIAUX



Incontournables et solidement implantés dans leurs écosystèmes régionaux, les Campus territoriaux sont encore trop souvent méconnus au niveau national quant à leur organisation en réseau, leurs missions ou leurs projets. Ce focus vise à y remédier et présenter les opportunités de collaboration avec chacun des Campus territoriaux.

Organisation du réseau

«Projet initié par l'Etat, le Campus Cyber est avant tout un maillage régional via son réseau des Campus territoriaux. Depuis 2022, onze régions métropolitaines ont rejoint la dynamique Campus (Auvergne-Rhône-Alpes, Bretagne, Bourgogne Franche-Comté, Corse, Grand Est, Hauts-de-France, Ile-de-France, Normandie, Nouvelle-Aquitaine, Occitanie et Sud). Parmi elles, huit ont décidé de créer un Campus Cyber territorial et certaines portent un projet en cours de préfiguration (le Campus Ile-de-France est le Campus Cyber national).

Le réseau des Campus territoriaux se pilote via une double gouvernance. Au niveau stratégique, le Collège des Campus territoriaux est constitué des conseillers régionaux en charge de la cyber. Il représente le réseau au sein du Conseil d'administration du Campus national et sert d'interface avec les instances politiques des régions.

Au niveau opérationnel, le réseau est porté par les directeurs et directrices des Campus qui se réunissent mensuellement pour coordonner les projets communs.»

Des Campus à la fois tous différents...

«Le réseau des Campus est par nature un réseau décentralisé et il n'existe pas un Campus similaire à un autre. Chaque région, en vertu de ses spécificités territoriales et de la maturité de sa filière cyber, est libre de créer de la manière la plus adaptée qu'il soit son propre Campus. Celui-ci est juridiquement indépendant du Campus national et dispose de ressources humaines et financières propres.

Ainsi, les Campus sont de statuts différents (association de loi de 1901, SAS ou SEM). Ils peuvent disposer d'un lieu physique unique, de pôles infrarégionaux ou encore être à 100% virtuels. Par ailleurs, chacun des Campus se spécialise dans les thématiques correspondant historiquement à son tissu socio-économique.

Le Campus Occitanie est naturellement porté sur les enjeux de l'aéronautique et du spatial alors que les Campus Bretagne, Normandie et Région Sud s'impliquent davantage dans les initiatives relatives aux enjeux maritimes et fluviaux.»

« L'objectif est de permettre l'émergence et faciliter la consolidation de champions français et européens de la cybersécurité, au service de l'agenda de souveraineté numérique européenne. »

...mais très semblables

«Par-delà les spécificités régionales, les Campus reposent sur un socle commun. Ils s'inscrivent tous dans les principes communs développés par le Manifeste du Campus Cyber, la Charte du réseau et la nouvelle feuille de route triennale du Campus national.

Encore plus. En outre des actions portées régionalement par chacun des Campus, ils ont décidé de porter des actions interrégionales qui viennent s'y superposer. C'est tout le sens de la feuille de route commune des Campus, dévoilée le 1er avril 2026 lors du Forum InCyber.»

La feuille de route commune des Campus

«Les Campus entendent répondre à une attente forte des écosystèmes cyber : pouvoir accéder facilement, partout en France, à un ensemble de ressources organisées pour répondre aux besoins de tous les acteurs publics et privés, qu'il s'agisse de protection, de sensibilisation, de formation, de recherche ou encore de marchés.

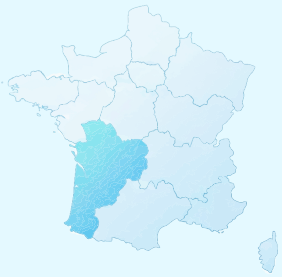
Cela s'organise autour de deux projets-phares dont les fondations seront posées en 2026 et qui seront déployés sur tout le territoire national à partir de 2027 :

• Une plateforme de services dédiée à l'accompagnement et à l'outillage des acteurs aujourd'hui les moins bien dotés et les plus vulnérables, en particulier les TPE-PME et les collectivités locales, qui, pour beaucoup, se trouveront dans le périmètre de la directive européenne NIS II, en cours de transposition en France.

• Une forge à entreprises innovantes et technologiques, d'ampleur nationale. L'objectif est de permettre l'émergence et faciliter la consolidation de champions français et européens de la cybersécurité, au service de l'agenda de souveraineté numérique européenne. Cela se fera via la création d'un parcours entrepreneurial cohérent et coordonné couvrant l'ensemble des phases de croissance des entreprises cyber.

L'objectif est de relayer efficacement la stratégie nationale cyber en région, au plus près des réalités des territoires, avec une force de frappe commune et une logique de dernier kilomètre de la cyber parcouru ensemble.»

• Campus régional de cybersécurité et de confiance numérique Nouvelle-Aquitaine



« Face à un environnement numérique instable et une cybercriminalité croissante, la Région a choisi l'anticipation et l'organisation collective. Le Campus Cyber Nouvelle-Aquitaine s'impose comme le pivot régional de la confiance numérique. Outil opérationnel au service des territoires, il protège PME, collectivités, associations et filières stratégiques. Il développe un modèle régional pour une cybersécurité au service du développement économique, de la continuité des services publics et de la souveraineté territoriale. Notre vision : l'expertise au dernier kilomètre. Face à des menaces globales, la réponse est territoriale. Nous croyons en une cybersécurité humaine, accessible et ancrée localement, capable de transformer les orientations nationales en actions concrètes. Soutenu par le Conseil régional, le Campus Cyber Nouvelle-Aquitaine est reconnu comme un modèle d'organisation territoriale de la résilience numérique, conciliant excellence technique, solidarité locale et coopération avec l'État. »

Mathieu Hazouard,
Président du Campus régional de cybersécurité et de confiance numérique Nouvelle-Aquitaine, conseiller régional de Nouvelle-Aquitaine délégué aux Enjeux Numériques

Directeur du Campus	Guy Flament	**Localisation du CCT**	Pessac
Pôles infrarégionaux	Niort, La Rochelle, Limoges, Périgueux, Agen, Mont-de-Marsan, Pau et Bayonne (en création : Poitiers, Angoulême et Tulle)	**Site internet**	campuscyber-na.fr

Le Campus Cyber Nouvelle-Aquitaine se distingue par une approche pragmatique et souveraine de la défense numérique, illustrée par des projets pionniers comme son SOC (Security Operations Center) Open Source. Ce centre de supervision, conçu pour être accessible et trans-parent, permet de mutualiser les outils de détection sans dépendre de solutions propriétaires coûteuses, offrant ainsi une alternative robuste pour les acteurs publics et les PME.

Parallèlement, le Campus mise sur l'agilité avec le programme «Star-Hack», un bug bounty pédagogique unique en son genre. Ce dispositif permet de confronter des étudiants et de jeunes talents à des environnements réels (en partenariat avec des entreprises locales) pour identifier des vulnérabilités, transformant ainsi l'apprentissage de la cybersécurité en un exercice de terrain éthique et stimulant.

Cette dynamique de protection s'accompagne d'un accompagnement stratégique majeur via son groupe de travail dédié à la directive NIS2.
Ce cercle d'experts aide les entités essentielles et importantes du territoire à anticiper les nouvelles exigences réglementaires européennes, garantis-sant ainsi que le tissu économique régional reste conforme et résilient face aux pressions cyber.

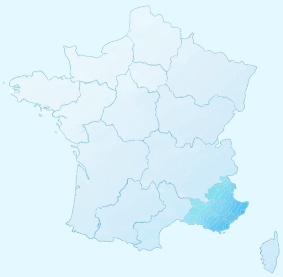
En s'appuyant sur des membres investis comme Capgemini, Cheops Technology ou des acteurs académiques, le Campus ne se contente pas de surveiller les réseaux : il bâtit une véritable culture de la sécurité partagée.
Cette synergie entre outils ouverts, détection de failles et conformité réglementaire fait de la Nouvelle-Aquitaine un laboratoire d'excellence pour la confiance numérique.

• Campus Cyber Région Sud

Référente du Campus à la Région Sud	Pauline Sintes	**Pôles infrarégionaux**	Marseille, Toulon, Sophia-Antipolis, Salon-de-Provence

Le Campus Cyber Région Sud comprend quatre pôles qui animent, au plus près des réalités du terrain, l'écosystème cyber.

• Campus Cyber.ia Euromed



« Né d'une vision d'entrepreneurs et de dirigeants, le Campus Cyber.ia Euromed est parfaitement aligné avec l'ambition du réseau national des Campus Cyber : offre servicielle d'écosystème pour l'accompagnement des entreprises et collectivités, promotion de la filière et des expertises souveraines au service de la cyber résilience du territoire. »

Pierre Boulogne
Président du Campus Cyber.ia Euromed

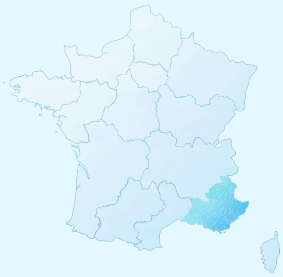
Délégué général	Clément Rossi	**Localisation du CCT**	Marseille
Site internet	www.campuscyber-regionsud.fr		

Officiellement lancé en novembre 2024, le Campus Cyber.ia Euromed accompagne et oriente les entreprises dans leur maturité cyber et le déploiement de projets IA sécurisé et souverain.

Co-fondé par 5 entreprises engagées du territoire (Aéroport Aix-Marseille, CMA-CGM, CEPAC, FDJ United, Unitel Group), et situé dans le quartier d'affaires Euroméditerranée à Marseille, il dispose de 2 000 m2 de locaux mêlant centre de gestion de crise cyber, coworking, espace événementiel modulaire et bureaux.
Véritable plateforme, physique et numérique, de mise en relation entre filière locale de cyber x IA et demande (PME, ETI, grand compte), il compte près de 40 partenaires-membres.

En 2025 ce sont près de 60 événements qui ont été organisés au Campus, dont plus de 100 participants répartis sur 9 cellules de crise pour l'exercice REMPAR25, ce qui faisait d'Euromed le 1er site national hors Campus Cyber national.

• Campus Sophia Antipolis



« Sophia Antipolis a toujours été un territoire laboratoire, un lieu où se rencontrent chercheurs, entreprises et institutions. Avec le Campus Cyber, nous franchissons une nouvelle étape essentielle : structurer, fédérer et amplifier notre écosystème pour faire émerger des solutions souveraines et compétitives en cybersécurité et intelligence artificielle. Ce campus hors les murs reflète notre manière de travailler : souple, collaboratif, profondément ancré dans l'innovation. Face à l'accélération des menaces numériques, notre responsabilité collective est d'accompagner les entreprises, de protéger les citoyens et de renforcer la résilience de tout notre territoire. »

Jean Leonetti
Président de la Communauté d'agglomération Sophia Antipolis, maire d'Antibes-Juan les Pins

Directeurs	Jean-Pierre Mascarelli (C.A.S.A.) et Bernard Kleyhoff (Région Sud)	**Localisation du CCT**	Sophia Antipolis

Le Campus Cyber Sophia Antipolis constitue l'un des piliers de la stratégie régionale Sud en matière de cybersécurité.
Ancré au cœur de la première technopole d'Europe, il s'appuie sur un écosystème unique réunissant plus de 2 700 entreprises, 5 500 chercheurs et 7 500 étudiants, dans un environnement où le numérique, l'innovation et la recherche sont profondément ancrés.

Conçu comme un campus hors les murs, il fédère les forces locales plutôt que de les centraliser, en mobilisant entreprises, laboratoires, établissements académiques et institutions publiques autour d'une ambition commune : faire de Sophia Antipolis un pôle d'excellence national et international en cybersécurité et intelligence artificielle.

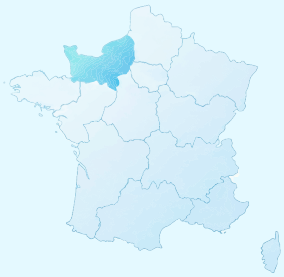
Cette spécificité repose notamment sur la présence du 3IA Côte d'Azur, du CSIRT régional, de centres de Recherche d'envergure (INRIA, EURECOM, Université Côte d'Azur…) et d'acteurs industriels majeurs (Amadeus, Kyndryl, SAP Labs, Fortinet, Orange Cyberdefense, Thales…) qui développent des technologies critiques en IA, en sécurité des données, en simulation d'attaques ou encore en détection automatisée des menaces.

À travers ses actions, le Campus Cyber accompagne la montée en compétences des entreprises – en particulier des TPE/PME – au moyen de dispositifs de sensibilisation, formation, innovation, et réponse aux incidents, tout en favorisant les coopérations entre acteurs publics et privés.

Soutenu par la CASA et le SYMISA, le campus s'inscrit dans une dynamique structurante pour le territoire : articulé avec le bâtiment Alpha (8 500 m²), il renforcera la visibilité et l'attractivité de Sophia Antipolis en facilitant le partage de données, la maîtrise du risque numérique, et la création de projets collaboratifs.

Par cette mise en réseau, Sophia Antipolis ambitionne d'être un catalyseur de solutions souveraines, compétitives et sécurisées au service des entreprises, des citoyens et des institutions.

• Campus Nomandie Cyber



« Labellisé « Campus Cyber Territorial » en mai 2024, devenant alors le 4ème Campus Cyber français, le Campus Normandie Cyber est la structure opérationnelle et le centre de ressource pour déployer la stratégie régionale « Normandie Cyber », il rassemble entreprises, acteurs de l'enseignement supérieur et de la recherche et collectivités territoriales autour d'une même ambition : faire de la Normandie une des « régions de confiance » autour de la sécurité numérique des organisations de tailles petite, moyenne et intermédiaire et, d'une manière plus générale, de tout le territoire normand. Depuis la fin 2025, il est porté par l'association Normandie Numérique. »

Stéphane Bresson,
Directeur du Campus Normandie Cyber

Directeur du Campus	Stéphane Bresson	**Localisation du CCT**	Caen, Rouen
Site internet	www.normandie-numerique.fr		

L'objectif du Campus Normandie Cyber® est de sensibiliser et d'accompagner la montée en compétences et renforcer la maturité de l'ensemble des acteurs économiques régionaux (bénéficiaires et offreurs de solutions) tout en fédérant et animant la communauté de la cybersécurité.

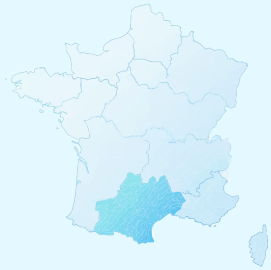
Il vise à transformer la menace liée à la cybersécurité en opportunités économiques, en développant l'écosystème cyber et le marché induit par ces enjeux. Pour répondre à ces objectifs, il développe les synergies au sein de l'écosystème régio-nal ainsi qu'avec plusieurs autres écosystèmes régionaux, nationaux, européens et internationaux. Il est le lieu fédérateur des actions d'animation, de sensibilisation et de prévention.

Le Campus Normandie Cyber® facilite la mise en relation entre l'offre et la demande, via des produits et services locaux au sein d'une place de marché. Il s'appuie sur les acteurs régionaux qui en sont à la fois les bénéficiaires et les fournis-seurs.

Avec ceux-ci, il propose plusieurs services qui constituent le socle de son offre de services : CSIRT territorial, DIH, observatoire de l'incidentologie et de la menace, plateforme d'expérimentation et d'innovation, plateforme d'animation, processus de qualification des ac-teurs et des projets, notamment.

Tout en restant généraliste, Il accompagne certains secteurs d'activité de manière plus spécifique, notamment le secteur maritime et fluvial ainsi que l'industrie.

• Cyber'Occ



« Protéger nos TPE, PME, associations et collectivités, c'est protéger l'ensemble de notre tissu économique et industriel. C'est une question de compétitivité, de survie, et Cyber'Occ a précisément été créé pour cela. En 2025, nous avons franchi des étapes décisives, qui seront poursuivies et augmentées en 2026. Notre Campus Cyber à Labège dans la Data Valley est désormais ouvert, le projet d'AMI-CMA Osmose a commencé à déployer ses actions de sensibilisation et de formation, le centre de réponse à incidents (CSIRT) joignable au 0800711313 est pleinement opérationnel. La Région Occitanie sous la présidence de Carole Delga a pris ses responsabilités en créant Cyber'Occ. Pour construire la résilience territoriale dont nous avons besoin. »

Marc Sztulman
Président de Cyber'Occ, conseiller régional d'Occitanie

Directeur du Campus	Olivier Auradou	**Localisation du CCT**	Labège
Site internet	www.cyberocc.com		

Dans un contexte de tension croissante sur les métiers de la cybersécurité, Cyber'Occ (centre régional de cybersécurité d'Occitanie), labellisé Campus Cyber territorial en novembre 2025, s'engage activement dans la structuration de la filière formation sur le territoire.

Dans le cadre du consortium OSMOSE, projet de cinq ans doté de 6 millions d'euros de soutien public et piloté par les universités de Toulouse et de Montpellier, Cyber'Occ contribue au développement d'un observatoire des compétences en cybersécurité.

Cet outil a vocation à cartographier les besoins en formation à l'échelle régionale, à identifier les tensions sur le marché de l'emploi et à produire des données utiles pour orienter les politiques de montée en compétences. En agrégeant des informations sur les profils recherchés, les niveaux de qualification disponibles et les évolutions des métiers cyber, l'observatoire permettra aux acteurs de la formation, aux entreprises et aux pou-voirs publics de disposer d'une vision partagée et actualisée de l'écosystème.

OSMOSE réunit 21 partenaires académiques, industriels et institutionnels, dont Airbus, Thales et Aumovio, et pro-pose un dispositif de formation couvrant un public allant des collégiens aux professionnels en reconversion.

Positionné au cœur de ce consortium, Cyber'Occ joue un rôle d'interface entre le monde académique et les besoins opérationnels des entreprises régionales.

Cyber'Occ s'affirme ainsi comme le point d'entrée unique de la cybersécurité en Occitanie avec l'ambition de faire du territoire une référence nationale en matière de formation et de souveraineté numérique.

• Hub Grand Est Cybersécurité

« Depuis 2023, les attaques contre nos collectivités ont bondi de 400 %. Avec le lancement du Hub Grand Est Cybersécurité, nous passons à la vitesse supérieure, pour mieux lutter ensemble contre la cybermenace. En complément de notre Centre d'Assistance Grand Est Cybersécurité, ce réseau de Pôles d'Excellence cyber territoriaux permet de sensibiliser, former et inventer de nouvelles solutions. C'est en se mobilisant ensemble que nous ferons du Grand Est un territoire numérique de confiance. »

Franck Leroy,
Président de la région Grand Est

Directeur du Campus	Kévin Sanna	**Pôles d'excellence**	Nancy, Marne-Ardennes, Mulhouse, Metz
Site internet	www.cybersecurite.grandest.fr		

Le Hub est le campus régional cybersécurité du Grand Est. S'appuyant sur des Pôles d'Excellence territoriaux disposant de spécialisations, il agit au plus près des acteurs du terrain pour fédérer formation, recherche et innovation, développer les compétences et renforcer la souveraineté numérique.

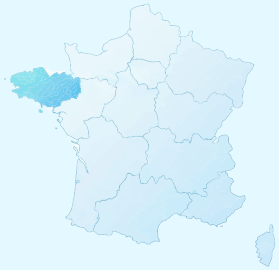
La Région Grand Est a choisi une approche unique : s'appuyer sur les forces vives locales et les expertises réparties sur les territoires pour construire une réponse régionale forte et coordonnée.

Le Hub Grand Est Cybersécurité devient ainsi un véritable lieu de convergence et d'innovation, un Hub grand et proche à la fois, où entreprises, universités, institutions et citoyens peuvent collaborer pour renforcer la cybersécurité de notre région.

Dans une région marquée par une forte densité industrielle et des territoires ruraux mais également située au carrefour de l'Europe, le Hub Grand Est favorise la coopération entre tous les acteurs à différents niveaux géographiques et d'expertise.

Une coopération qui permet de rendre la cybersécurité plus accessible, de mutualiser et d'approfondir les expertises, au service de la résilience collective face aux cybermenaces.

• Bretagne Cyber Alliance



« Avec Bretagne Cyber Alliance, la Bretagne dispose d'un outil au service des bretons qui va permettre de faire rayonner l'ensemble de son écosystème cybersécurité sur les plans nationaux et européens pour répondre aux grands enjeux actuels. »

Jérôme Tré-Hardy, Président de Bretagne Cyber Alliance, conseiller régional de Bretagne

Directeur du Campus Tiphaine Leduc **Site internet** www.cyberalliance.bzh

Le Campus Cyber breton, Bretagne Cyber Alliance est né de la volonté collective de la Région et de 5 territoires bretons (Brest Métropole, Rennes Métropole, Lannion Communauté, Lorient Agglo, Vannes Agglo) d'agir pour le développement d'une filière régionale majeure et contribuer à la protection des filières économiques comme de la société tout entière.

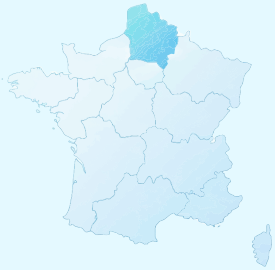
Le Campus Cyber breton, qui rassemble le tissu académique, les acteurs de la formation, les acteurs du développement économique et les entreprises, se donne comme engagements d'activer et de dynamiser la communauté cyber, de favoriser les interactions entre les différents acteurs de la filière et de faire rayonner l'écosystème cyber breton comme une référence en France et en Europe pour un monde numérique plus sûr.

Bretagne Cyber Alliance structure son action autour de 4 missions :
• Accompagner la croissance des acteurs économiques de la cybersécurité
• Conforter la performance de la recherche et de l'innovation
• Diffuser la culture de la cybersécurité dans toute la société
• Répondre aux besoins en compétences

Bretagne Cyber Alliance produit des ressources mises à disposition de la communauté des pure player cyber et des filières à sécuriser :

• Le baromètre de maturité cyber, outil clé pour mesurer, piloter et accélérer la ma-turité cyber des entreprises et collectivités. Avec 400 répondants, il est une véritable boussole au service de la sécurisation des acteurs.
• L'observatoire NIS 2 permet l'identification des cibles assujetties à NIS 2 sur le territoire régional. C'est un outil qui permet d'anticiper et d'accompagner les acteurs concernés par la directive à venir.
• La cartographie des aides mobilisables recense et synthétise les aides mobilisables au niveau européen, national et régional pour se lancer dans une démarche de sécurisation.
• L'annuaire des acteurs cyber régionaux permet d'identifier les prestataires, solutions et services qui protègent et sécurisent.
• Le catalogue des offres de formation : avec 120 établissements de formation, l'offre de formation est particulièrement variée et permet de couvrir la chaine de valeur des compétences cyber.

• Campus Cyber Hauts-de-France Lille Métropole



Directeur du Campus	Chekib Gharbi	**Localisation du CCT**	Lille
Site internet	hdf.campuscyber.fr		

Le Campus Cyber Hauts-de-France Lille Métropole s'impose aujourd'hui comme un acteur clé de la cybersécurité en région, en fédérant près de 150 entreprises dont des leaders reconnus comme Advens ou Vade-Hornetsecurity. Sa raison d'être est claire : renforcer la résilience numérique du territoire en combinant formation, innovation et accompagnement des acteurs éco-nomiques.

Ce Campus Cyber se distingue notamment par deux singularités fortes : d'une part, une offre de formation immersive reposant sur une cyber range permettant des mises en situation réalistes (CTF, gestion de crise), et d'autre part, le développement d'un écosystème entrepreneurial, avec un incubateur dédié qui soutient une trentaine de startups cyber.

Positionné à la croisée des enjeux publics et privés, il héberge le CNF Cyber du ComCyber-MI, renforçant son rôle stratégique à l'échelle natio-nale.

Parmi ses enjeux clés, ce Campus Cyber vise à accélérer l'intensité technologique des entreprises cyber régionales. Dans cette dynamique, il pilote des projets structurants comme un programme de POC cyber financé par l'EDIH, permettant aux entreprises de tester des solutions innovantes en conditions réelles.

Partenaire historique du Forum InCyber, il a également développé le Campus Cyber Summit, devenu un rendez-vous de référence pour les professionnels du secteur.
Ainsi, le Campus Cyber Hauts de France Lille Métropole incarne une plateforme unique de convergence entre expertise, innovation et développement économique au service du territoire.
Le Campus est une BU d'Euratechnology.

6.2 LES TENDANCES RÉGLEMENTAIRES

1• Europe : vers un marché unique du numérique de confiance

La transformation numérique continue de s'opérer en Europe dans un contexte géopolitique marqué par des tensions croissantes et une menace grandissante. Face à ces défis, la concrétisation d'un marché unique du numérique de confiance, applicable à l'ensemble de l'Union Européenne, s'impose comme une priorité pour l'ensemble des acteurs de la filière. Les nouveaux risques liés aux nouveaux usages du numérique poussent les institutions européennes et les Etats membres à adapter leur arsenal législatif afin de mieux maîtriser leur avenir technologique et renforcer leur autonomie stratégique.

Dans ce paysage numérique de plus en plus concurrentiel, où la Chine et les États-Unis s'affrontent pour la domination technologique, il est nécessaire que l'Europe se positionne comme un acteur résilient, innovant et incontournable à l'échelle mondiale. C'est dans cette optique que le programme « Pour une Europe Numérique » a été conçu : il vise à faire de l'Europe un acteur majeur dans le domaine numérique, à renforcer sa souveraineté technologique et à assurer sa résilience dans un contexte de tensions croissantes dans le cyberespace.

De fait, l'année 2025 a marqué un tournant décisif dans cette dynamique, avec l'entrée en vigueur concrète de plusieurs règlements phares, tels que DORA (Digital Operational Resilience Act) et REC (Résilience des Entités Critiques). En effet, la gestion des risques fournisseurs et la résilience des chaînes d'approvisionnement deviennent des priorités. Désormais, les organisations doivent évaluer leurs partenaires non seulement sur des critères techniques, mais aussi sur leur conformité aux exigences européennes et leur capacité à garantir la souveraineté des données.

L'ensemble de ces travaux sont prioritaires pour la filière de la confiance numérique. Comme l'année 2025, l'année 2026 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 des 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

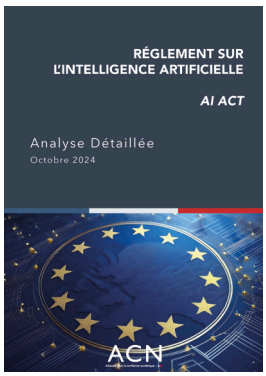
La mise en œuvre d'une identité numérique européenne interopérable

Les travaux de révision du règlement « Electronic Identification, Authentication and Trust Services » (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'Union Européenne. 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 (EUDI Wallet). Sa mise en œuvre se fera sur la base de normes techniques communes (Architecture and Reference Framework – ARF), toujours en discussion. Les Etats membres devront, dès 2027, permettre à tout citoyen européen de bénéficier gratuitement d'un portefeuille d'identité numérique.

Par ailleurs, **un projet de règlement « European Business Wallets » a été publié par la Commission européenne le 19 novembre 2025 dans le cadre de la publication du Digital Omnibus.**
Le Business wallet est une solution pensée pour alléger la charge administrative et permettre aux entreprises et aux organismes du secteur public d'identifier, d'authentifier et d'échanger des données de manière sécurisée, avec une effectivité juridique dans l'ensemble de l'Union européenne. Cette initiative sera accessible aux entreprises de toutes tailles (micro-entreprises, PME, ETI, grandes entreprises) ainsi qu'aux administrations publiques. Ce portefeuille permettra : la vérification d'identité des interlocuteurs, la création et le stockage des documents de confiance (permis, licences, certificats), la signature numérique ou encore la communication simplifiée entre entreprises et entre administrations publiques. Si les entreprises ne sont pas contraintes d'adopter ce portefeuille, la Commission souligne des gains substantiels en termes de simplification administrative, de la sécurité, de l'interopérabilité et de la croissance économique. **Après l'adoption de ce *business wallet* par le Parlement et le Conseil de l'UE, tous les échelons de l'administration des Etats membres auront deux ans pour mettre en œuvre le *business wallet*.**

La mise en place d'un cadre juridique européen pour l'intelligence artificielle

Le règlement sur l'intelligence artificielle (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 dispositions applicables concernent l'interdiction des systèmes d'IA présentant un risque inacceptable, ainsi que les obligations de transparence pour les modèles d'IA à usage général. À partir du 2 août 2026, l'ensemble des exigences organisationnelles, techniques et documentaires pour les systèmes à haut risque deviendront obligatoires. Les produits intégrant des systèmes d'IA à haut risque bénéficient d'un délai supplémentaire, avec une application reportée à août 2027. Ce calendrier progressif permet aux entreprises de s'adapter, mais il impose une accélération des programmes de conformité, en particulier pour les secteurs réglementés et les infrastructures critiques.



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

disponible en téléchargement sur :
urlr.me/SJU2sj

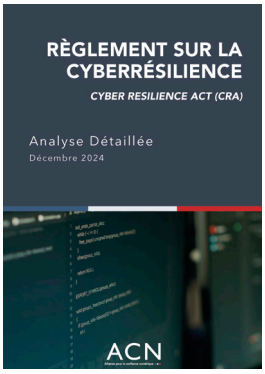
Le renforcement de la cybersécurité

Cyber Resilience Act

Le règlement sur la cyberrésilience (Cyber Resilience Act – CRA) est paru au Journal Officiel de l'Union Européenne le 20 novembre 2024 et est entré en vigueur le 10 décembre 2024. Le Cyber Resilience Act (CRA) a vocation à établir des standards communs européens de cybersécurité pour les produits qui seront mis sur le marché interne européen. Cela vise à renforcer la responsabilité des fabricants et des fournisseurs de produits comportant des éléments numériques en imposant la mise en place de garanties de cybersécurité adéquates. Ce texte concerne tous les produits comportant des éléments numériques et les services auxiliaires incluant les *hardwares* et *softwares* (quelle que soit la taille de l'entreprise fabricante). Toutefois, le texte ne s'appliquera pas si les produits n'ont pas de vocation commerciale ou s'ils sont déjà couverts par d'autres législations.

La mise en œuvre du CRA sera progressive : 18 mois après l'entrée en vigueur du CRA, les organismes d'évaluation seront habilités à vérifier la conformité des produits. À compter du 11 septembre 2026, les fabricants seront soumis à l'obligation de déclarer les vulnérabilités exploitées de leurs produits à l'ENISA. L'application intégrale du règlement est fixée à la date du 11 décembre 2027. Ainsi, 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.

A ce sujet, l'ACN multiplie les opérations d'information et de sensibilisation des acteurs de la filière afin que ces derniers puissent anticiper et préparer la mise en œuvre progressive du CRA.



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

disponible en téléchargement sur :
urlr.me/urQveD

• Organisation par l'ACN d'un webinaire sur le Cyberresilience Act – CRA en décembre 2025

Deux événements pour informer et sensibiliser nos membres sur le Cyberresilience Act
Dans le cadre de la mise en œuvre du règlement européen sur le Cyberresilience Act (CRA), l'ACN a organisé un webinaire de sensibilisation, en décembre 2025, avec la participation d'acteurs institutionnels, industriels et juridiques afin d'aborder le CRA sous différents prismes.

Cet évènement a été l'occasion pour les membres, d'être sensibilisés aux enjeux du CRA, ses obligations, sa mise en œuvre et les moyens de s'y préparer. Cela rappelle que la mise en conformité au CRA ne doit pas seulement être perçue comme une contrainte pour les entreprises mais une opportunité de se placer en tant qu'acteur de confiance au sein l'écosystème.

L'intérêt démontré des membres à cet évènement ACN a souligné l'importance de rendre le CRA accessible et intelligible pour l'ensemble des parties prenantes, et par conséquent de pérenniser la filière de la confiance numérique.

• Organisation de l'ACN Cybersecurity Certification Conference (ACCC) en février 2026

Dans le cadre de la quatrième édition de l'ACN Cybersecurity Certification Conference (ACCC), organisée par l'ACN en février 2026, nous avons eu le plaisir d'accueillir la Commission européenne, l'ANSSI et l'ENISA afin de discuter des enjeux stratégiques liés à la certification et à la normalisation, avec une attention particulière portée sur la mise en œuvre du CRA pour les entreprises de la filière.

Grâce à la qualité des interventions des institutions publiques ainsi que des experts de la filière, l'ACCC a offert un évènement riche en échanges et en recommandations opérationnelles pour la filière.
Les discussions ont notamment porté sur les différents schémas de certification européens et les manières d'anticiper les obligations du CRA.

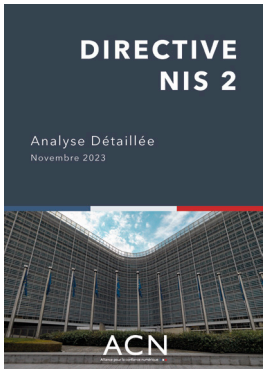
En outre, l'ACCC a permis de délivrer des pistes concrètes pour aider les entreprises de la filière à se conformer tout en renforçant leur compétitivité et leur innovation.

Cyber Solidarity Act

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.

NIS 2

La Commission européenne a publié au Journal Officiel de l'Union européenne la directive NIS 2, révision de la directive NIS, le 27 décembre 2022 et est rentrée en application le 17 janvier 2023. Les mesures mises en place par la directive NIS 2 sont destinées à assurer un niveau commun élevé de cybersécurité dans l'ensemble de l'Union européenne. Elle vise à garantir un cyberespace de confiance pour les citoyens et les entreprises et à renforcer la coopération entre les États membres. Les textes de la directive sont en cours d'examen et de transposition dans le droit national français (cf. p. 102 Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité).

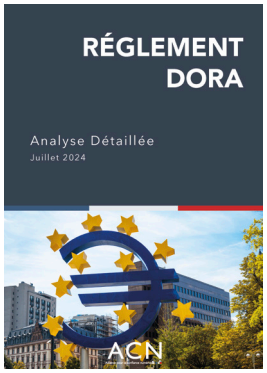


Rapport ACN « Analyse détaillée directive NIS 2 »

disponible en téléchargement sur :
urlr.me/VWAHzj

La résilience opérationnelle numérique du secteur financier

Le règlement sur la Résilience opérationnelle numérique (DORA) et la directive associée sont entrés en vigueur le 16 janvier 2023. 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.



Rapport ACN « Analyse détaillée règlement DORA »

disponible en téléchargement sur :
urlr.me/9M2Ubf

Vers une simplification et une rationalisation du cadre règlementaire – Digital Omnibus

Face à la complexité croissante de ce « millefeuille numérique », la Commission européenne a lancé le 19 novembre 2025 le package Digital Omnibus. Ce projet vise à simplifier et clarifier les règles applicables en matière d'intelligence artificielle, de données et de cybersécurité, afin de réduire les chevauchements entre les différents textes (CRA, NIS 2, DORA) et de faciliter la mise en conformité des TPE/PME.

Parmi les initiatives phares figurent la création de bacs à sable réglementaires « *regulatory sandboxes* » à l'échelle de l'UE. Ces espaces permettent aux innovateurs de tester leurs solutions dans un cadre contrôlé, sans craindre des sanctions immédiates en cas de non-conformité. Cette approche vise à encourager l'innovation tout en garantissant un niveau élevé de protection des données et de sécurité.

La Commission européenne travaille également à l'harmonisation des procédures de certification et d'audit, afin de réduire les coûts et les délais pour les entreprises. L'objectif est de transformer les contraintes réglementaires en leviers de croissance, en favorisant l'émergence de champions européens dans les domaines de l'IA de confiance, du *cloud* souverain et de la cybersécurité.

2• 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 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.

Dans le cadre d'une commission d'enquête spéciale chargée d'examiner le projet de loi, 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'ACN salue l'intégration cohérente des textes REC/NIS2/DORA dans un seul projet de loi, favorisant la lisibilité et la compréhension des exigences pour renforcer la sécurité et la résilience nationale. Elle appelle à une transposition et mise en œuvre rapides pour répondre aux enjeux de résilience collective et d'autonomie stratégique, tout en soutenant l'écosystème français de la confiance numérique. L'ACN insiste sur l'accompagnement massif (communication, formation, bonnes pratiques) des entités régulées, souvent novices en cybersécurité. Un crédit d'impôt cybersécurité et des subventions européennes ont été proposés pour l'allégement des coûts, surtout pour les TPE-PME, et éviter les risques économiques liés à l'inaction. Enfin, il a été suggéré de créer une instance associative pour suivre l'efficacité des décrets, et d'intégrer des mesures complémentaires : prise en compte du facteur humain, politique de divulgation des vulnérabilités, et encadrement législatif de l'OSINT.

La transposition de la directive NIS 2 connait un retard dû à l'instabilité politique française. La commission spéciale de l'Assemblée nationale s'est réunie début septembre 2025 lors de la session extraordinaire et a déposé le texte à l'issue de celle-ci. Celui-ci devrait être examiné en séance publique à l'Assemblée nationale au cours du premier semestre 2026, avant de poursuivre son parcours législatif et son application dans le droit français.

Parallèlement, en attendant la publication de l'ensemble des textes de transposition, l'ANSSI a publié un référentiel de cybersécurité NIS 2 intitulé « ReCyF » en mars 2026. Ce référentiel a pour objectif de préparer les entités à leur mise en conformité avec NIS 2 et plus particulièrement, à renforcer leur niveau de sécurité dans un contexte de menace cyber permanente.

La Stratégie nationale de cybersécurité 2026-2030

La Stratégie nationale de lutte cybersécurité 2026–2030 a été présentée le 29 janvier 2026 par Anne Le Hénanff, ministre déléguée chargée de l'Intelligence artificielle et du Numérique et repose sur cinq piliers structurants, déclinés en quatorze objectifs stratégiques.

Le premier pilier « faire de la France le plus grand vivier de talents cyber d'Europe » vise à développer le tissu métiers et talents de la cybersécurité en France. Il s'agit d'investir massivement pour orienter vers ces métiers dès le plus jeune âge et soutenir les plans de formation et d'attractivité en ce domaine.

Le deuxième pilier « renforcer la résilience cyber de la nation » se concentre sur l'élévation du niveau global de cybersécurité de l'ensemble des acteurs économiques et sociaux. Ce plan reposera sur une synergie renforcée entre l'Etat, les collectivités territoriales, les entreprises, les acteurs de la recherche et de la société civile.

Le troisième pilier « entraver l'expansion de la cybermenace » est dédié à la lutte contre la cybercriminalité, avec un renforcement des moyens de l'ANSSI, de la police et de la justice spécialisées et une place centrale est dédiée au Centre de coordination des risques cyber (C4) pour mobiliser des leviers de réponse aux cyberattaques, en collaboration avec l'ensemble des acteurs étatiques. Les mesures de protection contre les cyber-attaques seront établies en collaboration étroite avec les acteurs privés.

Le quatrième pilier « garder la maîtrise de la sécurité de nos fondements numériques » a pour objectif de réduire les dépendances technologiques, en soutenant la consolidation et l'élévation de la filière cyber. Ce pan reposera sur la poursuite des investissements de l'Etat en matière de cybersécurité dans le cadre du plan France 2030 et sur un dialogue renforcé entre les parties prenantes.

Le cinquième pilier « soutenir la sécurité et la stabilité du cyberespace en Europe et à l'international » vise à développer une cyberdéfense européenne et internationale dans trois cercles d'action : l'UE, l'OTAN et au-delà des organisations en développant des coopérations avec des partenaires partageant des intérêts communs en cyberdéfense.

Publication du SGDSN « Stratégie nationale de cybersécurité 2026-2030 »

disponible en téléchargement sur :
urlr.me/mnAY3q

La Stratégie nationale de lutte contre les manipulations de l'information 2026-2030

La Stratégie nationale de lutte informationnelle, publiée en février 2026 par le Secrétariat Général de la Défense et de la Sécurité Nationale, s'articule autour de quatre piliers, qui se déclinent en quinze objectifs stratégiques.

Le premier pilier « Mobiliser la Nation pour renforcer la résilience » a pour objectifs de former et sensibiliser la société française avec la volonté de développer une culture collective de vigilance contre les manipulations de l'information. Ces thématiques seront intégrées dans les parcours scolaires et au cours des journées de citoyenneté (JDC, Service civique). Aussi, l'Académie de la lutte contre la manipulation de l'information (LMI) sera créée, placée sous l'égide de VIGINUM.

Le second pilier « Réguler les plateformes en ligne et les services d'intelligence artificielle générative » est dédié au renforcement de la régulation des plateformes numériques et de l'IA générative afin de limiter les risques systémiques de manipulation, avec une mise en œuvre rigoureuse du règlement européen Digital Services Act DAS.

Le troisième pilier « Renforcer la capacité nationale opérationnelle de lutte contre les ingérences numériques étrangères » vise à améliorer la capacité opérationnelle de l'Etat pour détecter et contrer les ingérences numériques étrangères, en consolidant un dispositif permanent de veille (COLMI) et en structurant une doctrine interministérielle de réponse. Une attention particulière est portée au renforcement des capacités judiciaires, notamment lors des périodes électorales, afin de garantir une réaction rapide aux tentatives de manipulation. L'objectif douze de ce pilier soulève spécifiquement l'accompagnement de l'émergence d'une filière souveraine de renseignement en source ouverte (OSINT). L'idée est de combiner un écosystème d'outils, de compétences et de coopération public-privé, tout en soutenant la communauté indépendante des analystes.

Le quatrième pilier « Assurer l'existence d'un espace informationnel libre, ouvert et sécurisé dans une approche multilatérale » a pour ambition de construire une coopération internationale pour garantir un espace informationnel sécurisé. Il prévoit la structuration d'une communauté européenne de lutte contre les manipulations et un soutien aux Etats et aux zones vulnérables.

Publication du SGDSN « Stratégie nationale de lutte contre les manipulations de l'information 2026-20230 »

disponible en téléchargement sur :
urlr.me/UGbunw

FOCUS

L'INDICE DE RESILIENCE NUMERIQUE : UN OUTIL POUR MESURER SES DEPENDANCES NUMERIQUES

La résilience numérique : un enjeu stratégique pour les organisations

La transformation numérique s'accompagne d'une dépendance croissante aux technologies, aux fournisseurs et aux infrastructures.

Cette évolution se traduit par une perte progressive de maîtrise sur les systèmes d'information, une complexité accrue et des interdépendances de plus en plus difficiles à appréhender : une part significative et croissante des dépenses numériques européennes est orientée vers des technologies extra-européennes (265 Md€ en 2025).

Dans le même temps, moins de 10% des organisations mesurent objectivement leurs dépendances technologiques, alors même que celles-ci conditionnent leur capacité à maîtriser leurs risques, leurs coûts et leur autonomie stratégique.

Dans ce contexte, la résilience numérique devient un enjeu central, à la croisée de la souveraineté, de la performance et de la continuité d'activité.

L'Indice de Résilience Numérique : une démarche structurante

L'Indice de Résilience Numérique (IRN) a été conçu pour répondre à ce besoin de visibilité et de pilotage. Il s'agit d'un référentiel commun permettant de mesurer et d'objectiver les dépendances numériques des organisations, à partir de leurs systèmes et processus critiques.

La démarche repose sur plusieurs étapes clés :

- **Identifier** les processus les plus critiques des organisations
- **Mesurer** les dépendances à travers l'analyse des applications et des actifs technologiques de ces processus
- **Révéler** les zones de fragilité via une cartographie des dépendances
- **Décider** en objectivant les arbitrages stratégiques
- **Transformer** en mettant en œuvre des plans de remédiation et d'évolution du système d'information

L'IRN propose une approche *full stack*, couvrant l'ensemble des dimensions de la résilience (technologique, opérationnelle, data, cyber, juridique, supply chain, etc.), et s'appuie sur un standard ouvert, partageable et comparable entre organisations.

Il a vocation à s'articuler avec les démarches existantes de gestion des risques et de conformité (telles que NIS2, DORA ou les référentiels ISO), en les complétant par une approche centrée sur l'analyse des dépendances numériques et leur pilotage dans une logique stratégique.

Portée par un écosystème d'acteurs publics et privés, la démarche vise à faire émerger un langage commun et un cadre de référence pour piloter la résilience numérique à l'échelle des entreprises et des secteurs.

Un accompagnement structuré des organisations

Le déploiement de l'IRN repose sur un écosystème d'acteurs organisé autour de l'association aDRI, qui agit comme tiers pour garantir la robustesse méthodologique du référentiel, sa neutralité et sa diffusion à large échelle :

- Des entreprises accréditées qui valident la capacité des entreprises agréées à réaliser leurs missions,
- Des entreprises agréées qui conduisent les diagnostics et peuvent labelliser le niveau de résilience numérique des entreprises utilisatrices

Dans ce cadre, un modèle d'accompagnement structuré est mis en place. Les organisations peuvent s'approprier le référentiel de manière autonome ou être accompagnées par des acteurs accrédités, habilités à conduire les diagnostics et à accompagner les démarches de labellisation.

Ce dispositif vise à créer un marché de compétences qualifiées autour de la résilience numérique, fondé sur un standard commun, ouvert et partagé. Il permet également d'assurer une homogénéité des pratiques, une comparabilité des résultats et une montée en maturité progressive des organisations, quels que soient leur taille ou leur secteur.

L'IRN s'inscrit ainsi dans une logique d'intérêt général : au-delà d'un outil de diagnostic, il constitue un langage commun entre directions générales, directions IT et fonctions risques, et un levier pour piloter le système d'information comme un actif stratégique :

- **Mise à disposition** du référentiel et des méthodes d'évaluation pour permettre à chaque entreprise d'effectuer son auto-évaluation,

- **Accréditation et labellisation** – S2 2026

Le déploiement de l'IRN dans les entreprises se fera au travers d'un réseau d'entreprises accréditées et agréés :

  - Les entreprises accréditées (par l'aDRI) agréent les entreprises qui pourront intervenir sur l'IRN auprès de leurs clients,
  - Les entreprises agréées conduisent les diagnostics et peuvent labelliser le niveau de résilience numérique des entreprises utilisatrices,

- **Communication et promotion** du label IRN.

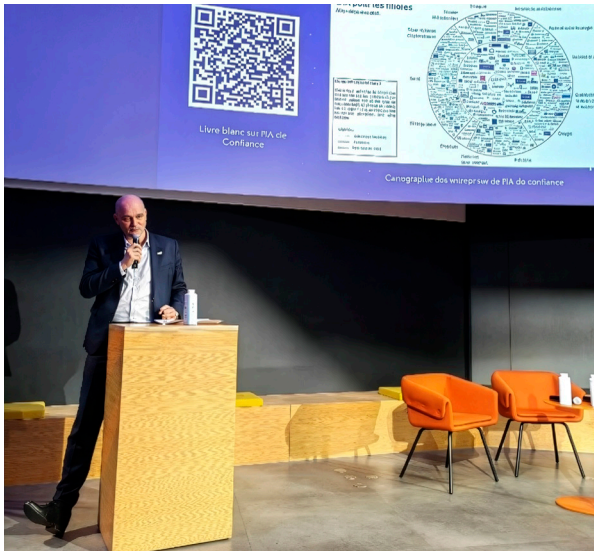
« La démarche IRN a vocation à s'appuyer sur un écosystème d'acteurs certifiés, capables d'accompagner les organisations dans l'analyse de leurs dépendances et la mise en œuvre de leur trajectoire de résilience. (...) Docaposte fera partie des entreprises habilitées à délivrer ces accompagnements.»

FOCUS

ACTIONS DANS LE CADRE DU SOMMET DE L'IA – FÉVRIER 2025

Le Sommet mondial de l'IA, organisé à New Delhi du 10 au 12 février 2026 sous la présidence conjointe de l'Inde et de la France, a réuni plus de 120 pays, ainsi que des milliers d'acteurs industriels, universitaires et représentants de la société civile. L'objectif était de promouvoir une IA utile adaptée aux contextes locaux, au service de l'intérêt public et de l'atteinte des Objectifs de développement durable. Ce sommet a également permis de faire le point sur l'avancée des actions engagées lors d'édition précédente du sommet, organisé à Paris en février 2025, où les bases d'une gouvernance mondiale de l'IA de confiance avaient été posées.
Dans ce cadre, la seconde édition des Rencontres de l'IA de Confiance (RIAC) s'est tenue le 27 janvier 2026, au Campus Cyber, et a été labellisée dans le cadre du sommet mondial de l'IA à New Delhi « IA Impact Summit ».

Anne Le Hénanff - Ministre déléguée chargée de l'Intelligence artificielle et du Numérique



Grégory Wintrebert
Président de l'ACN

Guillaume Poupard
Co-Président du Conseil national de l'IA et du Numérique

Cet évènement a réuni des acteurs publics, privés et institutionnels pour discuter ensemble de la notion de confiance dans les enjeux liés à l'IA. A cette occasion, Anne Le Hénanff, ministre déléguée chargée de l'Intelligence artificielle et du Numérique, a réaffirmé l'engagement du gouvernement en faveur d'une IA de confiance, soulignant son rôle clé dans l'innovation et la compétitivité de la France. Parallèlement, Madame la ministre a rappelé le rôle primordial de l'ACN dans la représentation et la structuration de cette filière.

L'évènement avait pour objectif d'explorer le rôle des institutions dans la mise en œuvre d'une IA fiable et les leviers économiques pour développer un tissu industriel robuste de l'IA de confiance. Ce fut l'occasion de croiser les regards d'acteurs étatiques (ANSSI, DGE, CNIL), industriels (Docaposte, Safran. AI, ...) et universitaires autour de deux tables rondes et des cas d'usage concrets ont illustré l'application opérationnelle de l'IA de confiance dans l'industrie.

Les échanges ont confirmé que l'IA de confiance est un enjeu stratégique pour la France et l'Europe en tant que levier d'innovation et de croissance économique.

Livre blanc ACN « L'intelligence artificielle de confiance »

disponible en téléchargement sur :
urlr.me/Kr6S4J

Publication par l'ACN du livre blanc sur la Blockchain

En mai 2026, l'ACN a publié un livre blanc sur la blockchain s'adressant au grand public. Ce livrable a pour objectif de mettre en valeur la présence de la blockchain et les marchés dans lesquels elle se place. Ce livre blanc explore la blockchain comme pilier stratégique pour l'économie numérique en analysant les enjeux stratégiques, économiques et opérationnels liés à la technologie de la blockchain. Il dresse : le panorama des marchés blockchain, les défis de souveraineté numérique pour la France et l'Europe ainsi que les cas d'usage concrets de la blockchain.

Livre blanc ACN « La Blockchain »

disponible en téléchargement sur :
www.confiance-numerique.fr/publications/

Publication par l'ACN d'un livrable sur la cartographie des normes de sécurité

En mai 2026, la commission NORSEC du CSF IS, instance de discussion sur les sujets de normalisation et qui prend place au sein de l'ACN, a entrepris l'écriture d'un livrable avec l'objectif de cartographier : les enjeux de la normalisation, les différentes instances de normalisation et les normes associées à chacune d'elles dans le domaine de la sécurité.

Le livrable « Panorama des normes de sécurité-sûreté » s'adresse aux utilisateurs quotidiens des normes, aux pouvoirs publics et aux acteurs économiques avec l'objectif de promouvoir la normalisation pour ses caractéristiques et atouts stratégiques. Il s'agit de soutenir la résilience collective, dans l'optique de créer un environnement plus sûr, plus souverain et plus résilient.

Livrable ACN « Panorama des normes de sécurité-sûreté »

disponible en téléchargement sur :
www.confiance-numerique.fr/publications/

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.

1• Les innovations électroniques et numériques qui génèrent de nouveaux marchés

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

• **Les systèmes et composants électroniques sont marqués par la miniaturisation couplée à la baisse des coûts.** Cette tendance, incarnée par la loi de Moore, a marqué très fortement l'économie mondiale ces 50 dernières années et devrait se poursuivre à minima sur la décennie à venir avec le développement des mémoires 3D multicouches et la miniaturisation des processeurs. Cependant, cette tendance touche à sa fin. Les investissements pour continuer la loi de Moore et se maintenir dans la course à l'innovation croissent de façon exponentielle et atteignent déjà des niveaux tels que seulement sept entreprises se maintiennent au niveau mondial : Samsung (Corée du Sud), TSMC (Taïwan) et Intel (États-Unis) dans les processeurs et Samsung (Corée du Sud), SK Hynix (Corée du Sud), Micron (États-Unis), Western Digital (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 2030.

À cet égard, l'offre NumSpot, née de la collaboration entre Docaposte, la Banque des Territoires, Dassault Systèmes et Bouygues Telecom, vise à établir une offre de cloud indépendant et souverain en France. S'appuyant sur l'infrastructure IaaS d'Outscale (filiale de Dassault Systèmes), premier fournisseur à avoir obtenu la qualification SecNumCloud au niveau IaaS, NumSpot a commercialisé sa plateforme de services au premier trimestre 2025 et a engagé en parallèle son propre processus de qualification SecNumCloud, ciblant l'horizon du premier trimestre 2026.

L'écosystème du cloud souverain français s'est significativement étoffé en 2025 : fin 2025, l'offre PREMI3NS de la société S3NS – détenue à 95 % par Thales et à 5 % par Google et opérant sur la technologie Google Cloud Platform – a obtenu la qualification SecNumCloud, illustrant la possibilité d'associer performance d'un hyperscaler et cadre de confiance souverain. D'autres acteurs sont en cours de qualification, dont Bleu, Scaleway et OVHcloud.
Sur le volet adoption, la doctrine gouvernementale « *Cloud* au centre », qui impose le recours au *cloud* pour tout nouveau projet numérique de l'État, a généré 84 millions d'euros de commandes en 2025, en hausse de 62 % par rapport à 2024, dont 70 % dirigés vers des fournisseurs européens – confirmant l'accélération et la montée en maturité du cloud souverain français. Le marché SecNumCloud reste encore modeste à l'échelle nationale (estimé à 18 millions d'euros), mais son potentiel européen est évalué à 600 millions d'euros, témoignant de l'enjeu industriel de long terme de cette filière.

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 ont pris le relais depuis septembre 2025 : APTITUDE, coordonné par l'Agence France Titres et réunissant 117 partenaires de 11 pays européens, qui expérimente des cas d'usage liés au voyage et au paiement (titre de transport numérique, carte grise, authentification forte) ; et WEBUILD, centré sur les usages liés aux personnes morales, notamment la gestion d'attestations d'identité d'entreprises et l'interopérabilité avec les registres nationaux dans une logique de KYC simplifié.

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.

Authentification sans mot de passe — Passkeys et standard FIDO2. La sécurité des mots de passe constitue depuis des décennies le maillon faible de la chaîne de confiance numérique. Le standard FIDO2, développé par la FIDO Alliance avec l'appui d'Apple, Google et Microsoft, marque une rupture technologique en proposant une authentification fondée sur la cryptographie asymétrique et les capacités matérielles des terminaux (biométrie, module de sécurité intégré, clé matérielle externe). Concrètement, lors de l'enrôlement, l'appareil génère une paire de clés cryptographiques : la clé publique est transmise au service, la clé privée ne quitte jamais l'appareil de l'utilisateur. Il en résulte une authentification résistante au phishing, à la compromission de serveur et aux attaques par rejeu – là où les mots de passe et même les OTP par SMS restent vulnérables. Les passkeys connaissent une adoption accélérée en 2025-2026, soutenue par leur support natif dans les principaux systèmes d'exploitation et navigateurs. Sur le plan réglementaire, FIDO2 est reconnu comme méthode d'authentification conforme aux exigences du RGPD, de NIS2 et de la DSP2. La feuille de route de la Commission européenne prévoit d'achever la migration des cas d'usage critiques vers des mécanismes résistants au phishing d'ici 2030. Des acteurs français et européens tels que Thales participent à cet écosystème à travers leurs solutions de gestion des identités et d'authentification forte.

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

En décembre 2023, le président de la République a créé sept «agences de programmes» dans la recherche publique française, dans le but de coordonner la recherche nationale autour de grandes priorités stratégiques, dans le cadre notamment de France 2030. Ces agences de programmes visent à réduire la fragmentation du système français de recherche et à améliorer la capacité de l'État à orienter les efforts scientifiques vers des enjeux économiques, environnementaux ou technologiques estimés majeurs par lui. Les agences constituent ainsi une nouvelle mission confiée aux organismes nationaux de recherche.

Pour favoriser la coopération entre organismes, universités, laboratoires et acteurs économiques, les agences cherchent à orienter davantage la recherche publique vers les grands défis économiques, sanitaires, environnementaux et technologiques. Elles doivent donc devenir un instrument de pilotage stratégique de la recherche française. Aussi :

- **elles identifient les priorités scientifiques et technologiques nationales** dans chacun des grands domaines de leurs programmes (actions de prospective) ;

- **elles conçoivent des actions de recherche et de transfert** (techno, connaissance) sur la base de ces priorités et tentent d'en obtenir le financement par l'État ;

- **elles pilotent ces programmes s'ils sont lancés**

- **elles fédèrent le monde académique** (universités, écoles, ONR) autour de ces programmes, améliorant ainsi la coordination entre les acteurs du système scientifique français ;

- **elles ont aussi un rôle de promotion des actions françaises** en Europe et plus généralement à l'international.

À titre d'exemple, en 2025, plusieurs nouvelles actions de recherche ont été conçues par les Agences sus-citées et financées par l'État : Camelia autour du composant pour l'IA (commun aux 2 agences), Phoenix sur la conception de composants et initiative Packaging (agence ASIC), évaluation de l'IA, Engineering Digital Twins et AI for scientists publication knowledge (agence du numérique).

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 attaques ciblent aujourd'hui toute la «pile» des applications aux composants matériels (y compris avec des attaques logicielles, type Spectre), en passant par les couches basses du système d'exploitation »

Dans le domaine de la cybersécurité, un programme de recherche (PEPR, relevant à présent des deux programmes évoqués ci-dessus et copiloté avec le CNRS) avait été lancé dès 2022 et se conclura en 2029. Le temps est ainsi venu de la réflexion pour réévaluer les enjeux et les priorités qui pourront mener, le cas échéant, à poursuivre certains travaux ou à en soutenir de nouveaux.

Cette réflexion est multi-formes, mais nous pouvons évoquer ici un travail effectué par les différents programmes des agences, conformément à leur mission de prospective, sur la base de la «Revue nationale stratégique» publiée en juillet 2025 et dans un cadre fixé par l'État.

En matière de cybersécurité, la transformation numérique des infrastructures critiques nous expose collectivement à des menaces qui ne se limitent plus aujourd'hui à l'exploitation de vulnérabilités logicielles. Les attaques ciblent aujourd'hui toute la «pile», des applications aux composants matériels (y compris avec des attaques logicielles, type Spectre), en passant par les couches basses du système d'exploitation.

Face à ce constat, limiter les solutions de sécurité au matériel ou au logiciel est certainement contre-productif : un SI basé sur un système d'exploitation sécurisé déployé sur une plateforme hardware compromise tout comme un SI basé sur une plateforme matérielle sécurisée mais pilotée par un système d'exploitation vulnérable, resteraient exposés à des attaques.

Une vision intégrée logiciel/matériel nous semble donc nécessaire.
C'est pourquoi les programmes cybersécurité des agences ont proposé de bâtir un environnement informatique complet et vérifiable, de la micro-architecture matérielle à l'espace utilisateur, en s'intéressant :

- **à l'évaluation de la sécurité matérielle** : identifier, mesurer et documenter les surfaces d'attaque présentes dans les composants hardware (processeurs, microcontrôleurs, mémoires, interfaces de communication, etc.)

- **au développement d'un OS aux propriétés de sécurité formellement définies**, vérifiables et ancrées dès le démarrage dans les garanties offertes par le matériel évalué sous-jacent.

Ce projet vise à engendrer une dynamique qui ne peut être à terme qu'européenne, pour réduire la dépendance aux solutions propriétaires opaques et donc retrouver notre souveraineté numérique, tout en augmentant notre résilience.

2• Les innovations propres à la filière qui génèrent de nouveaux produits

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

1. Cryptographie

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

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

La dynamique française en matière de cryptographie post-quantique s'accélère sous l'impulsion réglementaire et institutionnelle. L'ANSSI a annoncé qu'à partir de 2027 elle n'acceptera plus en entrée de qualification des produits de sécurité n'intégrant pas de cryptographie post-quantique, et qu'il ne sera plus raisonnable d'acquérir des produits sans cryptogaphie post-quantique après 2030. Ces jalons s'inscrivent dans une feuille de route européenne commune, adoptée par les États membres en juin 2025, qui fixe le début de la transition d'ici fin 2026 et la protection des infrastructures critiques au plus tard fin 2030. Sur le plan des premières réalisations concrètes, l'ANSSI a émis en octobre 2025 ses deux premiers visas de sécurité pour des solutions intégrant des algorithmes de cryptographie post-quantique : la carte à puce MultiApp 5.2 Premium de Thales et le microcontrôleur S3SSE2A de Samsung, tous deux exploitant le schéma de signature ML-DSA et évalués par le CEA-Leti, premier centre agréé pour la portée cryptographie post-quantique. Ces premières certifications concrétisent la disponibilité d'une offre de produits de confiance intégrant la cryptographie post-quantique sur le marché français.
En parallèle, l'écosystème des centres d'évaluation se renforce : le laboratoire CESTI d'Almond (Amossys) est en cours d'agrément pour cette portée, aux côtés de Quarkslab, Synacktiv et Thales/CNES.

Au-delà de l'évaluation de produits, des acteurs comme Almond accompagnent d'ores et déjà les éditeurs et organisations dans leur transition vers la cryptographie post-quantique. Cette activité comprend: inventaire des actifs cryptographiques, audit des algorithmes en place, définition de plans de migration et mise en œuvre d'architectures hybrides combinant algorithmes classiques et post-quantiques.

• **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.

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* est désormais bien avancé : l'e-UICC s'est largement imposé dans les smartphones, les wearables, les laptops et le secteur automobile, porté par l'adoption massive de l'eSIM.

La prochaine frontière est celle de l'iSIM (integrated SIM, ou i-UICC), qui intègre la fonctionnalité SIM directement dans le chipset de l'appareil, supprimant ainsi tout composant distinct. Les premières architectures iSIM sont en phase de déploiement précoce – notamment dans les smartphones haut de gamme et les applications automobiles, avec une validation conjointe Qualcomm-Thales sur Snapdragon 8 Gen 3 –, mais le déploiement de masse reste à venir. En parallèle, le nouveau standard GSMA SGP.32, qui vise à unifier les approches M2M et grand public pour l'IoT, est en début de déploiement en 2026 et devrait accélérer l'adoption de l'eSIM

dans les flottes industrielles et les environnements contraints.

Thales et IDEMIA demeurent parmi les leaders mondiaux de cet écosystème, aux côtés de Giesecke+Devrient et STMicroelectronics. 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.

• Sécurité des applications et certification cyber (Security By Design).
La multiplication des cyberattaques exploitant des vulnérabilités logicielles, couplée aux exigences croissantes des réglementations européennes – au premier rang desquelles le Cyber Resilience Act, qui impose des exigences de sécurité dès la conception pour tous les produits numériques commercialisés dans l'UE – confère une importance stratégique croissante à la sécurisation des applications et des logiciels dès leur phase de développement (Security By Design). Ce principe, qui consiste à intégrer les exigences de sécurité dès la conception d'un produit plutôt que de les ajouter a posteriori, devient un impératif industriel et réglementaire.

La certification de produits constitue le pilier de cette dynamique. En France, le système de certification s'articule autour de plusieurs schémas encadrés par l'ANSSI : la Certification de Sécurité de Premier Niveau (CSPN), les Critères Communs (CC) pour les évaluations approfondies, et désormais le nouveau schéma européen EUCC (Common criteria based European Cybersecurity Certification scheme), adopté par la Commission européenne en janvier 2024 dans le cadre du Cybersecurity Act. L'EUCC a vocation à remplacer progressivement les schémas nationaux et à devenir le standard de certification cyber unifié à l'échelle de l'UE – permettant à un certificat délivré en France d'être reconnu dans l'ensemble des États membres.

La France est particulièrement bien positionnée pour tirer parti de cette dynamique de certification européenne. Almond a lancé en octobre 2024 son Security Evaluation & Analysis Lab (SEAL), laboratoire technique cyber regroupant les compétences d'analyse de son pôle expertise et celles du CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information) opéré par Amossys, agréé par l'ANSSI depuis 2011. En octobre 2025, le SEAL a obtenu l'agrément EUCC aux niveaux Substantiel et Élevé, faisant d'Almond l'un des deux seuls laboratoires français habilités à évaluer et certifier des logiciels et équipements réseaux selon les standards les plus stricts : CSPN, Critères Communs et EUCC. Au-delà de la certification, le SEAL mène des analyses offensives avancées, accompagne les éditeurs dans une approche Security By Design dès la phase de développement, et participe à la transition vers la cryptographie post-quantique. Son ambition affichée est de constituer un laboratoire de dimension européenne, accessible également aux PME et start-ups du monde de l'édition logicielle, dans un contexte où les obligations réglementaires européennes créent une demande structurelle forte en expertise de certification.

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.

Livre blanc ACN « La Blockchain »

disponible en téléchargement sur : www.confiance-numerique.fr/publications/

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

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

5.Plateformes d'*Open Hardware/Software* pour l'*edge computing* et les IoTs.
Le partage de code logiciel (*Open Software*) est déjà pratiqué depuis un certain temps, mais depuis quelques années, la tendance porte sur le développement du partage du *design* de composants électroniques (*Open Hardware*). Les logiciels et les matériels en mode *open source* accélèrent l'innovation en permettant aux développeurs et aux concepteurs de partager et de réutiliser les développements réalisés par d'autres.

La re-publication en *open source* des nouveaux développements alimente le processus d'innovation et bénéficie à toute la communauté. Les atouts de la France dans ce domaine de l'*open source* sont nombreux. Le marché national est très développé, il représente le quart du marché européen.

La communauté tant des chercheurs que des développeurs est sans conteste la plus nombreuse et la plus avancée. Cependant, la sécurité est peu présente dans le monde *open source*. Le marché de la sécurité est encore dominé par les grands éditeurs de logiciels propriétaires, nord-américains pour la plupart. Une politique d'achat volontariste et l'incitation au développement de briques technologiques et de plates-formes certifiées et orientées vers l'*open source* contribueraient au renforcement de ce domaine, en particulier pour les applications innovantes associées à l'*edge computing* ou aux IoTs pour lesquels la domination américaine ne se fait pas encore trop ressentir.

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

7. *Open Source Intelligence* (OSINT).
L'OSINT existe depuis des dizaines d'années sous une forme embryonnaire (sources humaines, documentation, bibliographie…).

C'est avec l'explosion du nombre de données ouvertes disponibles en ligne depuis le début des années 2010 que le marché de l'OSINT se développe réellement, au travers du développement d'outils informatiques permettant la collecte et l'exploitation de ces données.

Ces données proviennent de différentes sources : réseaux sociaux, sites internet, médias, imageries géospatiales, forum, appareils de mesure, etc., lesquelles représentent une mine d'or d'information exploitable à des fins, 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. Architecture Zero Trust.
Face à la généralisation du *cloud* hybride, du télétravail et de l'éclatement des périmètres de sécurité traditionnels, le modèle Zero Trust s'est imposé comme le paradigme de référence en matière d'architecture de sécurité. Son principe fondateur – « ne jamais faire confiance, toujours vérifier » – implique une authentification continue de chaque utilisateur, appareil et flux, indépendamment de leur localisation dans ou hors du réseau. Ce modèle est désormais étroitement articulé à la mise en conformité réglementaire : la directive européenne NIS2, transposée en France et applicable à plus de 15 000 entités françaises dans les secteurs critiques (énergie, transports, santé, numérique, etc.), pousse de facto les organisations à adopter des architectures Zero Trust pour répondre à ses exigences de gestion des risques, de contrôle des accès et de surveillance continue. L'écosystème français dispose d'acteurs bien positionnés sur ce marché souverain, avec des solutions certifiées par l'ANSSI : Stormshield (segmentation réseau), Wallix (gestion des accès à privilèges), Sekoia.io et HarfangLab (détection et réponse aux menaces). L'ANSSI a publié en 2025 un guide dédié à la mise en œuvre du Zero Trust dans les administrations, faisant de cette architecture une recommandation institutionnelle.

9. 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…**

3• 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 2 572 entreprises réalisant en France 22,4 Milliards d'euros de chiffre d'affaires dans ce secteur en forte croissance (7,4% de croissance annuelle moyenne depuis 2016).

Les 95 membres de l'Alliance pour la confiance numérique (ACN), dont 80% 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

OTENTIK AIGCEV

BRETAGNE Next

cea

cnrs

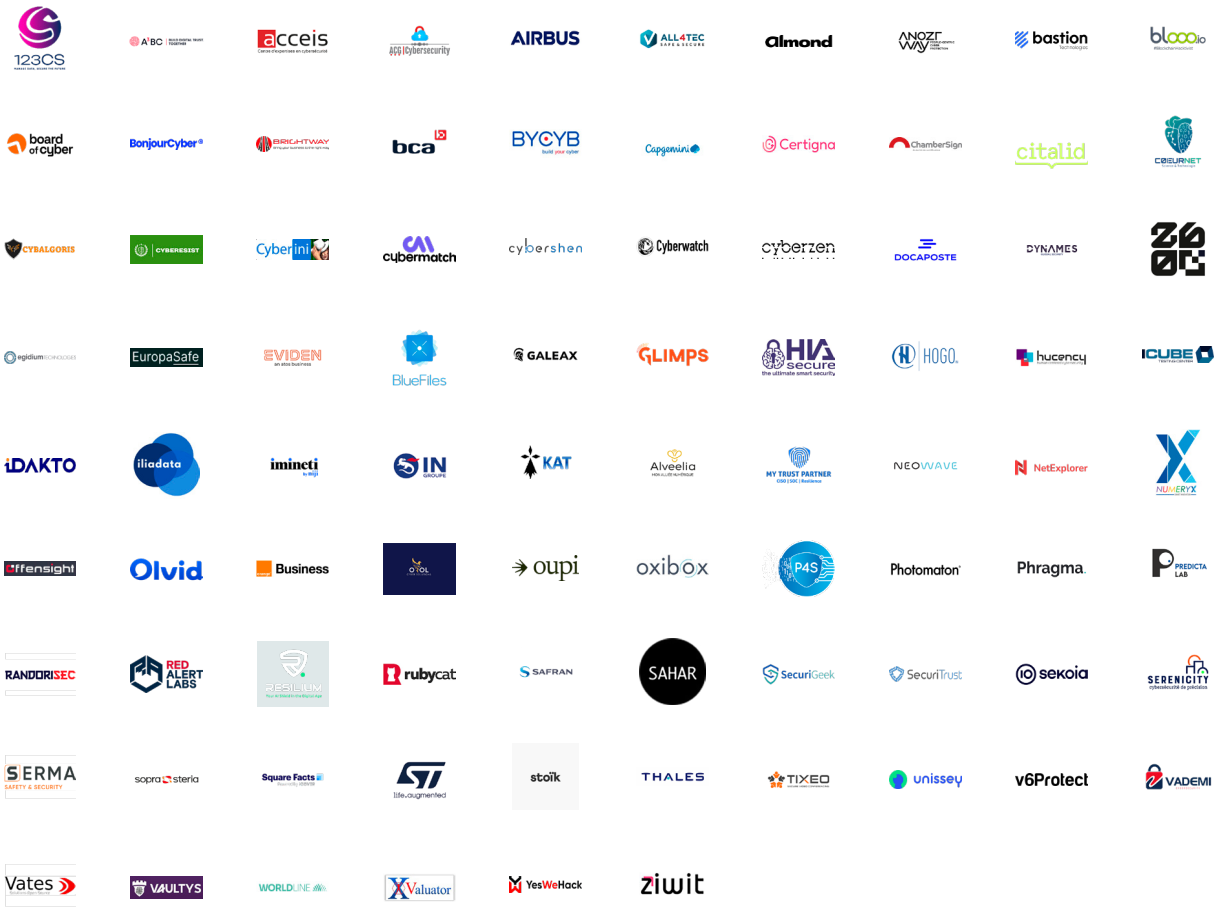
ceis

GICAT

Inria inventeurs du monde numérique

SPAC Smart Physical Access Control

Membres 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

ACN

Alliance pour la confiance numérique

Inspirer Rassembler Renforcer Agir

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