skema THINK TANK PUBLIKA

TRIBUNE
REGLES DU JEU

CYBERSECURITE FRANÇAISE

Juin 2026

Une offre qui croît plus vite que son absorption

Jean Langlois-Berthelot et Christophe Gaie

Face à l'explosion des cyberattaques, la profusion de nouvelles solutions donne parfois l'impression d'un emballement artificiel, voire de la création d'une bulle. Elle n'en est pas une au sens classique : la menace est tangible, les incidents sont réels, et le secteur produit déjà des revenus et des emplois substantiels. Le point économiquement pertinent est plus précis. Certaines couches de l'offre, en particulier la plus visible, faite de jeunes éditeurs, de promesses de plateformes, de récits de souveraineté et désormais d'habillages IA, croissent désormais plus vite que la capacité du marché à les absorber. Une lecture sérieuse de la situation économique de la cybersécurité en France met en regard quatre séries d'indicateurs : le chiffre d'affaires, l'emploi, la démographie des acteurs et la vitesse de conversion de la demande en achats et en performance. C'est à ce niveau que l'équilibre actuel entre le rythme de l'innovation technologique et la capacité de financement des acteurs économiques change de nature.

Les périmètres statistiques ne sont pas parfaitement identiques d'une source à l'autre, ce qui nous oblige à réaliser un diagnostic structurel. En 2023, la Direction générale des entreprises (DGE) évaluait la filière cybersécurité française à 10,45 milliards d'euros de chiffre d'affaires et 50 000 emplois[1]. L'Observatoire 2025 de l'Alliance pour la confiance numérique (ACN), sur un périmètre plus large de « confiance numérique », mesure 21,3 milliards d'euros de revenus et 107 000 emplois en 2024, avec une croissance annuelle moyenne de 7 % depuis 2018, contre 0,8 % pour le PIB français sur

[1] Gouvernement. (2024). La cybersécurité. Direction générale des entreprises. https://www.entreprises.gouv.fr/secteurs-dactivite/le-secteur-du-numerique-en-france/la-cybersecurite

la période, la cybersécurité y représente 53 % du chiffre d'affaires total[2]. Même en tenant compte des effets de périmètre, l'ordre de grandeur est clair : la base économique existe. La France n'est donc pas face à une fiction spéculative, mais face à un marché réel, déjà structuré.

C'est précisément pour cette raison que le décalage actuel mérite d'être pris au sérieux. La stratégie nationale de cybersécurité annoncée en 2021 mobilisait 1 milliard d'euros, dont 720 millions d'argent public, avec pour objectif de porter la filière de 7,3 à 25 milliards d'euros et de 37 000 à 75 000 emplois à l'horizon 2025[3]. Trois ans plus tard, l'estimation de la DGE place la cybersécurité à 10,45 milliards en 2023, et l'Observatoire ACN n'évalue l'ensemble plus large qu'à 21,3 milliards en 2024. Le volontarisme public a donc progressé plus vite que l'échelle économique effectivement atteinte. La question n'est pas l'existence du secteur, mais l'alignement entre la dynamique de l'offre et la profondeur réelle du marché.

A. UNE INDUSTRIE BIEN REELLE, MAIS UNE COUCHE START-UP QUI S'EPAISSIT MAL

La première erreur de perspective consiste à raconter la cybersécurité française comme une histoire de logiciels et de plateformes. La base économique du secteur reste, structurellement, une économie de services. L'Observatoire ACN chiffre les services de cybersécurité à 5,036 milliards d'euros, 29 271 emplois et 717 entreprises en 2024, dont 2,189 milliards pour l'audit, le planning et le conseil, 1,614 milliard pour la mise en œuvre, et 1,119 milliard pour la sécurisation de l'infogérance et de l'exploitation. Les produits de cybersécurité totalisent, eux, 24 641 emplois[4]. Ces chiffres montrent que la cybersécurité en France est d'abord une industrie d'intégration, d'audit, d'exploitation et de mise en conformité. La couche start-up n'en est pas le cœur économique mais elle en est la bordure la plus visible.

[2] ACN. (2025). Observatoire de la Filière de la Confiance Numérique. https://www.confiance-numerique.fr/wp-content/uploads/2025/06/observatoire-acn-2025-de-la-confiance-numerique.pdf

[3] Ministère de l'Économie, des Finances et de la Relance. (2021). Cybersécurité : renforcement par le Gouvernement de la protection des citoyens, des administrations et des entreprises. https://www.economie.gouv.fr/cybersecurite-renforcement-gouvernement-protection-citoyens-administrations-entreprises

[4] ACN. (2025). Observatoire de la Filière de la Confiance Numérique. https://www.confiance-numerique.fr/wp-content/uploads/2025/06/observatoire-acn-2025-de-la-confiance-numerique.pdf

Or c'est précisément cette bordure qui commence à envoyer des signaux de déséquilibre local. Le Radar Wavestone–Bpifrance 2025 recense 179 start-ups et 46 scale-ups de cybersécurité en France, contre 168 start-ups et 42 scale-ups un an plus tôt. À première vue, la progression semble robuste. Mais le détail est moins flatteur. Les start-ups du radar n'emploient plus que 1 685 personnes en 2025, contre 1 687 en 2024. Autrement dit, le nombre d'acteurs augmente, mais pas l'emploi dans la couche la plus jeune. La taille moyenne d'une start-up du radar passe ainsi d'un peu plus de 10 salariés à moins de 9,5 en un an. Plus inquiétant encore, 70 % de ces start-ups comptent moins de 10 salariés, contre 67 % l'année précédente, tandis que la part de celles qui dépassent 20 salariés recule de 12 % à 7 %[5]. Même en tenant compte des biais de sélection inhérents à ce type de radar, le signal reste net : le stock d'acteurs s'élargit plus vite que leur épaisseur économique.

L'analyse du financement confirme cette lecture. Le montant total levé par l'écosystème de la cybersécurité français remonte à 289 millions d'euros entre juin 2024 et mai 2025[6], contre 229 millions l'année précédente. Pris isolément, ce chiffre paraît rassurant, d'autant que la French Tech dans son ensemble a levé 7,4 milliards d'euros en 2025, en baisse de 5 % en valeur et de 15 % en volume. Mais la variable structurante n'est pas le total, c'est sa distribution. Dans la cybersécurité, le nombre de levées passe de 29 à 19 en un an. Les petits tours, indicateur de profondeur d'amorçage, se contractent nettement : neuf levées inférieures à 10 millions pour 17 millions d'euros en 2025, contre vingt-et-une levée pour 56 millions en 2024. À l'inverse, dix tours supérieurs à 10 millions concentrent l'essentiel des montants, et la France reste quasiment absente des levées supérieures à 30 millions. Le marché ne semble donc pas s'élargir mais plutôt se polariser[7].

Cette polarisation serait moins problématique si elle s'accompagnait d'une consolidation industrielle nette. Or le *turnover* des acteurs révèle l'inverse. En 2025, 43 start-ups entrent dans le radar et 33 en sortent. Parmi les sorties,

[5] Wavestone–Bpifrance. Radar des startups cybersécurité françaises 2025 : avec 179 startups et 46 scale-ups, l'écosystème français poursuit sa croissance malgré un rythme moins soutenu. BpiFrance. https://presse.bpifrance.fr/radar-des-startups-cybersecurite-francaises-2025-avec-179-startups-et-46-scale-ups-lecosysteme-francais-poursuit-sa-croissance-malgre-un-rythme-moins-soutenu/?lang=fra

[6] Ibid.

[7] Ibid.

on compte 11 cessations d'activité et 8 acquisitions[8], contre une seule acquisition l'année précédente. Le marché se sélectionne déjà. Surtout, les nouvelles entrées se concentrent dans des bandes fonctionnelles très lisibles comme la sécurité applicative, l'anti-fraude, la gouvernance, l'intelligence artificielle ou la gestion des vulnérabilités. Ces nouveaux entrants se concentrent sur des segments déjà fortement occupés, ce qui est problématique car un écosystème qui attire ses nouveaux acteurs sur les mêmes couches produit des redondances plus vite qu'il n'ouvre de nouveaux espaces.

Le cas de l'IA est particulièrement éclairant. Le Radar 2025 indique que 53 % des start-ups et scale-ups intègrent désormais l'IA dans leur offre, 30 % l'utilisent pour automatiser ou accélérer des actions de cybersécurité, et 15 structures se positionnent spécifiquement sur la sécurisation des usages ou des modèles d'IA, contre 11 un an plus tôt. Cette extension thématique est logique mais, dans un marché en approfondissement réel, elle devrait s'accompagner d'un épaississement des preuves industrielles. Or celles-ci restent concentrées. Seules 15 % des start-ups disposent d'au moins une certification en cybersécurité, contre 49 % des scale-ups. L'internationalisation agit comme un révélateur supplémentaire avec 61 % de structures exportatrices, et même 93 % chez les scale-ups. Le clivage principal ne sépare donc pas innovation et conservatisme, il distingue les acteurs capables de convertir leur offre hors du marché national de ceux qui en dépendent encore.

Il faut ici mesurer ce que cela signifie économiquement. Les 46 scale-ups du radar totalisent 4 483 emplois, contre 1 685 pour les 179 start-ups. L'essentiel de l'épaisseur de cette couche innovante repose donc sur un nombre limité d'acteurs déjà consolidés. La dynamique actuelle correspond moins à un approfondissement homogène qu'à une phase de sélection. Quelques trajectoires s'épaississent, tandis que la base se fragmente.

B. LE VRAI GOULOT D'ETRANGLEMENT EST L'ABSORPTION

Ce diagnostic ne repose pas sur une faiblesse de la demande. Au contraire. L'ANSSI a traité 4 386 événements de sécurité en 2024, en hausse de 15 %

[8] Ibid.

sur un an. Son panorama 2025 relève 196 incidents impliquant une exfiltration de données, contre 130 en 2024[9]. Le CESIN estime que 40 % des grandes organisations ont subi au moins une attaque significative en 2025, et que 81 % des victimes ont enregistré un impact sur leurs activités[10]. Le besoin est réel, constant et mesurable.

Pour autant, ce besoin ne se convertit pas mécaniquement en marché fluide pour l'ensemble de l'offre. Sur les grands comptes, la pression réglementaire est massive : 85 % des entreprises se déclarent concernées par au moins un texte sur la cybersécurité, dont 59 % par NIS2, 32 % par DORA et 30 % par le règlement sur la cyber résilience[11]. Mais cette pression ne produit pas automatiquement une allocation efficace. Le baromètre EY–Hexatrust montre que 49 % des organisations n'ont pas défini de plan d'action pour ces cadres, 40 % ne font aucune veille sur les solutions souveraines, et si 75 % connaissent les labels du secteur, seuls 47 % les utilisent comme critère d'achat[12]. La pratique reste donc plus lente à s'adapter que les discours sur la souveraineté se développent.

Le point le plus structurant est la capacité d'absorption opérationnelle. L'étude CESIN–I-Tracing d'avril 2026 montre que 85 % des organisations utilisent au moins deux outils pour suivre les vulnérabilités, et 15 % en utilisent cinq ou plus, 24 % pilotent encore partiellement via des fichiers partagés, 22 % n'ont ni tableau de bord ni outil dédié, et seules deux entreprises sur cinq disposent d'un processus transverse de priorisation. Dans le même temps, les vulnérabilités critiques sont exploitées en 24 à 48 heures, mais moins de 8 % sont corrigées en moins de 24 heures[13]. Si les capacités de détection des attaques cybernétiques existent, leur remédiation est moins nette. Ceci semble indiquer que l'écosystème de la

[9] ANSSI. (2025). Panorama de la cybermenace 2024 : mobilisation et vigilance face aux attaquants. https://cyber.gouv.fr/actualites/panorama-de-la-cybermenace-2024-mobilisation-et-vigilance-face-aux-attaquants/

[10] CESIN. (2026). 11e édition du baromètre annuel du CESIN. https://cesin.fr/document.php?d=69772cd352310

[11] EY et Hexatrust. (2025). Baromètre de la souveraineté numérique 2025. https://www.ey.com/content/dam/ey-unified-site/ey-com/fr-fr/services/cybersecurity/documents/ey-barometre-de-la-souverainete-numrique-sep-2025.pdf

[12] Baromètre EY–Hexatrust (2025). Cybersécurité et souveraineté : où en sont les entreprises françaises ?. https://www.ey.com/fr_fr/insights/cybersecurity/cybersecurite-et-souverainete-ou-en-sont-les-entreprises-francaises

[13] CESIN–I-Tracing. (2026). Gestion des vulnérabilités : Comment réduire votre exposition aux cyberattaques ?? https://cesin.fr/document.php?d=69d5029a53a29

cybersécurité produit davantage de visibilité que de réduction effective du risque.

Le CESIN documente le même décalage sous un autre angle. Le *phishing* reste le premier vecteur d'attaque à 55 %, devant l'exploitation de failles à 41 % et les attaques via des tiers à 35 %[14]. Un tiers des organisations estime que plus de la moitié de leurs incidents proviennent de tiers. Pourtant, 81 % des entreprises pensent disposer d'une visibilité complète sur leurs actifs, mais cette confiance chute à 31 % pour les environnements *cloud*. Les angles morts persistent sur les accès à privilèges, les sous-traitants et les environnements hybrides. Ces éléments confirment un manque d'intégration efficace des solutions disponibles sur le marché.

La situation des PME et ETI accentue ce décalage. 82 % laissent l'informatique au dirigeant, 72 % n'ont aucun personnel dédié, 68 % dépensent moins de 2 000 euros par an en cybersécurité, et seulement 10 % envisagent d'augmenter ce budget[15]. Ce segment constitue un volume économique considérable, mais pas encore un marché solvable pour des offres complexes. Il appelle des modèles simples, mutualisés et opérés, bien plus que la multiplication de plateformes.

Enfin, la question de la souveraineté révèle une limite structurelle. L'Union européenne représente environ un quart des achats mondiaux[16] de cybersécurité, mais seulement 5 % du marché mondial[17]. La demande communautaire existe, mais elle se convertit largement en revenus pour des acteurs non européens. Sans mécanismes de conversion de la commande en

[14] CESIN. (2026). 11e édition du baromètre annuel du CESIN. https://cesin.fr/document.php?d=69772cd352310

[15] Cybermalveillance.gouv.fr. (2024). Cybermalveillance.gouv.fr, le Club EBIOS, la CPME, le MEDEF et l'U2P lancent ImpactCyber pour inciter les TPE-PME à se sécuriser. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cp-lancement-impactcyber

[16] GINEIKYTE-KANCLERE, V., EGGERT, M., SKIOTYTE, G., & Visionary Analytics. (2025). European software and cyber dependencies (By European Parliament's Committee on Industry, Research and Energy (ITRE) & European Parliament). https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778576/ECTI_STU(2025)778576_EN.pdf

[17] Commission européenne. (2026). Proposal for a Regulation of the European Parliament and of the Council on a framework of measures for strengthening the Union's semiconductor ecosystem, repealing Regulation (EU) 2023/1781 (Chips Act 2.0) (COM(2026) 504). Direction générale des réseaux de communication, du contenu et des technologies.

traction domestique, la croissance de l'offre nationale ne garantit pas la consolidation industrielle.

La Cour des comptes souligne d'ailleurs que la stratégie nationale de cybersécurité reste à traduire en programmation opérationnelle détaillée. L'intervention publique a joué un rôle d'amorçage légitime. Mais un écosystème qui a crû sous impulsion publique plus vite que ne s'installe son autonomie commerciale reste exposé à un ajustement.

Ainsi, la cybersécurité française ne présente pas les caractéristiques d'une bulle au sens classique. Elle repose sur une demande réelle, des incidents avérés et une base économique solide. En revanche, les données convergent vers un désajustement croissant entre la densité de l'offre, la capacité du marché à la discriminer, et la production effective de gains défensifs mesurables. Si l'écosystème consolide ses acteurs, épaissit ses équipes, améliore ses indicateurs opérationnels et convertit davantage sa demande domestique, la phase actuelle apparaîtra comme une sélection normale. À défaut, la multiplication des offres ressemblera moins à un approfondissement de marché qu'à une saturation préalable à la consolidation.