PÔLE D'EXCELLENCE CYBER

Livre blanc

INNOVATION

Novembre 2025

Région BRETAGNE

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

Sommaire

Sommaire

PRÉFACE


Crédit photo : © Ministère des Armées

L'intensification des tensions internationales et l'accélération du progrès technologique marquent une bascule géopolitique et stratégique majeure. Dans ce contexte mouvant, les menaces cyber se distinguent par leur caractère proliférant : elles touchent aussi bien les infrastructures critiques que les usages du quotidien, elles ciblent à la fois les États, les entreprises et les citoyens. Elles mettent en jeu la résilience de nos institutions, la continuité de notre économie, mais aussi, plus largement, les valeurs de notre démocratie.

Cette situation exige une réponse ferme et structurée. La cybersécurité n'est plus seulement un enjeu technique : elle est devenue une condition indispensable de notre autonomie stratégique et de notre souveraineté nationale. Elle appelle à mobiliser toutes les forces de notre société : la puissance publique, le tissu industriel, le monde académique, les innovateurs et entrepreneurs mais aussi les citoyens via la nécessité d'adopter une hygiène numérique. Dans cette équation complexe, l'innovation occupe une place centrale. Elle est le moteur qui permet de garder une longueur d'avance sur l'adversaire, de transformer des idées en capacités concrètes, et de faire émerger des solutions souveraines, adaptées aux spécificités de notre environnement opérationnel. L'innovation ne se décrète pas : elle naît d'initiatives audacieuses, de prises de risque assumées, d'expérimentations parfois imparfaites mais toujours fécondes. Elle se nourrit des échanges entre disciplines, de la confrontation des idées, et de la coopération entre acteurs très différents par leurs cultures mais unis par une même exigence.

La Loi de programmation militaire 2024-2030 consacre des moyens sans précédent à la cybersécurité, avec plusieurs milliards d'euros mobilisés. Cet effort traduit une volonté claire : doter la Nation de capacités robustes, renforcer la résilience de nos forces et de nos infrastructures, et soutenir les talents qui portent nos innovations. Au-delà des chiffres, c'est un signal politique fort : la cybersécurité est désormais considérée comme une composante à part entière de notre supériorité opérationnelle.

Mais disposer de moyens ne suffit pas pour obtenir des résultats tangibles. C'est ici que le Pôle d'excellence cyber joue un rôle essentiel. En fédérant chercheurs, industriels, collectivités et acteurs institutionnels, il crée un écosystème où les idées peuvent circuler, être confrontées, protégées et concrétisées. Il favorise le passage du laboratoire au terrain, de l'expérimentation au déploiement. Il permet aussi d'inscrire les innovations dans la durée : car innover, ce n'est pas seulement inventer, c'est aussi tester, certifier, adapter, puis porter à l'échelle.

Ce livre blanc illustre parfaitement cette dynamique. Il met en lumière la richesse des initiatives, la diversité des parcours, et la vitalité de celles et ceux qui, chaque jour, explorent de nouvelles voies pour renforcer notre cybersécurité. Il témoigne aussi d'une conviction partagée : l'innovation cyber ne repose pas uniquement sur des technologies de pointe, mais aussi sur des organisations agiles, des usages repensés, et une culture commune de la protection et de la résilience.

À travers les contributions rassemblées dans ces pages, vous découvrirez des expériences inspirantes, des dispositifs d'accompagnement, mais aussi des pistes concrètes pour transformer une idée en projet, un projet en produit, et un produit en capacité opérationnelle. Cet ouvrage se veut un guide, mais aussi une invitation : à oser, à entreprendre, à collaborer. La cybersécurité est un domaine exigeant, mais elle est aussi un formidable terrain d'innovation et d'aventure collective. Je forme le vœu que ce livre blanc inspire et accompagne celles et ceux qui, par leur audace et leur détermination, construiront la souveraineté numérique de demain.

Bonne lecture.

Emmanuel CHIVA
Délégué général pour l'armement
Direction Générale de l'Armement (DGA)

INTRODUCTION

Jean-Luc GIBERNON
Vice-président
Développement Industriel
du Pôle d'excellence cyber

Nadine PRIAM
Relations extérieures cyber
Direction Générale de l'Armement
Maîtrise de l'information

Benoît WINTREBERT
Spécialiste en intelligence artificielle,
drones et technologies spatiales
Inria

Dans le domaine de la cyber, l'innovation revêt une importance cruciale. Les technologies et les usages numériques évoluent à une vitesse vertigineuse, comme en atteste l'émergence de l'intelligence artificielle générative. Les éditeurs de solutions cyber et les prestataires de services doivent impérativement suivre ce rythme soutenu.

Parallèlement, les cyberattaquants ne sont pas en reste. Leurs outils, méthodes et agilité témoignent d'une capacité d'adaptation impressionnante. Ils inventent, expérimentent et se réinventent sans cesse. Ainsi, tous les acteurs de la cyber doivent non seulement suivre les évolutions des menaces, mais aussi anticiper les ruptures technologiques.

Le monde est de plus en plus interconnecté et en constante mutation, l'innovation ne se limite plus à être un simple levier de différenciation. Elle devient un impératif absolu pour quiconque souhaite transformer une idée en un avantage durable et pérenne.

À la lumière de ce constat, le Pôle d'excellence cyber (PEC) a réuni des acteurs issus du monde de l'innovation, tant du secteur privé que du milieu académique, pour élaborer le livre blanc que vous vous apprêtez à découvrir. Le contexte dans lequel nous évoluons est particulièrement singulier. Le parcours de l'innovation est exigeant, mais ce livre blanc se propose de mettre en avant des aides disponibles et de présenter les parcours les plus inspirants. Il a pour ambition de vous aider à passer de la réflexion à l'action : vous y trouverez des pistes concrètes pour identifier comment innover, adopter les attitudes et méthodes propices à l'émergence d'un produit ou service à fort impact, et vous lancer dans la création de votre propre structure – qu'il s'agisse d'une nouvelle idée au sein d'une entreprise existante ou de la fondation d'une start-up.

Et si la prochaine rupture était déjà sous vos yeux, sans que vous l'ayez identifiée ?

Dans de nombreuses entités, les projets les plus prometteurs ne sont pas toujours les plus visibles. Ce que vous développez aujourd'hui pour résoudre un problème opérationnel précis — une fonctionnalité, un protocole, une architecture — peut receler un levier stratégique, pour peu qu'il soit regardé autrement, cultivé à l'abri des regards, et révélé au moment juste. L'information que vous détenez déjà est une force. Encore faut-il en prendre conscience.

Cependant, l'innovation s'accompagne d'un défi de taille : concilier l'ouverture indispensable à la co-création et à la collaboration avec la sauvegarde des informations sensibles, souvent désignées sous le terme d'«innovation confidentielle ». Le Pôle d'excellence cyber, grâce à son expertise et son soutien, incarne parfaitement ce dilemme entre ouverture et protection: il encourage le partage des savoir-faire pour accélérer la transition de l'idée au marché, tout en assurant un cadre sécurisé pour préserver la propriété intellectuelle

En vous plongeant dans ce livre, vous découvrirez comment le Pôle d'excellence cyber facilite la mutualisation des expertises et des ressources pour transformer les bonnes idées en innovations à forte valeur ajoutée, tout en préservant les informations sensibles. Vous verrez notamment :

- Comment repérer une opportunité et mesurer son potentiel dans des secteurs soumis à d'importantes contraintes de confidentialité.
- Comment s'appuyer sur un écosystème d'innovation ouvert, tout en protégeant la propriété intellectuelle et en maîtrisant les risques cyber.
- Comment bâtir un réseau solide grâce à la dynamique initiée par le Pôle d'excellence cyber, favorisant la confiance et la coopération sécurisée.

Pour donner vie à cette ambition, nous avons recueilli les témoignages de profils variés : entrepreneurs audacieux, acteurs de l'industrie, start-upers qui ont su conquérir leur marché, et même des porteurs de projets ayant essuyé des échecs riches d'enseignements. Leurs expériences mettent en lumière le rôle primordial de la détermination, portée par la passion, pour surmonter les obstacles et concrétiser une vision. Au fil des pages, vous découvrirez des conseils pratiques, des retours d'expérience inspirants, ainsi que des outils pour structurer vos démarches d'innovation.

En somme, cet ouvrage se veut un guide pour ceux qui aspirent à transformer leurs idées en projets concrets et impactant. Laissez-vous inspirer par ces trajectoires uniques et osez vous lancer : l'innovation est un terrain d'aventure où l'audace, l'ouverture maîtrisée et la protection de vos savoir-faire constituent les clés du succès.

Le Pôle d'excellence cyber offre une perspective singulière sur l'innovation. Il nous a paru essentiel de partager cette vision le plus largement possible. Nous vous souhaitons une lecture enrichissante et inspirante !

Jean-Luc GIBERNON, Nadine PRIAM & Benoît WINTREBERT
Coordinateurs de cet ouvrage

PARCOURS INSPIRANTS

La difficulté d'innover en cyber

SIEM, SOAR, XDR, NDR, EDR, IAM, PAM, SSO, CSPM, NGFW, IPS…
La cybersécurité semble saturée d'acronymes et de solutions toujours plus nombreuses. À première vue, l'écosystème donne l'impression d'être déjà couvert sous tous les angles. Face à une abondance d'offres de plus en plus sophistiquée, une question se pose : **où reste-t-il de la place pour l'innovation ?** Et pourtant, les cyberattaques ne cessent d'évoluer, notamment au rythme des technologies émergentes.

Un marché saturé… en apparence seulement

C'est un défi majeur. En plus d'adresser l'ensemble de la surface d'attaque existante, de manière exhaustive et sans rentrer en conflit avec les contraintes métiers, le secteur de la sécurité doit fournir des solutions pour faire face aux attaques rendues possibles par l'adoption de nouvelles technologies. Et la maturité des profils d'attaquants fait qu'**on ne peut plus se permettre d'attendre une adoption massive d'une technologie émergente avant de traiter le risque cyber.** Une attitude attentiste crée une dette cyber difficilement rattrapable. C'est sur cette conviction que j'ai fondé Skyld, une startup deeptech pionnière à l'intersection de la cybersécurité et de l'intelligence artificielle. L'IA devient omniprésente dans nos sociétés, et ce dans tous les secteurs de l'économie, comme la santé, la défense, l'industrie 4.0, les mobilités autonomes. Au fur et à mesure de cette adoption, **les algorithmes permettant l'IA vont également devenir des cibles**, et cette menace est encore trop souvent sous-estimée. Or la confiance devrait être le socle de toute adoption technologique, afin d'éviter des répétitions de l'histoire cyber, avec l'adoption massive d'une technologie sans une conscience aigüe des risques associés ni de solution clé en main pour répondre à ces risques.

Protéger l'intelligence artificielle : un nouveau champ de bataille

J'ai voulu créer cette brique de confiance, en développant des solutions capables de **protéger les systèmes d'IA contre des menaces spécifiques** : le vol de modèle, les exemples adversariaux, la fuite d'information par inversion de modèles, etc. Et très vite, j'ai eu une autre conviction : développer ce type de solutions innovantes ne pourra se faire qu'avec l'aide de laboratoires de pointe en recherche en cybersécurité et en intelligence artificielle. En effet, c'est **dans ces laboratoires que s'inventent les standards industriels de demain.** De nombreux organismes de recherches (l'Inria, le CNRS ou encore les universités) déploient activement des dispositifs permettant ce type de partenariat entre un laboratoire de recherche et une entreprise émergente. Cela nous a permis de créer une entreprise avec un actif en propriété intellectuelle déjà important. De plus, s'entourer de partenaires établis nous a permis de renforcer notre crédibilité.

Construire une deeptech : entre conviction, recherche et entrepreneuriat

Mais une technologie, aussi innovante soit-elle, ne constitue qu'un point de départ. Créer une startup technologique sur un besoin naissant signifie aussi **se confronter à un marché immature.** Travailler sur une menace encore peu visible, c'est aussi accepter de jouer un rôle pédagogique. Expliquer pourquoi un système d'IA peut être vulnérable, comment un attaquant peut le manipuler, pourquoi il faut agir maintenant. Tout cela demande du temps, des preuves, de la conviction. Une innovation technologique sans prise de conscience qui pourrait mener à son adoption ne crée pas une entreprise.

Enfin, il faut être en capacité de dépasser la posture de l'inventeur pour devenir chef d'entreprise. Et le chef d'entreprise a trois rôles principaux : porter la vision de l'entreprise, trouver des financements et embaucher l'équipe qui lui permettra d'exécuter sa vision. Pour moi, la vision était claire : **l'intelligence artificielle a besoin d'être sécurisée**, et cela ne se fera pas en adaptant les solutions de sécurité existantes mais en concevant des solutions innovantes et sur-mesure.

Reste alors à trouver les premiers capitaux pour rendre cette vision réalité. En France, nous avons la chance de bénéficier d'un important dispositif d'aides, opérées notamment par la BPI, pour financer les entreprises dites deeptech, donc issues d'une collaboration avec les laboratoires de recherche. Ces aides permettent de compenser la difficulté à s'auto-financer : difficile de vendre un produit qui met plusieurs mois, voire années, à se construire ! En revanche, ces aides restent conditionnées à l'obtention de capitaux privés. Les trouver pour pouvoir prétendre à ces dispositifs n'est pas chose aisée

Si l'ancrage local est pour nous un facteur important de stabilité et de succès, j'ai voulu porter, dès le début, une ambition internationale. J'ai eu la chance de trouver un accélérateur porté par l'université de Berkeley, donc friand de nouvelles technologies et de startups deeptech, mais avec un financement européen, plus adapté à un secteur aussi stratégique que la cybersécurité. C'est ce qui a permis à Skyld de prendre son envol.

Soutenir financièrement des jeunes pousses est une aventure risquée, mais c'est aussi un facteur clé si nous souhaitons préserver notre souveraineté numérique. En effet, c'est le maillon manquant entre les universités et les laboratoires de recherche qui financent le transfert de technologies et les fonds de capital-risque qui prennent le relais sur les aventures à peine plus matures.
Aujourd'hui, Skyld continue de grandir grâce à une équipe solide. Nous collaborons avec des partenaires industriels et institutionnels pour sécuriser les systèmes d'IA dans les contextes les plus critiques. Ce n'est que le début. Je suis convaincue que la cybersécurité est nécessaire pour une adoption en toute confiance de l'intelligence artificielle. Je suis fière d'être en première ligne de cette transformation.

Créer une entreprise est une aventure exigeante, mais profondément porteuse de sens. C'est un savant cocktail entre innovation technologique, aventure humaine et création de partenariats solides. Si je partage ce parcours, c'est pour encourager celles et ceux qui, aujourd'hui, voient un angle mort : **vous avez peut-être entre vos mains les graines d'une innovation clé.**

Cyrille Vignon, Valérian Comiti, Jérémy Bouetard et Frédéric Grelot étaient ingénieurs au Ministère des Armées, en Investigation des Malwares et Produits de Sécurité (IMPS), avant d'être choisis pour lancer le projet pilote de l'incubateur Cyber Défense Factory, rattaché au Ministère.

Frédéric Grelot ayant quitté l'entreprise en 2024 pour retrouver des missions de recherche à l'AMIAD, ce sont Cyrille (CEO), Valérian (Directeur des Opérations) et Jérémy (Directeur de la R&D) qui reviennent sur leur parcours, de l'idée à la concrétisation, vers la success-story.

Des travaux de recherche à l'incubateur

A l'origine, les quatre ingénieurs travaillaient sur des missions de reverse engineering au Ministère des Armées. Ils ont alors rapidement détecté le potentiel de ces travaux, et se retrouvaient même sur leur temps libre pour poursuivre les recherches. Progressivement, ils sont arrivés à des résultats qui dépassaient leurs espérances, cela allait même au-delà de ce qui était publié dans les revues scientifiques sur ce sujet. "A ce moment-là, il y avait une frustration, car on commençait à développer des outils, mais nous n'avions pas le temps de nous concentrer dessus avec nos missions à accomplir en parallèle au Ministère", se souvient Jérémy Bouétard. Le Ministère des Armées leur a alors proposé de rejoindre l'incubateur, ce qu'ils ont accepté. Pour Valérian Comiti, le "goût de l'aventure et le défi technologique" ont été des éléments déclencheurs pour se lancer dans ce projet.

Il fallait l'avoir, cette envie d'aventure, car les débuts n'ont pas été simples. Il a été nécessaire d'adapter le projet, initialement de recherche, au marché, et de trouver le business model idéal. La difficulté était qu'il fallait aller très vite, la cybersécurité étant un secteur très dense et évolutif. "J'étais convaincu de la pertinence de notre produit. Mais quand j'ai été pour la première fois au Forum InCyber de Lille, j'ai pris une claque en découvrant l'ampleur de l'écosystème cyber. Je me suis dit "comment va-t'on pouvoir faire entendre notre voix ?". Notre chance dans tout ça, c'était d'avoir peu de concurrents avec un produit similaire, et surtout d'être adaptables", se rappelle Cyrille Vignon.

Le cœur du projet d'entreprise était au départ axé sur le reverse-engineering. Pour s'adresser à un public large et ne pas s'enfermer dans une niche, il a fallu l'étendre vers l'analyse de malwares, puis l'analyse de grands volumes de fichiers.

Selon Cyrille Vignon, une autre des grandes difficultés a été de passer, pour nous 4, "d'un monde de salariés avec des limites bien définies, à un monde dans lequel il n'y avait plus de cadre, ou du moins c'était à nous de le définir et on partait d'une feuille blanche.

Pour les aider, les fondateurs ont pu compter sur l'accompagnement de plusieurs organismes. Cyrille

Vignon a constaté “à quel point tous les organismes bretons travaillaient en synergie ensemble” (BDI, BPI, le Poool, la Région Bretagne, la Métropole de Rennes…).

En 2020, les co-fondateurs ont cherché à renforcer leurs fonds propres, avec des prêts d’honneur, (Réseau Phar Bretagne de la Région, et la CCI Ille-et-Vilaine) et une levée de fonds “friends & family”. Cela a permis de décrocher le projet de subvention RAPID (de l’Agence de l’Innovation de Défense), pour finaliser GLIMPS Audit et financer les premiers pas de GLIMPS Malware.

Le chemin vers la rentabilité

En 2021, une levée de fonds auprès d’investisseurs a permis d’apporter 6 millions d’euros. L’accent a été mis sur le recrutement d’une équipe R&D de plus de 10 personnes, indispensable pour développer la solution. Les fonds ont aussi servi à agrandir les autres équipes (commerce, marketing, fonctions support…). Il fallait trouver des personnes qui permettraient à la synergie d’opérer.

“A mon sens, si on veut que son entreprise grandisse, il faut réussir à déléguer et chercher à devenir inutile en quittant l’opérationnel. Parallèlement, il faut se structurer, mettre en place des process”, indique Cyrille Vignon. L’obstacle que les fondateurs ont rencontré et qui a été un moment de frustration, est lié au manque de structuration dans les équipes après avoir beaucoup recruté. « Ce n’est qu’une fois qu’on a pris le temps de se réorganiser, notamment en mettant en place du middle management, que l’effet levier lié à la croissance des équipes est revenu », ajoute-t’il.

Pour les fondateurs, tout n’est pas qu’une question de structure et de process. Selon Valérian Comiti, Directeur des Opérations, “La bienveillance, c’est l’une des valeurs phares de notre entreprise. Les collaborateurs doivent pouvoir s’exprimer librement, et il ne faut pas brider cette créativité”. Il faut aussi les encourager à penser différemment, à proposer de nouvelles idées, à innover, pour que GLIMPS soit efficace sur le marché”.

Dans le secteur de la cybersécurité, et d’autant plus lorsque l’on est nouveau sur le marché, les cycles de vente sont très longs. Il a fallu évangéliser pour faire connaître la solution, mais cela ne se concrétisait pas immédiatement. « Nous étions dépendants des budgets annuels, il fallait attendre que l’achat de notre produit par une entreprise soit mis au budget de l’année suivante », se souvient Cyrille Vignon.

En France sur le marché de la cybersécurité, les entreprises ont tendance à vite se considérer comme concurrentes. Mais Cyrille Vignon ne voit pas les choses de cet œil. « Je crois que nous avons tout à gagner à travailler ensemble et à capitaliser sur nos complémentarités ». C’est ce qui a été fait avec des partenaires comme Sekoia.io.

Le défi des très grands volumes de fichiers

Les besoins en analyse de très grands volumes de fichiers ont beaucoup augmenté, et il a fallu être capable d’absorber ce besoin, pour traiter des dizaines de millions de fichiers par jour.

Selon Jérémy Bouétard, Directeur R&D, “cette croissance est liée à une évolution des usages en entreprise et notamment à l’explosion du cloud. Pour y répondre, nous avons optimisé nos infrastructures, pour maximiser le nombre de fichiers pouvant être traités, mais sans augmenter les ressources nécessaires. A cela s’ajoute la nécessité d’être capable de détecter toujours plus de nouvelles menaces, dans des types de fichiers encore plus variés, pour être compétitifs ». Le plan France 2030, dont l’entreprise a été lauréate, a permis de financer ces travaux d’amélioration des performances.

À propos de la souveraineté

> “C’est un défi pour les acteurs français de la cybersécurité, mais aussi une opportunité de développement.”

L’augmentation des capacités du produit impliquait de passer à l’échelle dans le déploiement de la solution, toujours dans la logique de mobiliser le moins de ressources possibles. Ce positionnement s’inscrit aussi dans la démarche RSE de l’entreprise, qui collabore avec OVHCloud, hébergeur français.

L’ambition : devenir le VirusTotal à la française

6 ans après sa création, GLIMPS poursuit son passage à l’échelle. Elle ne perd pas de vue son ambition, qui a pleinement pris son sens dans le contexte géopolitique et réglementaire de ces derniers mois. Dans de pareilles circonstances, les acteurs privés et publics tendent à préférer des solutions de sécurité françaises, pour garantir la souveraineté de leurs données.

Cyrille Vignon y voit « un défi pour les acteurs français de la cybersécurité, mais aussi une opportunité de développement pour GLIMPS. L’entreprise pourrait devenir un acteur incontournable de l’analyse de fichiers et de la détection des malwares, mais aussi une alternative crédible au géant américain VirusTotal ».

Stéphanie, pourriez-vous nous parler de votre parcours professionnel ?

Diplômée d'une école de commerce, j'ai travaillé dans le marketing, la gestion de crise et la gestion de projets transverses. Mon parcours diffère donc notablement de celui de nombreux professionnels de la cybersécurité. Il est aussi possible de s'épanouir en cyber avec les métiers non techniques !

Pendant quinze ans, j'ai occupé des postes de gestion de projet, de direction et de membre du CODIR, sans avoir de compétences techniques. Je collaborais avec la direction des systèmes d'information, mais sans être moi-même une experte en la matière. Cela démontre qu'il n'est pas obligatoire d'avoir une formation initiale en informatique ou en cybersécurité pour réussir dans ce domaine.

Ma vocation et ma passion résident dans la gestion de crise, qui m'a toujours fascinée par sa diversité et son imprévisibilité. C'est cette passion qui m'a poussée à fonder ALCYCONIE.

Après plus de vingt ans dans ce domaine, je constate que chaque crise est unique, tant dans les réactions des individus que dans la dynamique des équipes.

La rencontre entre la gestion de crise et la cybersécurité, avec des enjeux tels que la désinformation, la déstabilisation, et les aspects techniques et géopolitiques, ajoute une dimension supplémentaire à cette passion. Avec toute l'équipe, nous avons la satisfaction de contribuer à l'intérêt collectif chaque jour, ce qui renforce notre motivation et notre culture d'entreprise. Nous partageons des valeurs communes qui nous permettent d'avancer ensemble.

Comment l'aventure ALCYCONIE a-t-elle démarré ?

J'ai toujours envisagé de fonder une entreprise. Ce qui a déclenché cette décision, c'était l'envie de me consacrer entièrement à la gestion de crise. Je souhaitais développer et approfondir mes connaissances dans ce domaine. À l'époque, les crises cyber commençaient à être mentionnées, mais elles étaient perçues comme des problèmes techniques.

Mon expérience en gestion de crise dans les secteurs aérien et ferroviaire m'avait montré que les crises impliquent bien plus que le métier directement touché : ressources humaines, communication, géopolitique, intelligence économique, etc. C'est ainsi qu'est née l'idée d'ALCYCONIE. En observant le marché de la cybersécurité, j'ai constaté qu'il n'y avait pas d'entreprise offrant ce type de services. Bien que je ne vienne pas du milieu informatique, j'ai décidé de me former en retournant sur les bancs de l'école dans le cadre d'un Executive MBA, pour acquérir les compétences nécessaires.

Quel message aimeriez-vous transmettre à une femme qui veut se lancer dans l'entrepreneuriat ?

Il n'existe pas de métier préconçu pour les femmes. Lorsque j'ai lancé ALCYCONIE, je n'avais pas de formation en informatique et j'étais enceinte. Malgré les défis, il est crucial d'écouter les avis, mais aussi de se forger sa propre idée et de persévérer. L'entrepreneuriat exige beaucoup de travail, de sérieux et de rigueur. Le fait d'être une femme apporte une force et une perspective différentes.

Il est important d'être passionnée par ce que l'on fait et d'accepter de prendre des risques. Avoir une expérience professionnelle préalable est un atout majeur pour aborder la dimension humaine du management.

Pouvez-vous nous parler des échecs ou des moments difficiles que vous avez surmontés ?

Comme beaucoup d'entrepreneuses, je n'ai pas été rémunérée au lancement d'ALCYCONIE. C'est une réalité à laquelle il faut être préparé, et que son entourage doit aussi comprendre et accepter. Les autres difficultés, souvent humaines, tiennent au recrutement : une erreur peut coûter cher, et j'en ai fait l'expérience. Ces moments difficiles m'ont appris à être plus vigilante, à faire davantage confiance à mon instinct — car, comme on dit souvent, quand il y a un doute, il n'y a pas de doute.

Qu'est-ce qui vous a le plus surprise ?

J'ai été très touchée par l'accueil réservé à ALCYCONIE. En Bretagne, puis à Paris, j'ai rencontré des personnes attentives et à l'écoute, tant chez les clients que dans les institutions, face à ce projet d'entreprise unique.

Mon discours simple et honnête a semble-t-il plu, et mon approche non technique a suscité de l'intérêt.

Quelle démarche avez-vous mis en place pour réussir à pénétrer le monde de la CYBER et à vous faire connaître ?

Je viens d'une famille d'entrepreneurs, alors peut-être que j'ai ça dans le sang ! Grâce aux conseils de mon père, chef d'entreprise, j'ai contacté des personnes de mon réseau pour leur expliquer mon projet et solliciter leur aide. Cette démarche m'a permis d'obtenir mon premier client. La communauté cyber est marquée par une grande solidarité et une volonté de collaboration. Il est essentiel de se faire reconnaître par les autorités et les instances officielles pour démontrer sa légitimité.

Le secret pour réussir ?

Pour réussir, il faut créer un collectif basé sur la confiance. Il est crucial de garder les pieds sur terre et de ne pas se laisser distraire par les tentations de la tech, comme les levées de fonds ou les projets de développement à grande échelle. Il faut rester fidèle à la mission initiale de l'entreprise et contribuer à des innovations utiles.

À quoi ressemblera ALCYCONIE dans 10 ans ?

Dans 10 ans, je forme le vœu qu'ALCYCONIE poursuive sur sa lancée en contribuant à renforcer notre économie et notre patrimoine informationnel. Nous continuerons à innover et à avancer, en restant fidèles à notre mission d'utilité collective. Nous avons bénéficié de subventions et de crédits d'impôt recherche, nous nous sentons redevable d'en faire un bon usage.

Aujourd'hui, avez-vous les moyens de bien choisir vos clients ?

Il est essentiel de bien choisir ses clients pour établir une relation de confiance et de proximité. Nous n'avons jamais cherché à attirer des clients par des moyens agressifs. Notre développement a été plus lent, mais nous avons des clients fidèles depuis six ans. Il est important de s'entourer de pairs et de mentors pour discuter des difficultés et des questionnements communs.

Je me dis tous les jours « heureusement que je suis bien entourée », à commencer par ma vie personnelle. Ça compte beaucoup. La vie d'un entrepreneur est tout sauf un long fleuve tranquille, alors il faut avoir un socle, une base qui soit solide.

On a l'impression que la simplicité revient dans tout ce que vous dites, et ce que vous faites…

Vous avez raison et c'est certainement l'héritage, l'éducation peut être aussi mon côté « breton ». Je pense que parfois l'innovation, ce sont des choses très simples et qui répondent à des besoins concrets. Il vaut mieux souvent développer des choses simples que les gens comprennent.

Et le mot de la fin ?

Il faut se faire confiance et croire en soi. Oser se lancer et persévérer est essentiel.

Du Forum aux Arènes de la Cyber : le parcours inattendu d'une entrepreneure

Rien ne me prédestinait à gratter ici ma plume. Merci aux auteurs de cet ouvrage pour cet honneur.
Arrivée de Carthage à Lutèce en 2006 pour intégrer les classes préparatoires, j'ai embarqué pour une nouvelle contrée. Un monde où les mots avaient plus d'importance que les silences, où la culture générale était une religion (et pas uniquement les mathématiques !), et où les élèves semblaient tous s'être nourris de classiques, de théâtre et de musées depuis le berceau. Et moi, malgré mon amour dévorant pour la lecture, je récoltais la pire note en culture générale. Un comble.

Mais il en faut plus pour ébranler une détermination forgée par des années de lecture et d'imagination. Remettre en cause le chemin établi est devenu ma boussole. Je choisis Numérobis et jamais Amonbofis. J'ai cumulé finance et droit, jonglé entre les salles d'audience et le régulateur financier, en petite souris travailleuse d'un cabinet américain entourée de bienveillants mentors. Quand j'ai commencé à travailler comme avocate d'affaires, la pression était constante, l'adrénaline aussi. Mais c'était une cage dorée, et après quatre belles années mes ailes me démangeaient. Alors, je suis devenue directrice juridique et secrétaire du conseil d'un groupe, où les dossiers se chiffrent toujours en millions, parfois en milliards. Six années où j'ai vu au plus près ce qu'est le courage d'un entrepreneur et appris à mêler efficacité et relations humaines auprès des meilleurs, pour atteindre l'impossible.

Cette persévérance, je l'ai emportée avec moi en créant Astran il y a quatre ans. Une aventure entrepreneuriale et familiale qui, entre revers cuisants et succès éclatants, a pris les allures d'un tour de grand huit sans fin sur Toutatis . Mes associés, notre formidable équipe d'Astranautes et moi, avons ensemble parlé à des centaines de personnes, écrit des milliers de lignes de code, remporté plus de concours que de raison, effectué des recherches et déposé deux brevets (aujourd'hui en cours d'extension aux Etats-Unis et au Canada !), participé à des dizaines d'événements, réalisé pilote sur pilote, négocié jusqu'au bout de la nuit, passé des certifications de sécurité dignes de la légion romaine, et vécu ensemble sept lancements produit, huit kick-offs d'équipe et une bonne quarantaine de all hands ! Notre équipe est désormais la source intarissable de mon énergie, en binôme avec notre grande vision.

Aujourd'hui, notre mission est la résilience opérationnelle : aider les entreprises à maintenir leurs fonctions vitales face aux cyberattaques et aux interruptions graves. Écouter les clients, investir dans la recherche en cryptographie et en IA, réinventer sans cesse le produit et perfectionner notre positionnement… On ne compte plus les nuits blanches passées à peaufiner chaque détail pour répondre à ce besoin vital. Pour aujourd'hui diffuser la solution magique qui rend nos utilisateurs irréductibles face aux cyberattaques. Avec la vision demain de leur donner le super pouvoir d'être toujours plus innovants et productifs : nous construisons des agents IA qui automatisent les processus métiers (pendant une cyberattaque, et même tous les jours),

tout en investissant dans les plus hauts niveaux de recherche en cryptographie distribuée pour sécuriser les données vitales sous-jacentes.

Le travail de forçat commence à porter ses fruits. Eiffage, Sanofi, Vinci… Des partenaires prestigieux – d'aucuns diraient des empires – nous font progressivement confiance. Et de nouveaux horizons s'ouvrent à nous, de Lutèce à Londinium en passant par la Gallia Belgica. Quelle aventure. Quel honneur de rencontrer, chaque jour, des personnes exceptionnelles qui partagent cette passion de bâtir l'avenir.

Et je continue à lire, lire, lire… De Technopolitique d'Asma Mhalla à Pompéi de Mary Beard, en passant par Silo d'Hugh Howey et Madelaine avant l'Aube de Sandrine Collette. Pour continuer à découvrir et à apprendre, et pour rester ancrée à la terre ferme lorsqu'on est en apesanteur sur le grand huit de l'entreprenariat. Et chaque jour se dire : n'ayons peur de rien, à part que le ciel nous tombe sur la tête.

INNOVATION
OÙ EN EST-ON ?

L'innovation à l'AID et la DGA

L'agence de l'innovation de défense

L'organisation de l'innovation de défense vise à doter le pays d'une capacité d'innovation dans tous les domaines et sur toutes les échelles de temps, en encourageant la dualité et donc le soutien du tissu académique et industriel et la captation de l'innovation civile. Cette démarche, garante de notre supériorité opérationnelle et de notre autonomie stratégique, se doit d'être permanente, inventive, rapide. C'est l'objectif poursuivi par l'Agence de l'innovation de défense (AID), créée en 2018 par le Ministère des Armées afin d'engager une démarche de transformation globale et de recherche de performance, et de pouvoir organiser la création, la captation, la maturation et l'intégration de l'innovation tout au long du cycle de vie des systèmes d'armes et des projets.

L'AID fédère les différents acteurs du ministère des Armées et les initiatives qui concourent à l'innovation de défense en France, et s'appuie sur l'expertise de la Direction Générale de l'Armement (DGA) et de l'Agence ministérielle de l'intelligence artificielle de défense (AMIAD), ainsi que sur la capacité d'innovation des états-majors, directions et services (EMDS) qui fournissent les cas d'usage pour le ministère. Son ambition est de transformer les projets d'innovation en produits et services au profit des forces.

Les objectifs stratégiques de l'innovation de défense et les moyens associés sont fixés par le Document de référence de l'Orientation de l'Innovation de Défense (DrOID). Le DrOID établit les ambitions du ministère des Armées en matière d'innovation. Il précise également les axes d'efforts du ministère pour la captation, l'adaptation et la valorisation des technologies civiles ou duales tout en détectant les possibles ruptures technologiques.

La Loi de programmation Militaire 2024-2030 prévoit une enveloppe de 10 milliards d'euros sur la période. Ce budget permettra notamment d'offrir aux Armées la maîtrise des nouveaux champs de conflictualité à l'horizon 2030 (espace, fonds marins, champ informationnel, cyber). Il permettra également d'investir sur dix domaines technologiques prioritaires en s'appuyant notamment sur le développement de démonstrateurs ambitieux.

Pour dynamiser et fédérer l'écosystème de l'innovation de défense, l'AID est organisée en mode « projet ». On distingue quatre types de projets, chacun avec des finalités bien établies :

- Projets Technologiques de Défense : préparer les technologies de défense de demain en portant à maturation les technologies nécessaires aux besoins militaires.
- Projets de Recherche : permettre de détecter et faire émerger les futures technologies stratégiques auprès d'université, d'organismes de recherche, d'écoles ou d'entreprises.
- Projets d'Accélération de l'Innovation : accélérer l'innovation avec l'écosystème civil, en captant l'innovation issue du marché civil afin de les déployer au plus tôt.
- Projets d'Innovation Participative : encourager l'innovation provenant du ministère en permettant à tout personnel du ministère, civil ou militaire, de proposer un projet innovant.

Tout porteur de projet innovant peut consulter les appels à projet de l'AID via le lien :
https://www.defense.gouv.fr/aid/appels-projets/cours

Pour faciliter la mise en relation des porteurs de projet avec le Ministère des Armées, un guichet unique a été mis en place. Ce guichet unique est le point d'entrée pour soumettre un projet, ou demander un rendez-vous ou une mise en relation concernant une activité innovante. Grâce à son guichet unique, l'AID simplifie l'accès pour toutes les entreprises au ministère des Armées, et facilite la captation des innovations issues du monde civil. Start-ups, TPE, PME ou grandes entreprises, laboratoires de recherche, etc, peuvent toutes et tous déposer un projet. L'objectif est de consolider au plus tôt le cas d'usage et l'intérêt défense, et de structurer les projets d'intérêt pour qu'ils répondent au mieux aux besoins du ministère.

Vous souhaitez savoir si votre projet ou solution peut avoir une application au sein du Ministère, pouvant justifier son accompagnement ? Consultez le lien ci-dessous pour plus d'informations :
https://www.defense.gouv.fr/aid/deposez-votre-projet/guichet-unique

<u>En ce qui concerne la cyberdéfense, plusieurs dispositifs spécifiques ont été mis en place :</u>

Les défis CYBER

Pour répondre à des problématiques opérationnelles à fort enjeu, le Commandement de la Cyberdéfense (COMCYBER) et l'AID organisent chaque année des défis CYBER. Ces défis visent à détecter et évaluer des technologies ou solutions innovantes permettant d'adresser ces enjeux. Ils sont ouverts aux sociétés et laboratoires de recherche.
A titre d'illustration, deux thématiques font actuellement l'objet de défis : la détection de données falsifiées ou générées et la sécurisation de l'IA.

La « Cyber Defense Factory »

La « Cyber Defense Factory » est un espace ouvert dédié à l'innovation. Elle propose une offre de services complète : hébergement, accès à des données d'intérêt cyber, avis d'expertise, échange avec des utilisateurs opérationnels et capacité à tester les solutions avec des experts et des opérationnels du COMCYBER. Si vous avez un projet en cybersécurité susceptible d'intéresser la défense et que vous avez besoin d'accéder à un ou plusieurs services proposés pour mettre au point ou tester votre solution, vous pouvez déposer un dossier de candidature via ce lien :
https://www.defense.gouv.fr/aid/appels-projets/cours/appel-projets-cyber-defense-factory

L'accord de partenariat Creach Labs

Le dispositif Creach Labs soutient la recherche académique au niveau de la région Bretagne, au travers d'un partenariat entre le Ministère des Armées, la région, l'ANSSI et les organismes de recherche. Ce partenariat permet de favoriser l'émergence de sujets d'intérêt dual. Le soutien se concrétise notamment par le financement ou le co-financement de thèses et de post-doc, ainsi que par l'organisation de séminaires réunissant la communauté académique, étatique et industrielle. Parmi les dispositifs activables dans le cadre de Creach Labs, des conventions de chercheurs associés permettent à des ingénieurs de la DGA de travailler dans des équipes académiques, impulsant ainsi les besoins prioritaires de la DGA en matière de recherche Cyber. La quotité de temps allouée à un chercheur associé est en général de 20%.
Lien vers le site internet de Creach Labs :
https://www.creachlabs.fr

L'innovation cyber interne au ministère

La recherche et le développement interne à la Direction Générale de l'Armement (DGA) sont indispensables afin de renforcer nos compétences et pour développer une expertise pointue grâce à l'amélioration continue de nos savoir-faire et outillages métier. La R&D interne est cruciale pour explorer des concepts innovants qui enrichiront, à court ou moyen terme, les capacités défensives et offensives des forces du Ministère des Armées.

L'innovation interne est encouragée et favorisée au plus haut niveau, notamment par une quotité de temps réservée dans la capacité productive des agents. C'est un levier de motivation important pour les experts qui peuvent ainsi explorer des thématiques techniques non rencontrées dans un cadre projet. Dans un contexte d'évolution très rapide des technologies du numérique, l'innovation interne permet aux agents de garder une technicité pointue tout au long de leur carrière. Chacun est invité à proposer des idées et à monter des projets d'innovation multi-compétences en intra Cyber ou avec d'autres métiers du numérique. C'est une opportunité unique d'intégrer des technologies avancées telles que l'intelligence artificielle.

Les projets d'innovation interne sont valorisés de multiples façons, notamment lors de séminaires internes réunissant des centaines d'experts du pôle.

Les innovations au profit de l'expertise métier sont souvent entièrement développées en interne avant d'être déployées dans les moyens des différents laboratoires. Il est également possible, via un accord spécifique et après protection de l'invention, de mettre à disposition d'un industriel un outillage d'expertise développé dans le cadre de l'innovation interne DGA.

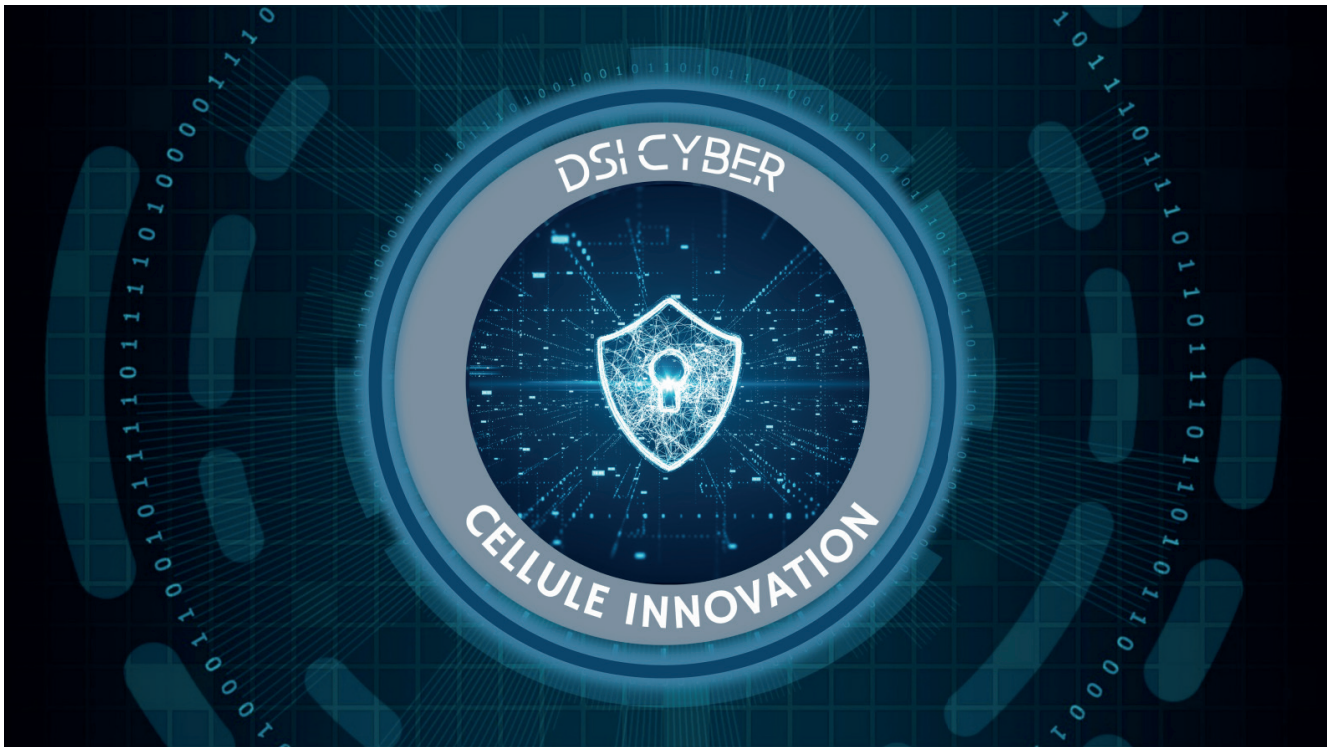
Un exemple marquant de cette innovation interne est un dispositif de recherche de signaux parasites compromettants, conçu par quatre experts. Ce dispositif se distingue par des performances très élevées, tout en affichant un coût et un encombrement divisé par 100 par rapport aux moyens existants.

Les innovations au profit du capacitaire Cyber vont jusqu'à la preuve de concept via des techniques de prototypage. Cela permet de vérifier la faisabilité du passage de l'idée à la réalisation effective et de mesurer les gains apportés. La valorisation de ces innovations peut ensuite se faire, en interne ou en externe, en passant ou non par une étape intermédiaire d'innovation externe, grâce aux dispositifs mis en place par le Ministère des Armées.

L'innovation interne apporte toujours un gain et permet de prendre des risques techniques. Même si certains verrous techniques ne sont pas levés, de nouvelles connaissances sont acquises et peuvent être mobilisées pour différents projets. Une innovation qui n'aboutit pas immédiatement peut aussi être reprise plusieurs mois ou années après un premier prototypage, lorsque la maturité de certaines techniques le permet, facilitant ainsi une mise en application fonctionnelle rapide.

Direction générale de l'armement

L'innovation au cœur de la cybersécurité : l'exemple de la DSI CYBER



Le manuel d'Oslo publié en 2018 par l'OCDE définit que le « concept d'innovation repose sur deux composantes phares : le rôle des connaissances en tant que fondement de l'innovation, de la nouveauté et de l'utilité, et la création ou la préservation de la valeur en tant qu'objectif présumé de l'innovation.». Il s'agit de connaître l'état de l'art des connaissances d'un domaine à un produit ou un procédé soit pour le créer soit pour l'améliorer.

Il est parfois difficile de comprendre et de mesurer ce gain. Or « le Manuel d'Oslo se fonde sur un principe clé, selon lequel l'innovation peut et doit être mesurée. » Ce principe permet d'adopter une approche qualitative et descriptive du processus d'innovation afin d'évaluer la portée et les effets de l'introduction de cette nouveauté. Face à une évolution numérique liée aux évolutions technologiques dont le rythme est difficile soutenable pour les acteurs privés et publics il est nécessaire de s'assurer de l'emploi des derniers SI à jour de l'état de l'art pour garantir l'efficacité et la sécurité des moyens mis en œuvre. Les efforts consentis dans la mise à jour de l'état de l'art des connaissances assurent la création et le développement de la valeur des systèmes employés.

Afin de rendre plus tangible le processus d'innovation, le manuel d'Oslo propose de définir l'innovation au travers de quatre dimensions.

La première repose sur les activités d'innovation. Ces dernières « désignent l'ensemble des activités de développement, financières et commerciales menées par une entreprise et ayant vocation à déboucher sur une innovation pour ladite entreprise. » L'innovation a besoin d'un socle solide pour se développer et aboutir aux objectifs visés. Il est donc nécessaire de faire converger la démarche de création ou d'amélioration avec les nécessités financières et commerciales dès le début du projet. Il s'agit donc de ne pas limiter la proposition de l'innovation mais de l'arbitrer pour permettre l'émergences de solutions qui répondent aux besoins du moment. C'est le rôle de la DSI cyber, de susciter les approches innovantes et les répartir dans le temps selon les besoins exprimés par les membres du ministère des Armées.

Pour mener à bien cette tâche, la DSI cyber a adopté l'approche de l'innovation d'entreprise, c'est-à-dire « un produit ou un processus d'affaires nouveau ou amélioré (ou une combinaison de ces deux éléments) qui diffère sensiblement des produits ou processus précédents de l'entreprise et a été commercialisé ou mis en œuvre par celle-ci. » Il s'agit de connaître le besoin initial exprimé par le demandeur pour le comparer ensuite à l'état de l'art des connaissances disponibles afin de proposer une solution plus avancée sur le plan technologique. Cette démarche est la vision classique de l'innovation dans le domaine technique. Or elle est limitée car elle ne prend pas en compte l'ensemble des connaissances disponibles sur une problématique. A titre d'exemple, les attaques

menées dans le cyberespace quel que soit leurs natures sont analysées au point de vue techniques (IOC, kill chain…) sans prendre en compte le volet humain (analyse comportementale, biais cognitifs …). Cette démarche limite la compréhension de l'attaque et plus globalement de la menace qui pèse sur les SI . La DSI bénéficie d'un écosystème universitaire organisé autour de chercheurs partenaires pour acquérir et entretenir cet état de l'art afin de le partager avec les membres de la CCA et ses partenaires étatiques (DGA, AID…). Du fait de ces prérogatives, le COMCYBER est un des acteurs naturels et légitimes pour animer.

Ces manifestations ont pour vocation de faire adhérer, les partenaires à la démarche d'innovation. A cette fin, comme le manuel d'Oslo le préconise, la DSI cyber met en avant l'innovation de produit. Ce type d'innovation « désigne l'introduction sur le marché d'un bien ou service nouveau ou amélioré qui diffère sensiblement des biens ou services proposés jusque-là par une entreprise. » Ainsi dans le cadre de l'introduction de connaissances issues du monde des sciences humaines et sociales (SHS) dans le domaine de la cyber sécurité il conviendra de convaincre les opérateurs puis de les former avant que ceux-ci puissent intégrer l'innovation dans le cadre de leur mission. En ce qui concerne la lutte contre la désinformation, une approche technologique ne permet pas de saisir les intentions des auteurs de messages car les systèmes d'IA disponibles ne sont pas encore assez efficaces dans la détection des intentions. Or, la reconnaissance des intentions est aussi importante que l'identification des émotions émises et perçues par les membres des groupes présents dans le cyberespace. L'innovation produit portée par la DSI repose sur une prise de hauteur pour observer le problème initial en embrassant un spectre plus large que celui de l'émetteur du besoin initial. Cette hauteur de prise de vue est possible du fait du placement de la DSI cyber au croisement de plusieurs écosystèmes (industriels, scientifiques, étatiques).

C'est cette place unique qui lui permet d'assurer la dernière dimension de l'innovation présentée par le manuel d'Oslo à savoir l'innovation de processus d'affaires. « Une innovation de processus d'affaires désigne un processus d'affaires nouveau ou amélioré pour une ou plusieurs fonction(s), qui diffère sensiblement des processus d'affaires antérieurs de l'entreprise et qu'elle a mis en œuvre. » C'est le volet de l'innovation qui a été le plus développé par la DSI cyber depuis maintenant deux ans. Les processus introduits permettent un développement et une diffusion des innovations aux organismes demandeurs, mais aussi du fait du rôle de la DSI, à des organismes qui ont des problématiques similaires mais qui n'ont pas encore exprimé leurs besoins. Il s'agit de les informer de l'existence de cette innovation afin de potentiellement la rendre disponible le cas échéant. L'adaptation de l'innovation du processus d'affaire par la DSI permet une rationalisation de l'innovation en évitant les doublons. Cela permet également d'orienter les ressources (humaines et financières) vers des innovations répondant à des besoins précis dans des délais compatibles avec les contraintes opérationnelles.

En conclusion, la présentation de l'innovation au travers des quatre dimensions proposées par le manuel d'Oslo permet de comprendre la nature complexe de ce concept reposant sur des processus précis et détaillés. Il est ainsi possible de mettre en place des métriques et des méthodologies permettant d'intégrer des connaissances issues de disciplines parfois éloignées (comme par exemple la psychologie et les sciences informatiques).

C'est pour répondre aux exigences de l'innovation que la DSI Cyber, la DGA et l'AID mettent en œuvre des dispositifs tels que « cyber defense factory » ou encore les défis CYBER. Au regard du contexte actuel, l'innovation est obligatoire pour comprendre et lutter contre les menaces protéiformes en évolution constante auxquelles la France doit faire face.

DSI Cyber - cellule innovation
Commandement de la cyberdéfense

Hacker les émotions pour accélérer l'innovation

Quand la peur, l'espoir et le mystère deviennent des technologies d'avance

Dans les secteurs sensibles comme la cybersécurité, le quantique ou la défense, l'accélération de l'innovation ne repose pas uniquement sur la maturité technologique. Elle passe aussi par l'activation de dynamiques humaines profondes : les émotions. Loin d'être accessoires, peur, espoir, colère ou fascination deviennent des leviers puissants. Dans une logique d'« innovation confidentielle », ces émotions peuvent même être instrumentalisées pour créer l'asymétrie, nourrir le secret, et maximiser l'effet de surprise.

La guerre cognitive repose justement sur cette dynamique : les décisions humaines sont d'abord émotionnelles, puis justifiées par la logique. Il ne suffit donc pas de démontrer une technologie pour l'imposer. Il faut la faire ressentir, l'ancrer dans une expérience affective. Le pari de l'innovation, dans ces domaines sensibles, est de conjuguer rigueur technique et intensité émotionnelle pour provoquer l'adhésion, la mobilisation, et la propagation.

C'est aussi là que s'exprime pleinement le paradoxe de l'innovation confidentielle : pour émerger, une innovation a besoin d'ouverture, de partage, de mise en lien ; mais pour survivre dans des environnements concurrentiels ou critiques, elle doit conserver un avantage, une opacité stratégique, un territoire encore inexploré.

Asymétrie d'information et sociabilisation : ressentir avant de comprendre, dire sans tout révéler

La première étape de toute innovation réside dans une perception singulière du monde. Ce n'est pas la connaissance factuelle qui distingue l'innovateur, mais la compétence à lire les signaux faibles, à cartographier les situations invisibles pour les autres. Là où certains cherchent à accumuler des données, l'innovateur mobilise une lecture stratégique du terrain, une sorte de carte qu'il est seul à savoir interpréter.

Dans le champ de la cyber, cela peut être une angoisse diffuse devant une vulnérabilité systémique, une frustration face à l'inefficacité de certains protocoles, ou encore une fascination pour une technologie émergente. Cette lecture personnelle permet de créer des liens nouveaux, de tisser des connexions sociales structurantes, qui ouvriront plus tard des trajectoires d'innovation originales.

La guerre cognitive s'infiltre ici : en orientant les récits, en cadrant les discussions, en créant du sens autour d'un projet, l'innovateur devient un opérateur de perception. Il ne transmet pas une information, il fabrique une interprétation du réel partagée.

Mais cette dynamique doit être entretenue avec finesse. Il s'agit d'en dire assez pour susciter l'intérêt, sans détruire le mystère. Cette sociabilisation partielle permet de créer une dynamique de propagation par la curiosité, le désir d'en savoir plus, et l'identification affective à un projet qui émerge.

Stratégie secrète et mystère : construire un projet émotionnellement actif

L'innovation confidentielle invite à organiser le mystère comme une ressource : montrer des signaux faibles, des indices, des avant-goûts, sans révéler le cœur du projet. Cela permet de nourrir une tension positive, de maintenir l'attention, et de laisser le temps à l'énergie collective de croître autour du projet.

Mais encore faut-il savoir où concentrer le secret. C'est ici qu'intervient la notion d'ADN du projet : chaque acteur doit identifier son territoire d'excellence, là où il est unique. C'est sur cette zone — qu'elle soit technique, culturelle ou opérationnelle — que l'on concentre la confidentialité.

Des approches comme les skunk works (cellules d'innovation autonomes) permettent de protéger cette dynamique. En France, il est d'usage fréquent de présenter des fonctionnalités plutôt que les technologies elles-mêmes, ce qui permet à la fois de susciter l'adhésion des utilisateurs tout en évitant la divulgation de l'innovation profonde.

Effet de surprise et propagation : créer le basculement

La sortie du secret est une étape cruciale. Loin d'être une simple communication produit, elle devient une mise en scène affective. L'objectif n'est pas seulement de dire « voici notre solution », mais de créer un moment de bascule :

« Pourquoi personne n'avait pensé à ça ? »
« C'est évident maintenant qu'on le voit. »

L'effet de surprise est d'autant plus fort qu'il s'adresse à des attentes latentes, à des intuitions préexistantes. On ne convainc pas par la preuve technique, mais par la résonance émotionnelle. Le timing de révélation est donc stratégique : c'est une opération cognitive structurée, une opportunité de capturer l'attention par l'étonnement.

Un exemple emblématique de cette dynamique est celui de Xavier Niel, que j'ai eu l'occasion d'interviewer. Lorsqu'il a lancé le forfait mobile à 2 € via Free, il a pris tout le marché de court. Ce n'était pas seulement une innovation de prix ou de business model : c'était une opération psychologique volontaire, qui a déclenché une onde émotionnelle — chez les clients, chez les concurrents, dans l'écosystème. L'effet de surprise a permis une propagation instantanée, alimentée par l'émotion et le récit de la transgression.

C'est alors que commence la propagation sociale et symbolique du projet : on passe du cercle des initiés à celui des premiers adopteurs, puis des relais d'influence. Chaque vague amplifie l'effet de surprise initial, renforcé par le capital émotionnel accumulé. Ce n'est pas seulement le projet qui se diffuse, c'est l'émotion qui l'accompagne qui rend la diffusion virale.

Émotions + technologies : un multiplicateur d'impact

Il est temps d'assumer que l'innovation n'est pas neutre. Elle n'est pas un simple agencement logique d'ingénierie et de financement. Elle est une aventure humaine. Et dans cette aventure, les émotions ne sont pas des parasites à réguler, mais des moteurs à cultiver.

Dans le cyber, cela signifie :

- Oser partir d'une peur pour concevoir une protection radicalement nouvelle.
- Canaliser une colère pour détruire un statu quo obsolète.
- Propulser une vision inspirante en jouant sur le mystère et l'envie d'en être.

Les émotions mettent en scène la technologie, la rendent lisible, désirable, et parfois redoutable. Elles sont un multiplicateur d'impact, parce qu'elles parlent le langage des humains.

Et c'est sans doute là que se trouve la clé de l'innovation confidentielle : oser ressentir avant de montrer, protéger avant d'expliquer, surprendre plutôt que convaincre.

Résumé du framework : asymétrie, secret, accélération

L'innovation confidentielle repose sur un enchaînement stratégique en trois temps :

1. Créer une asymétrie d'interprétation : en développant une lecture singulière du contexte, l'innovateur prend de l'avance non sur les faits, mais sur leur sens. Il construit une carte que d'autres ne savent pas encore lire.
2. Structurer un projet secret et différenciant : en identifiant son ADN unique, en dissimulant ce qui compte (la technologie, les compétences, la méthode) derrière des fonctionnalités visibles, et en cultivant le mystère, il protège son avantage.
3. Activer l'effet de surprise comme accélérateur : en orchestrant la révélation au bon moment, avec une mise en scène affective forte, il déclenche la propagation par l'adhésion émotionnelle, jusqu'à créer un basculement perceptif.

Ce triptyque offre une boussole pour celles et ceux qui souhaitent innover en terrain stratégique, là où la technologie seule ne suffit pas.

Benoît WINTREBERT
INRIA
Directeur anticipation stratégique

Face à l'incertitude : inventer l'avenir en travaillant sur les modèles mentaux

L'enjeu de l'incertitude

Depuis quelques années, l'incertitude s'est imposée comme un thème central du débat public. Elle est sur toutes les lèvres, dans les discours politiques, les plans stratégiques, les salles de réunion. Aux incertitudes anciennes s'ajoutent des bouleversements inédits : pandémie mondiale, retour de la guerre en Europe, remise en cause des équilibres politiques, inflation oubliée puis brutalement revenue, contestation croissante des institutions, fragmentation de la société nouvelles tensions géopolitiques, fragilisation du commerce mondial, effets disruptifs de la technologie.

La liste est longue, et elle ne cesse de s'allonger. L'avenir paraît de moins en moins prévisible, et cette impression diffuse affecte toutes les sphères de la société : l'économie, la politique, la finance, l'action publique et la vie quotidienne.

L'incertitude n'est pas simplement une absence d'éléments factuels. Elle est liée à une autre réalité, plus profonde : la fragilisation des modèles sur lesquels nous avons longtemps construit notre compréhension du monde. Les modèles sont les représentations individuelles et collectives de notre métier, de notre mission, de la raison d'être de notre organisation, de son modèle d'affaires mais aussi de la société dans laquelle nous vivons. C'est un ensemble de croyances que nous avons développées sur le monde. Ces modèles sont individuels (ce que je crois, par exemple, sur comment on gère une équipe), collectifs (les croyances partagées des agents d'une collectivité territoriale sur leur mission, celles d'une profession ou d'une entreprise) et sociétaux (croyances de la population sur les dangers et les enjeux). Les modèles constituent des points de repère pour la prise de décision. Ces modèles — explicites ou implicites — permettent aux individus, aux groupes et aux organisations de donner du sens à ce qu'ils vivent, de prioriser, de décider. Ce sont des croyances partagées sur notre métier, notre mission, le rôle de l'État, l'organisation de la société. Ils structurent le collectif car ils offrent une règle du jeu qui rend prédictible le comportement de chacun et définit ce qui marche et ne marche pas.

Le bouleversement de ces modèles entraîne la disparition de points de repères, et donc un désarroi qui peut s'avérer anxiogène : on a le sentiment, pas toujours injustifié, de ne plus rien pouvoir contrôler, d'être à la merci des événements, ce qui est d'autant plus désagréable que ces événements sont surprenants, voire insensés. C'est cette perte de sens, notre incapacité à donner un sens à ce que nous vivons, parce que les anciens modèles ne fonctionnent plus et que les nouveaux ne sont pas encore disponibles, qui est véritablement difficile à vivre. Cette difficulté à donner un sens explique aussi pourquoi le collectif est fragilisé : parce que les modèles sont fragilisés, ils ne sont plus partagés. Il n'y a plus de règle du jeu commune. C'est chacun pour soi.

Agir dans l'incertitude

Face à cette réalité, que faire ? Avant tout, accepter l'incertitude. Elle ne disparaîtra pas. Elle est là, durablement. C'est une donnée du monde contemporain. L'enjeu n'est donc pas tant de la réduire à tout prix, même si quelques efforts en ce sens peuvent être utiles, que de changer de posture : accepter que, si nous n'avons pas de contrôle sur ce qui peut se produire, nous pouvons

néanmoins contrôler notre manière d'y répondre. Cela suppose de recentrer l'attention sur ce qui reste entre nos mains : notre capacité à nous adapter, à coopérer, à apprendre et créer ensemble. Il ne s'agit plus de chercher la solution idéale en prédisant l'avenir, mais de construire, pas à pas, des réponses collectives.

Cela pointe une dimension importante de l'incertitude : si elle est anxiogène, elle signifie aussi que le futur n'est pas déterminé. Il peut donc être construit. Si des modèles deviennent obsolètes et d'autres les remplacent, cela ne se fait pas tout seul. Quelqu'un doit inventer ces modèles. C'est pour cela que l'incertitude, c'est aussi l'ouverture et l'opportunité. C'est ce qui rend possible l'innovation. Le monde ne peut pas se prédire ? Chouette ! Créons-le !

Et donc opérons un changement de posture : regardons la révolution ouverte par le cyber, et faisons en sorte d'avoir un impact sur cette révolution pour en tirer parti.

Comment faire ? En général, les grands innovateurs réussissent parce qu'ils portent un regard nouveau sur une situation.

Ainsi, Ford n'a pas inventé l'automobile. Quand il lance la Ford T en 1908, le marché existe depuis au moins vingt ans. Il y a déjà de nombreux constructeurs. Sa véritable innovation est d'inventer la voiture pour tous. Autrement dit, il change le modèle mental de la voiture : auparavant, elle était un objet de luxe pour les riches. Avec la Ford T, elle devient l'outil de tout le monde. Les observateurs et les experts sont surpris, voire choqués, mais quelques années après, le modèle de Ford est devenu une évidence.

Il faut procéder de même dans le cyber. Mettre en évidence les modèles que cette révolution remet en question, et imaginer de nouveaux modèles pour en tirer parti. Par exemple, le cyber abaisse les barrières à l'entrée : alors qu'auparavant il fallait de gros moyens pour disposer d'une infrastructure permettant d'agir sur ses adversaires, il suffit désormais d'un PC et d'une connexion Internet. Les développements rapides de la technologie permettent l'émergence d'une action low-cost, avec énormément d'impact, ce qui autorise le développement de stratégies du faible au fort. On a vu le même phénomène avec les drones en Ukraine : un drone de quelques milliers d'euros peut détruire un char de quelques millions d'euros. Bien utilisée, la technologie peut parfois rapidement redistribuer les cartes et annuler des avantages chèrement acquis.

Il y a donc un enjeu à dresser un inventaire détaillé des modèles mentaux du domaine pour identifier des sources de faiblesse mais aussi d'innovation. En voici quelques-uns, à titre d'exemples.

Du côté des cibles : beaucoup d'institutions se croient à l'abri des attaques parce qu'elles pensent ne pas représenter une cible importante ou parce qu'elles sont d'utilité publique. C'est le cas des hôpitaux, des universités et des associations, par exemple. « Nous sommes un hôpital, pas une entreprise ou une institution militaire, donc personne ne nous voudra du mal. » C'est oublier que les attaquants vont à la facilité, et ne poursuivent pas nécessairement un agenda moral ou politique.
Du côté des offreurs de solutions, un modèle mental considère la sécurité uniquement sous un angle technique alors que les failles humaines sont souvent les plus importantes. Par exemple, une clé USB oubliée dans la voiture. On pense aussi que plus on ajoute de mesures techniques, plus la sécurité augmente, mais ce n'est pas vrai : un excès de sécurité complexifie le travail des utilisateurs et ceux-ci vont chercher des raccourcis (ex : mots de passes consignés sur un post-it collés à l'écran). La sécurité a un coût marginal croissant, et donc un risque lui aussi croissant.

À l'extrême, un excès de mesures techniques déresponsabilise les utilisateurs qui finissent par se contenter de se conformer aux instructions. Or la grande leçon des changements systémiques comme le mouvement de la qualité lancé par les industriels japonais dans les années 60 est que la réussite passe par la responsabilisation des acteurs à tous les niveaux.

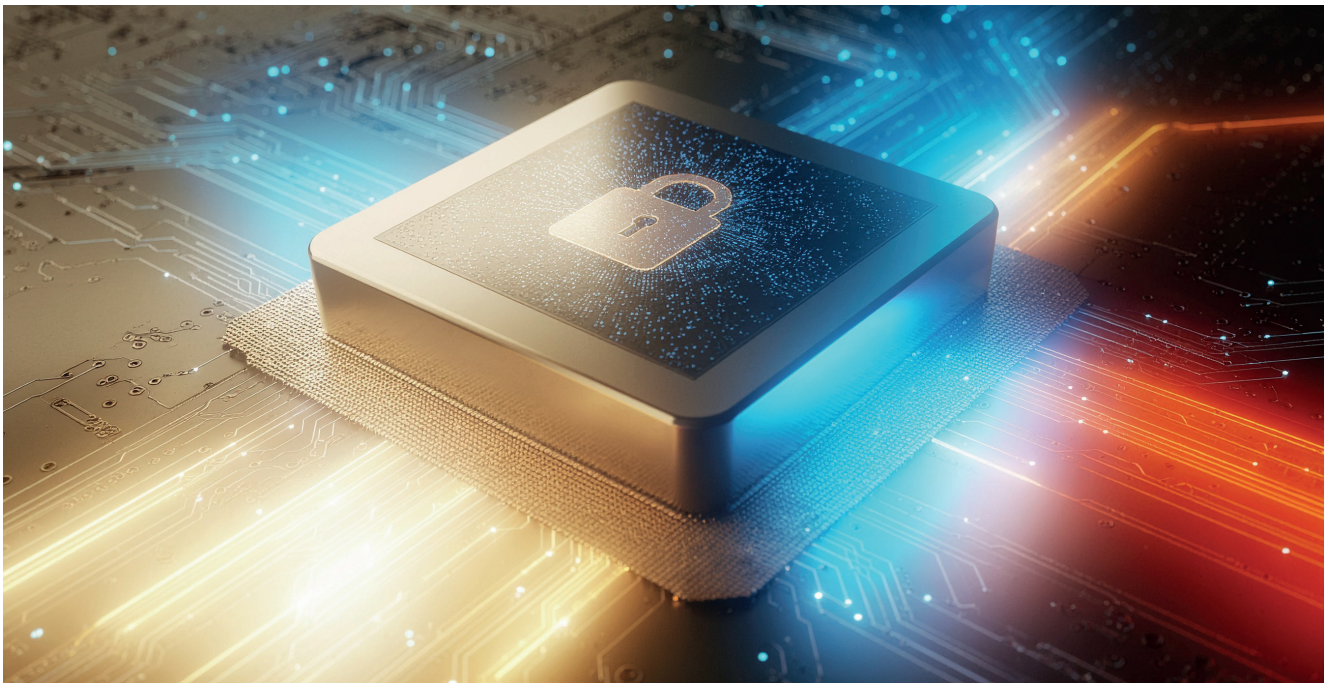
L'incertitude nous déstabilise, mais elle nous pousse aussi à imaginer, à oser, à créer. Elle nous rappelle que nous ne sommes pas des automates, mais des êtres libres, capables d'inventer, ensembles, des chemins nouveaux. En cyber comme ailleurs, la réussite repose sur une fine compréhension de la dialectique entre l'humain et la technologie, et donc sur une méfiance des modèles simplistes du tout-technologie.

Que peut donner cette dialectique ? Difficile de le savoir a priori, car le domaine est en émergence. Comme tout est nouveau, la prime ira à ceux qui peuvent rapidement tester, expérimenter et imaginer des solutions nouvelles.

Il s'agit moins de prédire ce qui se passera que de le construire soi-même. Ici encore Henri Ford, comme tant d'autres innovateurs après-lui, montre le chemin : identifier un modèle contesté, et agir pour le changer. C'est l'essence de l'innovation.

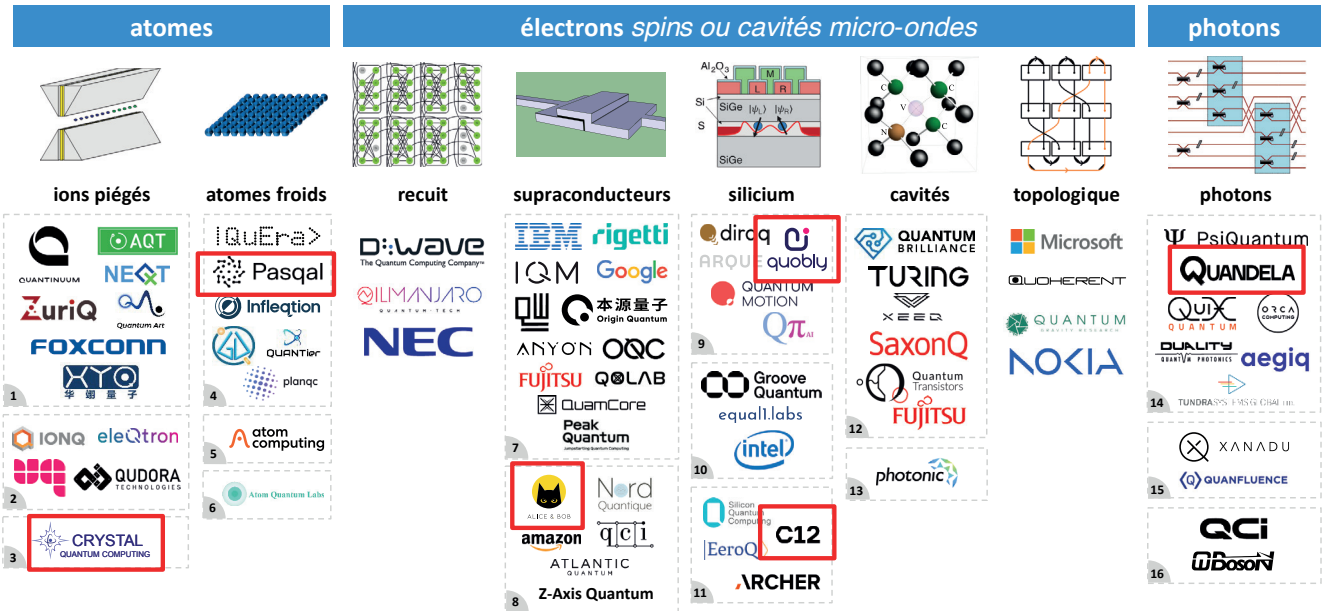
Philippe SILBERZAHN
Chercheur, auteur, conférencier

L'innovation dans l'informatique quantique



L'idée de la création d'ordinateurs quantique remonte aux propositions de Yuri Manin, Paul Benioff, puis de Richard Feynman entre 1979 et 1982. Les premiers ordinateurs quantiques sont arrivés progressivement, d'abord dans les laboratoires académiques. Une centaine d'entre eux ont été construits par des industriels et startups depuis une quinzaine d'année. Ils sont pour la plupart disponibles dans le cloud. On peut les tester avec des algorithmes quantiques à petite échelle, les premiers ayant été créés entre 1992 et 1996. L'avantage quantique attendu est une combinaison d'accélération de la vitesse de résolution de problèmes et d'augmentation de la qualité des résultats.

Malgré tout, les ordinateurs quantiques à même de surpasser les meilleurs ordinateurs classiques ne sont pas encore véritablement là. Environ 90 sociétés dans le monde ont l'ambition de les créer, comprenant quelques grands groupes informatiques tels qu'IBM et Google et des myriades de startups dans près de 20 pays, dont 6 en France (schéma ci-dessous). Elles doivent surmonter d'énormes défis scientifiques et technologiques, le principal étant lié au caractère imparfait des qubits qui sont le support de l'information dans ces ordinateurs. Pour le contourner, il faut mettre en œuvre des dispositifs de correction d'erreur qui augmentent de plusieurs ordres de grandeur le nombre de qubits nécessaires.



Les meilleurs ordinateurs quantiques actuels sont composés de quelques centaines de qubits. Pour pouvoir résoudre les problèmes de simulation chimique, de machine learning ou de combinatoire des entreprises, il faudra disposer d'environ une centaine de milliers à des dizaines de millions de qubits dits physiques, selon leur type. C'est un défi considérable. S'y ajoute celui du prix de ces machines et de leur consommation énergétique. Ce sont des inconnues à ce stade même s'il est possible de s'en faire une idée. L'écart entre les machines les plus sobres et les moins sobres pourrait être de deux ordres de grandeur !

Les processus d'innovation en œuvre dans ce marché sont assez particuliers à plusieurs égards.

Tout d'abord, l'incertitude scientifique prédomine aussi bien au niveau du matériel que des algorithmes. Les acteurs repoussent les limites expérimentales de ce l'on peut contrôler à l'échelle nanoscopique (photons, électrons, atomes) mais on n'a pas encore idée de tous les obstacles qui seront rencontrés sur ce chemin et de la manière de les contourner.

L'innovation est arrivée d'abord sur les algorithmes bien avant que le matériel permettant de les exécuter soit disponible. C'est un phénomène relativement rare dans les précédentes révolutions numériques (micro-informatique, Internet, smartphones, intelligence artificielle). Malgré leur nombre, on ne dispose pas encore d'assez d'algorithmes à même d'apporter une accélération pratique du temps de calcul. Le paradigme de pilotage des ordinateurs quantiques est très différent de celui des ordinateurs classiques. Il s'appuie ainsi sur le principe d'interférences, un concept connu dans l'électronique analogique. La créativité scientifique est encore en devenir pour créer des algorithmes utiles.

Malgré cette maturité en devenir, les positions de marché se prennent déjà, notamment dans les briques logicielles stratégiques de la chaine de valeur du calcul quantique. Ces briques se situent autour des frameworks de développement (Qiskit d'IBM, Braket d'Amazon, etc.), des compilateurs (comme celui de Classiq), de la correction d'erreurs (comme chez Riverlane) et des infrastructures de cloud (comme chez AWS et Microsoft).

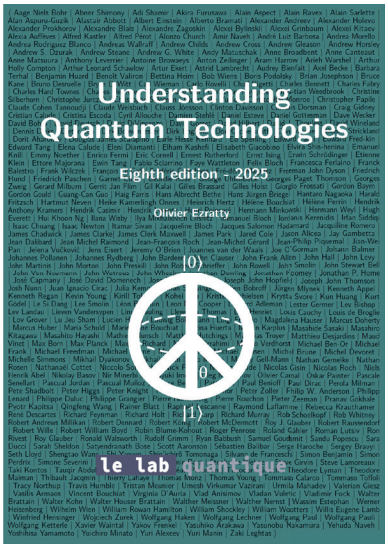
Les gouvernements investissent dans le domaine comme on ne l'a jamais vraiment vu par le passé, l'espoir étant de capter une partie de la valeur de ce nouveau marché prometteur. C'est aussi lié à l'aspect dual du calcul quantique et sa capacité potentielle dans le domaine de la cryptanalyse, même si son caractère offensif est limité par le déploiement à venir de la cryptographie post-quantique « classique » qui permettra de résister aux ordinateurs quantiques du futur. Des programmes d'équipement civils et militaires ont ainsi été lancés par la puissance publique des deux côtés de l'Atlantique. En Europe, c'est l'équivalent d'un véritable Small Business Act qui est en place, comme avec les commandes liées au programme EuroHPC (civil, Européen, couvrant 7 pays dont la France) et ProQCima (militaire, géré par la DGA en France). Cela contribue au financement non dilutif des startups du domaine qui en ont bien besoin pour supporter leurs efforts de R&D au long cours, en complément des financements plus traditionnels venant du capital risque.

Enfin, il s'agit surtout d'un marché professionnel. On ne peut pour l'instant pas s'attendre au développement d'un volet grand public des usages du calcul quantique. Il ne s'agit d'ailleurs pas de remplacer des infrastructures de calcul existantes mais plutôt de les compléter. Le calcul quantique va surtout devenir une nouvelle brique clé du calcul scientifique au même titre que les GPU.

#QEI
the quantum energy initiative

Olivier EZRATTY
Quantum Energy Initiative
Co-Founder

EPITA
Enseignant



Olivier Ezratty est l'auteur de l'ouvrage de référence « Understanding Quantum Technologies » dont la 8ième édition a été publiée le 29 septembre 2025. Il est diffusé gratuitement en format électronique et couvre tous les aspects des technologies quantiques dont plus d'une centaine de pages sur les communications et la cryptographie quantique et post-quantique ainsi qu'une description des écosystèmes quantiques de plus de 40 pays.

Brevet et cybersécurité : quelles sont les bonnes pratiques ?

Jean-Nicolas ROBIN

Bertrand Ermeneux

Cet article à vocation pratique est rédigé par deux avocats qui accompagnent des entreprises, organismes para-public, centres de recherches et autres depuis de longues années.
Les quelques réflexions qui suivent sont le fruit de l'expérience et de l'observation des comportements des organismes.

Les bonnes pratiques en matière de brevet et plus généralement de propriété intellectuelle

A l'instar de Monsieur JOURDAIN qui fait de la prose sans le savoir, de nombreuses entreprises font de la propriété intellectuelle sans le savoir.
Plus exactement, elles développent au cours de leur vie des technologies et du savoir-faire qui bien souvent sont ignorés.
Ces richesses immatérielles peuvent faire l'objet de fuites ou de détournement alors qu'elles mériteraient d'être identifiées et valorisées à deux niveaux :

- au cours de la vie d'une entreprise, notamment par des licences qui pourraient être consenties,
- En cas de cession d'une entreprise ou d'une partie des actifs. Ces richesses immatérielles permettraient d'optimiser la valorisation

Que faire ?
Il est conseillé de mettre en place le processus : identifier/dater/protéger/valoriser.

1. Identifier son patrimoine PI, le dater et en assurer la confidentialité

L'entreprise devra opérer une sorte d'introspection pour identifier quels sont ses avantages concurrentiels présents et futurs. Ceux-ci sont multiples : technologie/secret de fabrique/logiciel/base de données/savoir-faire.
A ce stade, il est opportun que l'entreprise opère des « arrêts sur image » réguliers, c'est-à-dire qu'elle se pose à intervalles réguliers (en moyenne entre 1 et 4 fois par an) pour qu'elle constate les développements qu'elle a opérés et ce tous azimuts. Le but est de prendre conscience des richesses qui sont développées.

2. Dater sa propriété intellectuelle quelle qu'en soit sa nature

Il est nécessaire que l'entreprise puisse justifier de la titularité de ses droits de propriété intellectuelle en pouvant arguer :

- d'un contenu certain,
- d'une date certaine.

Les outils sont nombreux : enveloppe Soleau ; cahier de laboratoire ; dépôt d'un titre de propriété intellectuelle ; dépôt APP ; dépôt chez un Commissaire de justice (autrefois dénommé Huissier de justice) ; dépôt chez un Notaire.

3. Décider d'une protection par brevet ou par secret

Un brevet pourra être déposé aux conditions classiques de nouveauté et d'activité inventive. Il confère une exclusivité pendant 20 ans sur les territoires visés par le dépôt. Il permet d'agir en contrefaçon et d'étoffer le patrimoine de l'entreprise.

Il présente néanmoins l'inconvénient de la divulgation. Parfois il sera plus opportun d'opter pour la protection pour le secret à la condition que ce secret ne soit pas aisément accessible, qu'il revête une valeur commerciale et qu'il fasse l'objet de mesures de protections raisonnables.
Le secret est généralement préféré au brevet notamment pour le savoir-faire et les process de fabrication.

4. Valoriser

Les précédentes étapes ayant été franchies, il sera possible de concéder des licences de brevet ou de savoir-faire afin d'en tirer des revenus. Usuellement, les quatre points de négociation sont les suivants : le domaine d'application pour lequel la techno est concédée, la durée, le montant des royalties et la zone géographique.
Ce patrimoine PI permettra également une valorisation en cas de cession totale ou partielle de l'entreprise.

Propriété intellectuelle et cybersécurité : quels enjeux pour le droit des brevets ?

La cybersécurité constitue aujourd'hui un champ stratégique majeur, à la croisée des intérêts économiques, technologiques et souverains. Les innovations dans ce domaine se sont multipliées au cours des dernières décennies, qu'il s'agisse de protocoles de chiffrement, de systèmes d'authentification, de solutions de détection

d'intrusion ou de gestion des identités numériques. Cette dynamique soulève naturellement la question de la protection de ces innovations, notamment à travers les instruments de la propriété intellectuelle. Parmi ceux-ci, le droit des brevets occupe une place centrale, bien que sa mise en œuvre dans ce secteur soulève des interrogations spécifiques.
Cet article se propose d'examiner les enjeux liés à la protection des innovations en cybersécurité par le droit des brevets, en exposant les apports du régime actuel tout en identifiant les zones de complexité, dans une approche pragmatique et constructive.

1. La propriété intellectuelle comme levier de valorisation de l'innovation en cybersécurité

Les outils de propriété intellectuelle offrent aux acteurs de la cybersécurité un arsenal juridique permettant de valoriser et protéger leurs créations. Plusieurs régimes peuvent être mobilisés de manière complémentaire :

- Le droit des brevets permet de protéger les inventions techniques nouvelles, impliquant une activité inventive et susceptibles d'application industrielle. Ce régime peut s'appliquer, sous conditions, aux méthodes de cybersécurité dès lors qu'elles revêtent un caractère technique.
- Le droit d'auteur protège automatiquement les codes sources des logiciels, ce qui permet de garantir une première couche de protection des outils de cybersécurité développés en interne.
- Le secret des affaires offre une protection utile, en particulier pour les méthodes ou algorithmes que l'on souhaite garder confidentiels, en complément ou en alternative au brevet.
- Les dessins et modèles, marques ou bases de données peuvent également être mobilisés pour protéger d'autres aspects des produits numériques, même si leur rôle est plus accessoire dans ce domaine.

Dans un secteur où la recherche et le développement sont particulièrement soutenus, le brevet joue un rôle essentiel de reconnaissance et de valorisation des efforts d'innovation. Il permet de sécuriser les investissements en R&D, de renforcer la compétitivité des entreprises et d'encourager les partenariats technologiques, notamment dans les phases d'industrialisation.

2. La brevetabilité en cybersécurité : entre exigences techniques et sécurité juridique

Le droit des brevets est, par nature, ouvert aux innovations en cybersécurité, dès lors que celles-ci remplissent les critères classiques de brevetabilité. Ainsi, des procédés cryptographiques, des méthodes de filtrage, ou des techniques de vérification d'intégrité peuvent parfaitement faire l'objet d'une demande de brevet, sous réserve qu'ils présentent une dimension technique au-delà de leur caractère purement abstrait ou algorithmique.
Il convient toutefois de noter que l'appréciation de la brevetabilité peut varier selon les offices, en particulier pour les inventions logicielles. En Europe, l'OEB exige la démonstration d'un effet technique supplémentaire. Aux États-Unis, la jurisprudence Alice Corp. v. CLS Bank a instauré une approche en deux étapes pour évaluer si une invention logicielle repose sur une idée abstraite et si elle met en œuvre des moyens techniques suffisants pour mériter une protection.

3. Cybersécurité et droit des brevets : enjeux économiques et stratégiques

La cybersécurité constitue un domaine sensible, au cœur des politiques de souveraineté numérique. Dans ce contexte, le dépôt et la maîtrise des brevets sont devenus des leviers d'influence stratégique.
Le brevet peut également jouer un rôle dans la gouvernance technique de l'Internet et des réseaux numériques. Les technologies de cybersécurité sont souvent intégrées à des standards ou protocoles, pour lesquels la question des brevets essentiels se pose. Les mécanismes de licence dite FRAND permettent de concilier la protection de l'innovation avec l'accessibilité aux standards.

4. Articulation entre brevet et secret en matière de sécurité des systèmes d'information

Le brevet implique une divulgation technique détaillée de l'invention, ce qui peut susciter des interrogations en matière de sécurité. Toutefois, cette exigence constitue également une garantie de transparence et de diffusion du savoir. L'entité devra donc arbitrer entre :

- Le brevet qui confère une exclusivité sur un ou plusieurs territoire(s) défini(s) pendant 20 ans avec comme avantage cette exclusivité et la transparence,
- Le secret qui, comme son nom l'indique, ne fera pas l'objet d'une divulgation avec comme avantage la sécurité de la solution technique et comme inconvénient l'absence d'exclusivité et le manque de transparence.

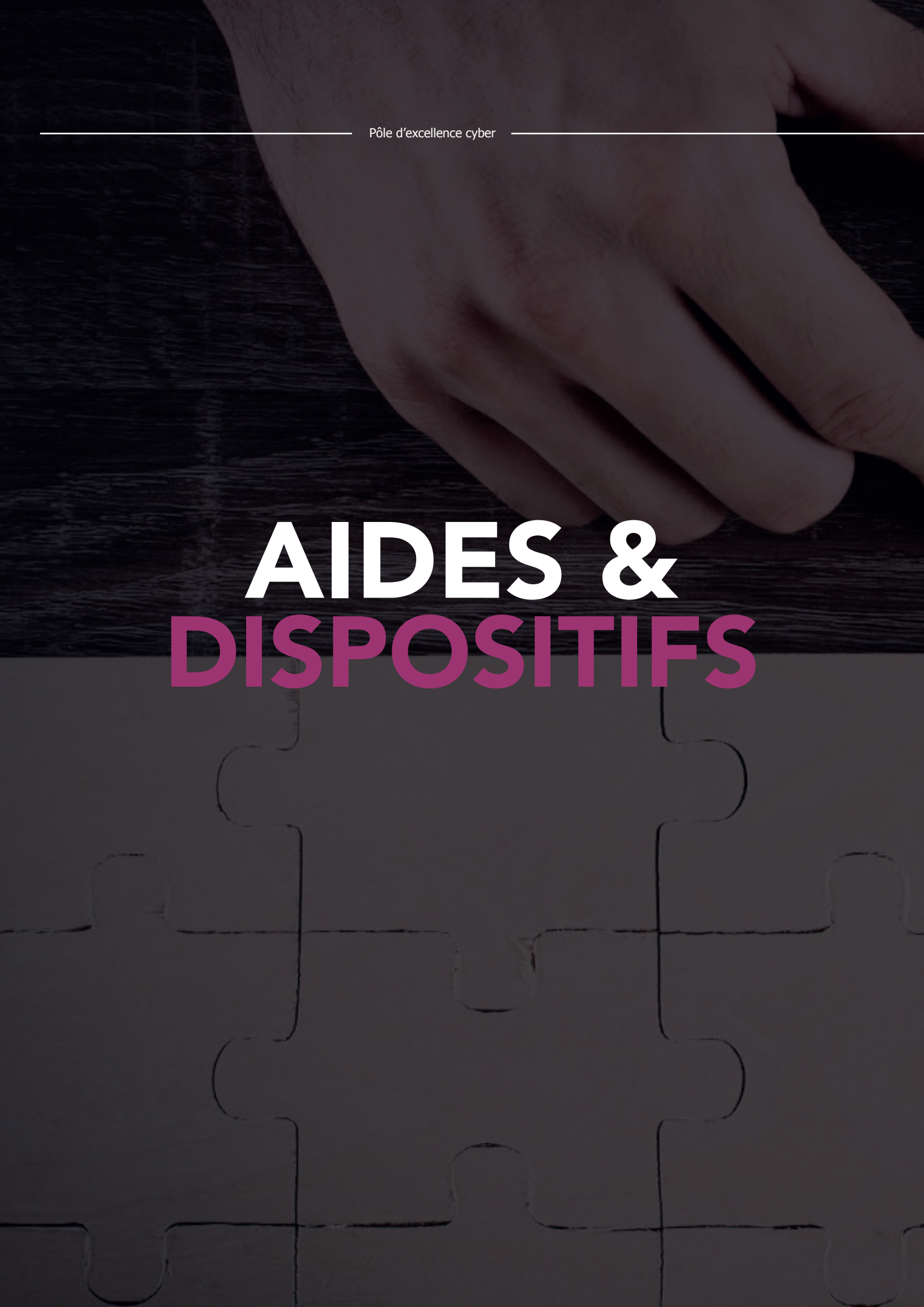
Le droit des brevets ne se suffit pas à lui seul pour sécuriser juridiquement une solution de cybersécurité. Il doit être articulé avec d'autres dispositifs contractuels et réglementaires. Cette approche intégrée permet de construire une chaîne de confiance juridique, qui combine innovation protégée, sécurité des échanges et conformité.

Conclusion

Le droit des brevets constitue un levier précieux pour accompagner l'innovation en cybersécurité. Il permet de valoriser les efforts de recherche, de structurer la stratégie industrielle des entreprises, et de soutenir les politiques publiques en matière de souveraineté numérique. Si certaines adaptations ou précautions sont nécessaires, le cadre juridique actuel offre des outils pertinents, à condition d'en faire un usage éclairé et stratégique.

AVOXA
SOCIÉTÉS D'AVOCATS

Jean-Nicolas ROBIN
Bertrand EMENEUX
AVOXA
Avocats associés



AIDES & DISPOSITIFS

Comment accompagner le passage à l'échelle des startups innovantes ?

Le Poool x La French Tech Rennes Saint-Malo est l'association de référence pour les startups et les acteurs de l'innovation en Ille-et-Vilaine. Opérateur de la dynamique French Tech, nous accompagnons les entrepreneurs innovants à chaque étape de leur parcours, du premier prototype jusqu'à l'internationalisation. Notre mission : faire grandir les projets, connecter les talents et accélérer la transformation économique du territoire.

Nous fédérons un écosystème de près de 350 startups et scale-ups, en lien étroit avec les grands comptes, les acteurs publics et le monde académique. Labellisés « Capitale French Tech », nous occupons une position stratégique pour valoriser les technologies de nos membres et comprendre les enjeux de développement des startups, dans tous les domaines, en particulier celui de la Cyber Sécurité, domaine d'excellence en bretagne.

Le Poool encourage la création de toutes les startups innovantes avec son incubateur, et spécialement dans la cybersécurité avec le Cyber Booster.
Notre cœur de métier s'est d'abord construit autour de l'accompagnement à l'émergence : de l'idéation jusqu'aux premières étapes de la création. Grâce à notre offre d'incubation et à notre proximité avec les écoles, laboratoires et centres de recherche, nous avons contribué à faire naître des projets technologiques à fort potentiel dans tous les domaines. Pour ce faire, nous aidons les entrepreneurs à passer de l'idée au marché, en les soutenant dans leurs premières phases de structuration, de financement et de commercialisation.

Etant donné le poids de la cyber sécurité dans la région, de nombreuses startups cyber se sont créées ces dernières années, et nous avons fait le choix d'être encore plus volontaristes sur le domaine en participant à la création du Cyber Booster, un dispositif d'incubation national, localisé à Rennes et à Paris qui vise à prendre en compte encore mieux les projets de création en cybersécurité, avec un réseau de mentor, des ressources et des experts connaissant parfaitement ce domaine.

Le Poool fédère et met en relation l'ensemble des acteurs de l'innovation en créant la communauté de l'innovation et de l'entrepreneuriat.
En effet, l'écosystème du Poool rassemble près de 600 membres, startups, scaleups ainsi que des entreprises partenaires, dans tous les domaines. Labellisé « capitale French Tech », nous occupons une place de premier rang dans la mise en relation B2B des start-ups et scale-ups de notre écosystème avec le reste de ses membres constitués des grands groupes privés et d'acteurs publics. Nous organisons régulièrement des événements de mise en réseau et facilitons la rencontre en B2B pour valoriser les technologies développées par nos membres. Le programme "Je choisis la French

Tech" constitue une opportunité pour notre écosystème en portant comme ambition de doubler les achats des grands groupes et acteurs publics auprès des start-ups d'ici 2027. Cette plateforme nous permet de mesurer les enjeux de l'écosystème, d'en observer les forces (comme la cyber sécurité), mais également les points d'amélioration.

Des startups qui émergent, mais qui sont peu nombreuses à casser le plafond de verre situé entre 1 et 4 millions d'€.
Si les outils d'émergence fonctionnent à plein (nous voyons plus de 20 nouveaux projets par mois) seuls 15% des projets créés de l'écosystème réalisent plus de 500K€ de CA annuel et celles qui ont dépassé le seuil de 1M€ seront peu nombreuses à passer les 4Md d'€, seuil significatif pour les investisseurs. Ce passage à l'échelle correspond à une période de transition d'une phase de croissance initiale vers une phase de croissance soutenue où les start-ups cherchent à étendre leur impact, leur portée et leur taille et doivent adapter leur fonctionnement. Après un travail d'enquête sur la base des milliers de projets accompagnés depuis quarante ans, deux raisons ressortent : l'ambition initiale (quelle est elle ? Comment l'influencer), et l'excellence de l'exécution sur quelques domaines clés : la vision internationale, la culture produit, le recrutement des meilleurs, la cyber et l'IA.

La création récente du parcours ambition : une réponse au défi du passage à l'échelle des start-ups à fort potentiel pour bâtir les succès de demain.
Ce parcours s'adresse à toutes les entreprises innovantes en développement, qui ont trouvé leur marché avec un chiffre d'affaires supérieur à 400k€ ou les entreprises ayant réalisé une levée de fonds significative et supérieure à 1M€. Pour jouer sur le levier de l'ambition, nous proposons une programmation attractive constituée de nombreux retours d'expérience d'entrepreneurs ou d'experts inspirants. Ces rencontres, souvent intimes entre une personnalité qui a une trajectoire hors norme ou qui a trouvé les clés d'un problème, sont très transformantes pour les membres du programme. Le programme inclut également et un suivi personnalisé des PME pour aborder leurs enjeux business et faciliter l'internationalisation de leur solution. Le parcours intègre notamment un volet Cyber&IA pour répondre aux nouveaux défis posés par l'économie du numérique et les risques associés.

Pour incarner ce parcours, valoriser les entrepreneurs et attirer les talents, un nouveau lieu : la CyberPlace.
A l'instar du campus cyber parisien, la métropole de Rennes s'est dôté d'un lieu-phare avec la Cyberplace, située à Cesson-Sévigné, qui facilite l'identification et le rassemblement des acteurs de la cybersécurité. Rassemblant sur le même site, une pépinière spécialisée en cyber, des startups cyber, le pôle d'excellence Cyber ainsi qu'une variété d'entreprises, ce bâtiment devient le cocon naturel d'un grand nombre d'animations. Présent dans ces locaux, nous cherchons à y renforcer les synergies et les opportunités de se rencontrer grâce à une offre événementielle qui aborde les sujets de l'innovation et de l'entrepreneuriat. Nous avons choisi de dédier ce lieu à l'accélération de croissance des start-ups que nous accompagnons, afin d'incarner notre ambition pour en faire « the place to grow ».

LE POOOL

Daniel GERGÈS
Directeur général
Le PoooL

Créer des champions européens de la cybersécurité : une impulsion collective pour une ambition globale

Dans un contexte où les tensions géopolitiques et les cybermenaces s'intensifient, la cybersécurité est devenue un pilier fondamental de la résilience européenne. Plus qu'un simple enjeu technologique, elle touche à la stabilité de nos institutions, à la continuité de nos activités économiques et à la protection de nos modèles démocratiques. Pourtant, l'Europe reste encore très dépendante d'acteurs non européens qui bénéficient d'une place dominante sur le marché, de l'effet plateforme et d'une capacité industrielle difficile à concurrencer. Face à ce constat largement partagé, il devient impératif d'ouvrir collectivement la voie pour faire émerger des alternatives européennes.

Cette ambition pour l'innovation européenne en cybersécurité repose sur quelques principes simples mais exigeants. Parmi les acteurs clés capables d'apporter cette innovation, les startups jouent un rôle fondamental. Créer une startup cyber aujourd'hui, c'est évoluer dans un environnement riche, parfois complexe, souvent saturé. C'est pourquoi nous sommes profondément convaincus que toute démarche entrepreneuriale dans ce secteur doit commencer par une attention sincère et rigoureuse aux besoins du terrain et une logique de co-construction.

Cela signifie aller à la rencontre des utilisateurs pour comprendre leurs contraintes opérationnelles et identifier les zones de friction dans leur quotidien. Dans un contexte de rationalisation des solutions de cyber qui donne l'avantage aux plateformes déjà présentes, seule une solution qui apporte une réponse claire à un problème bien identifié peut espérer faire sa place. L'écoute des utilisateurs ne doit pas être une étape ponctuelle, mais un réflexe permanent, travaillant dès les premières phases avec des partenaires engagés et des décideurs prêts à challenger les projets. Au sein de CyGO Entrepreneurs, nous développons cette culture de l'itération au cœur des processus, permettant de mieux calibrer la réponse aux attentes et de créer des solutions véritablement pertinentes.

Une fois l'approche validée avec les premiers design partners et les early adopters, il est essentiel de savoir positionner l'offre de manière claire et lisible pour l'ensemble des acteurs de l'écosystème. Sur un marché encombré, seul un positionnement affûté et réellement différenciant, qui démontre la valeur concrète créée pour le client, peut trouver sa place. Les fondateurs doivent pouvoir articuler simplement leur vision : à quel besoin répondons-nous ? pour qui ? en quoi sommes-nous différents ? Il ne s'agit pas de surpromettre, mais de construire une proposition de valeur cohérente, mesurable et connectée au réel.

Enfin, l'impact réel d'une solution dépend de sa capacité à conquérir des clients. Dans les projets cyber, l'expertise technique est indispensable et souvent au cœur de la création des startups, mais elle ne peut porter seule l'ambition d'un projet. Pour faire émerger des acteurs solides, il est crucial que les fondateurs couvrent l'ensemble des compétences clés, notamment celles liées au go-to-market, à l'engagement des premiers clients et à la vision commerciale. Nous plaidons pour une approche équilibrée, où la technologie et la stratégie marché avancent de concert dès les premiers jours du projet.

Penser à l'échelle du marché, c'est aussi envisager l'international dès les premières étapes. La France, comme d'autres pays européens, peut parfois être un piège : son marché vaste et dense offre de nombreuses opportunités, ce qui incite souvent à s'y attarder trop longtemps. Pourtant, devenir un acteur global implique de ne pas considérer l'international comme une simple option secondaire. Le marché évolue rapidement, et il est crucial de s'imposer rapidement sur plusieurs territoires. Par définition, un acteur global est un acteur international. Arriver en retard sur ces marchés, c'est risquer de laisser d'autres concurrents occuper durablement la place. Pour s'assurer d'être le leader, il faut donc agir vite et s'implanter stratégiquement sur plusieurs pays.

À ce titre, la question du développement européen reste posée. Le marché européen demeure trop fragmenté pour offrir, en l'état, une trajectoire fluide aux startups. Plusieurs d'entre elles choisissent aujourd'hui de viser directement les États-Unis, malgré les risques et les coûts, car le marché y est plus unifié, plus ouvert à l'innovation et surtout beaucoup plus grand. Pour construire de véritables champions européens, il est souhaitable de pouvoir créer, à l'échelle du continent, des chemins plus clairs, plus connectés, permettant aux startups de grandir d'un pays à l'autre avec plus d'agilité. Cela passe sans doute notamment par une meilleure articulation entre écosystèmes, une coordination renforcée, une régulation plus globale ou encore un financement à la hauteur des enjeux.

Enfin, nous sommes convaincus que l'un des leviers les plus puissants est le collectif. L'émergence d'une alternative européenne en cybersécurité ne pourra se faire que si nous sommes capables de décloisonner les approches, de créer des liens entre ceux qui entreprennent, ceux qui décident, ceux qui financent, ceux qui opèrent. Ce besoin de collaboration traverse tous les stades d'un projet : de l'idéation à la mise sur le marché, du prototypage à l'adoption.

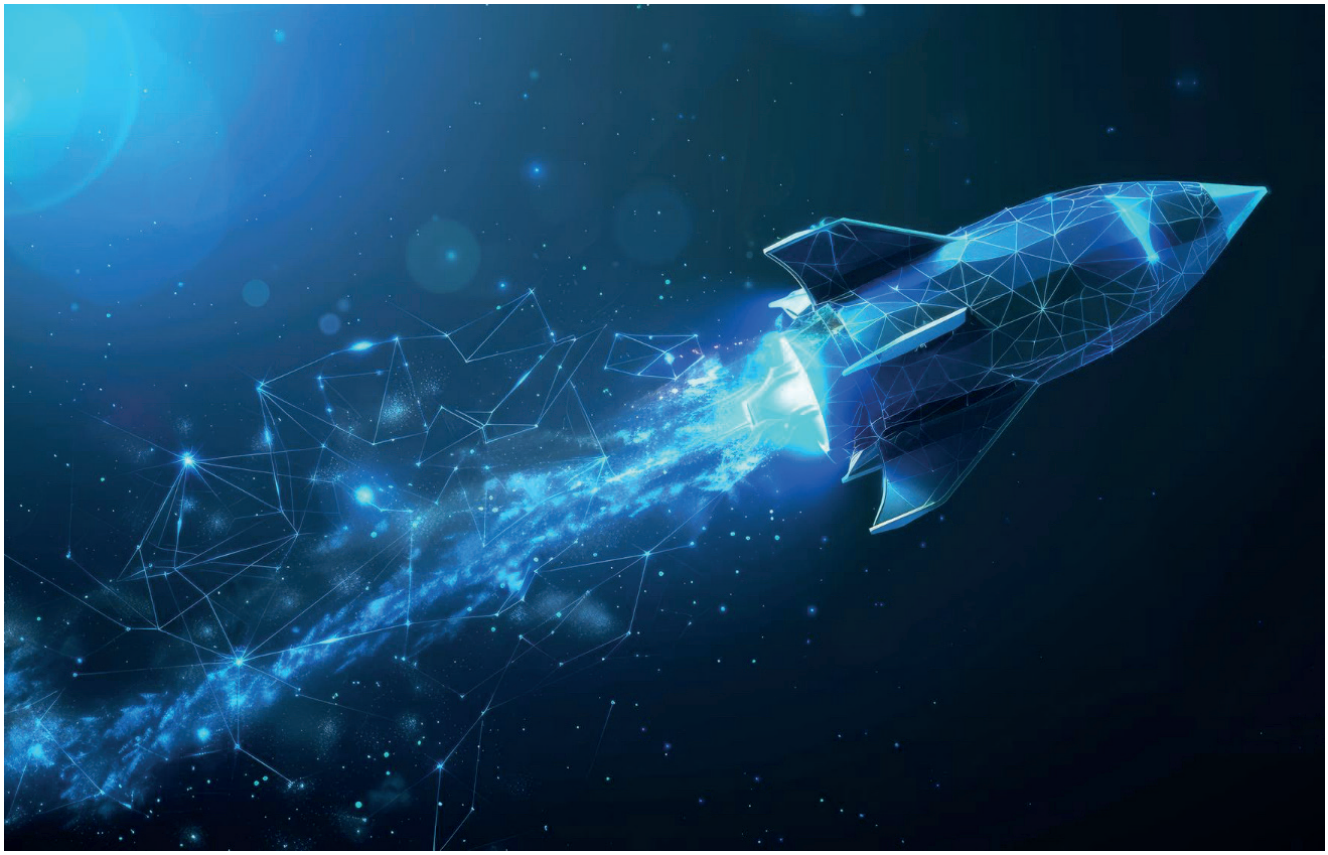
Créer des startups cyber capables de devenir des acteurs globaux, c'est une ambition collective, exigeante, mais accessible si nous savons nous appuyer sur les bonnes dynamiques, les bons réflexes, les bons partenariats. Nous ne manquons ni de talents, ni d'idées. Ce qu'il nous reste à renforcer, ensemble, ce sont les conditions concrètes pour transformer ces idées en solutions robustes adoptées par les organisations. L'émergence de champions européens de la cybersécurité ne relève pas seulement du bon sens ou de la bonne volonté collective ; elle passe avant tout par la concrétisation des bons de commande.

Toutes ces convictions et principes que nous développons ici reflètent pleinement l'approche que nous mettons en œuvre au sein de CyGO Entrepreneurs, le premier startup studio européen dédié à la cyber. Si vous souhaitez contribuer à la création de champions européens, vous êtes les bienvenu.e.s.

CYGO ENTREPRENEURS

Aurélie CLERC
CYGO entrepreneurs
Directrice générale

Six dynamiques qui propulsent l'innovation en cybersécurité



L'innovation en cybersécurité est principalement tirée par six dynamiques systémiques relativement uniques au domaine.

L'évolution constante de la menace

La cybersécurité est souvent perçue comme un poste de coûts. A l'opposé, l'essor démesuré des cybermenaces démontre comment les cyberattaques peuvent être un poste de profits pour les attaquants. C'est ce qui a permis à l'écosystème cybercriminel de se structurer si vite autour d'une chaine de valeur bien définie permettant aux différents acteurs de se spécialiser. Le paroxysme de cette industrialisation étant peut-être les offres de ransomware-as-a-service.

Une croissance aussi rapide et agile de la menace est, avant tout autre, la source principale de croissance de la cybersécurité.

Les méga-trends numériques comme moteurs indirects

Le sous-jacent direct de la cybersécurité est, bien entendu, le numérique. Il est donc naturel que les évolutions des deux soient liées.
Le marché global de la cybersécurité est composé de différents sous-marchés plus hétérogènes qui peuvent être classés en deux catégories : ceux de taille déjà importante, avec une croissance honorable (souvent à deux chiffres) et ceux émergeants, à la taille restreinte, mais avec une très forte croissance. Cette deuxième catégorie est le plus souvent liée à des tendances sous-jacentes du numérique comme l'IA, le Cloud, l'IoT, le Web3 dont les usages explosent amenant d'énormes besoins de sécurité.

L'intelligence artificielle : facteur d'accélération…

L'avènement de l'IA disrupte beaucoup de secteurs en amenant, le plus souvent, une capacité d'optimisation ou de passage à l'échelle. La cybersécurité étant particulièrement sensible à ces problématiques, y appliquer différents modèles d'IA est tout à fait logique. L'arrivée de l'IA générative a renforcé cette tendance.

La première étape (actuelle) consiste principalement en une aide à la décision pour les différents analystes et opérateurs humains. La deuxième vague de l'IA

générative, avec l'agentique, vise à pouvoir actionner automatiquement en fonction des résultats générés (via des agents). Néanmoins, cette deuxième étape est beaucoup plus sensible et difficile à mettre en œuvre avec de nombreux défis autour de l'éthique et de la responsabilité des systèmes à base d'agents IA.

La réglementation : une maturité à marche forcée

Dans beaucoup de secteurs, la réglementation est vue comme un frein à la croissance. La réglementation cyber est au contraire un accélérateur puissant parce qu'en réalité, il s'agit de réglementer d'autres secteurs (secteurs critiques, financiers, IoT, IA, etc.) en les forçant à intégrer les problématiques cyber.

Un effet de bord de ce constat est l'émergence naturelle de solutions pour suivre et valider la conformité cyber des différentes entités soumises aux réglementations.

Le mid-market une nouvelle frontière pour le cyber

Historiquement, la cible de prédilection des startups cyber a toujours été les grands comptes.

Néanmoins, deux phénomènes simultanés contribuent à changer cette situation. Tout d'abord, les grands comptes sont sursollicités par les startups cyber (et pour beaucoup déjà bien équipés) avec une volonté de plutôt rationnaliser les outils et les dépenses. En parallèle, des acteurs de taille plus restreinte ont également développé une maturité sur le sujet cyber et sont aujourd'hui massivement en demande de solutions adaptées à leur typologie. Ces acteurs (principalement les grosses ETI et les « petit grands comptes ») constituent ce que l'on peut appeler un mid-market avec un potentiel de croissance en France et en Europe. Avec du budget et des cycles de vente plus courts, ces clients potentiels représentent un relais de croissance important.

Les besoins croissants des domaines de défense et souveraineté

La cybersécurité est par nature très orientée vers le « dual use » (civil / militaire). Le monde de la défense a souvent eu pour stratégie, en cyber, de bénéficier des innovations du civil tout en ne finançant que les spécificités nécessaires pour les applications défense.

Il n'en demeure pas moins que le numérique fait aujourd'hui partie intégrante de l'armement et des conflits modernes. Avec les instabilités géopolitiques actuelles et une montée grandissante des besoins de défense, en particulier européenne, ce marché est à présent un levier de croissance à part entière pour beaucoup de startups cyber.

Dans ce contexte particulièrement dynamique, le positionnement d'acteurs pouvant contribuer à lever les différents verrous, pas que financiers, pour faciliter l'émergence des innovations est un différenciant important qu'il convient de favoriser.

Un rôle au-delà du financement

Les sujets early stage sont notoirement difficiles à appréhender mais les sujets cyber early stage sont encore pires. Et quant aux startups, elles ont des besoins d'accompagnement très spécifiques (recrutement spécialisés, marchés particuliers, go-to-market spécifiques, etc.) qui vont bien au-delà de la connaissance du secteur B2B SaaS.

Le rôle sur ce segment d'un acteur de l'investissement spécialisé est donc, d'une part, de pouvoir prendre des positions tôt et de les expliciter pour ouvrir la voie à des co-investissement avec des acteurs plus généralistes. Et d'autre part, Il doit pouvoir apporter un soutien ad-hoc, directement et via son réseau d'experts métiers spécialisés, sur tous les sujets spécifiques à la cyber (dont l'accès au marché qui peut s'avérer très particulier).

Intervenir à tous les stades de maturité technologique : de la preuve de concept au produit déployé

Une capacité fine à cerner les enjeux et les technologies permet également de se positionner à différents niveaux de maturité du pre-seed (typiquement TRL 3 à 6, ou juste pré-revenu), pour aider à passer la « valley of death » au seed (typiquement TRL 7 à 9, ou au début de la commercialisation) pour accélérer l'accès au marché.

Identifier les signaux faibles

Une vue très large sur l'early stage d'un domaine pointu comme la cybersécurité permet de capter très tôt de nouvelles tendances. Même s'il demeure difficile de savoir avec certitude comment les choses évolueront à long terme, capitaliser sur la proximité terrain avec les fondateurs et les clients donne une compréhension forte sur l'évolution à court terme et un avis fondé sur les possibilités à moyen terme dans le domaine.

auriga cyber ventures

William LECAT
Partner
Auriga Cyber Ventures

L'équation magique de la cybersécurité

L'équation magique de la cybersécurité

La principale raison pour laquelle j'ai décidé de me spécialiser dans la cybersécurité, alors qu'à l'origine j'étais passionné par l'informatique de manière générale et son impact sur le monde, est une équation assez simple. Les cyberattaquants, qu'ils soient cybercriminels ou au service d'un état, innovent pour trouver de nouvelles failles dans les systèmes informatiques et développer des tactiques offensives originales. La défense doit donc s'adapter en permanence pour espérer garder un niveau d'efficacité suffisant. Or, pour diverses raisons, en particulier l'acceptation d'une prise de risque élevée, l'agilité et la capacité de focaliser un effort intense en s'affranchissant de lourdeurs administratives, les start-ups sont souvent bien plus efficaces que les grands groupes pour innover. Evidemment, le succès n'est pas toujours au rendez-vous et la plupart n'ont pas de trajectoire spectaculaire, voire disparaissent à plus ou moins brève échéance. Cependant, certaines arrivent à prendre des parts de marché, à se développer à l'international, et à terme à atteindre la rentabilité. Une fois ces étapes franchies, les plus gros acteurs du domaine cyber, à la fois dans une logique de croissance de leur activité et de renforcement de leur offre de plateforme, se positionnent souvent comme consolidateurs.

Le temps entre la création d'une start-up cyber et son rachat par un grand groupe peut être très court et la valeur créée impressionnante. L'exemple récent le plus marquant est WIZ, spécialiste de la sécurité du cloud, créé en 2020 et racheté pour 32 milliards de dollars par Google en 2025. Extrêmement peu de secteurs, à part l'IA, permettent une telle vélocité, à une telle échelle.

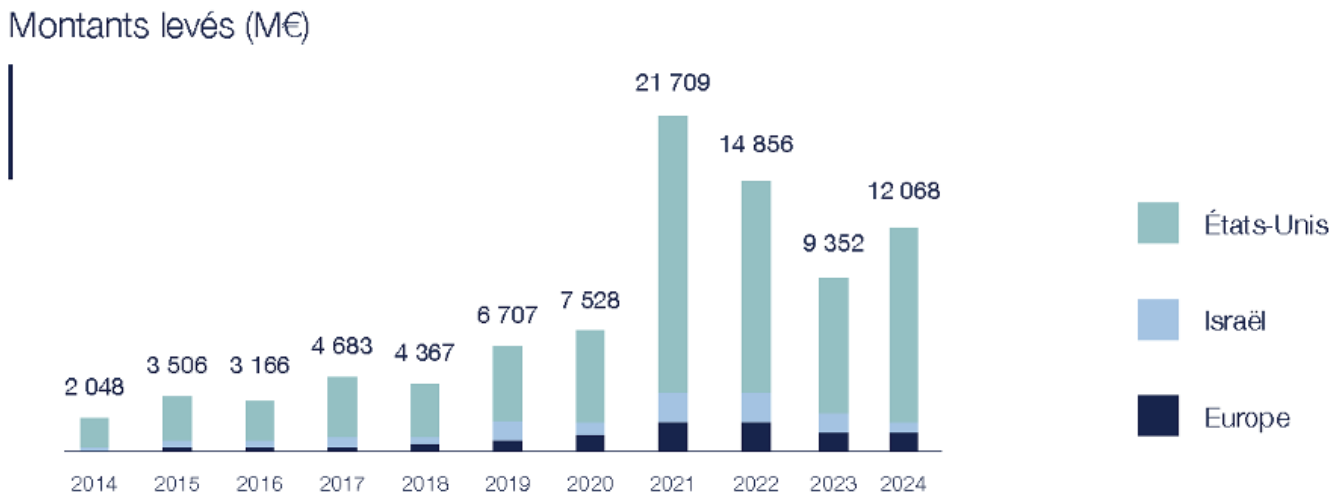
Cette équation rend le domaine cyber particulièrement attractif pour les entrepreneurs et les start-ups mais aussi évidemment pour les financiers et les fonds d'investissement.

Du marketing produit à l'investissement en cyber

Après diverses expériences de responsable produit en France et au Royaume-Uni et d'entrepreneur dans les logiciels de CRM, je me suis finalement installé avec un MBA en poche dans la Silicon Valley avec la ferme intention d'apprendre là où la plupart des géants de l'informatique ont vu le jour. Une rencontre avec Scott Cook, le fondateur d'Intuit, spécialiste des logiciels de gestion, m'a permis de rejoindre cette excellente école du marketing. En 2001, j'ai découvert la dynamique d'innovation et le potentiel d'hyper-croissance de la cybersécurité en rejoignant Brightmail, pionnier de la protection de la messagerie, comme VP Marketing.

Symantec, à l'époque le plus gros acteur cyber mondial, a fait l'acquisition de Brightmail en 2004 après avoir tenté, sans grand succès, de développer une offre alternative en interne. En 2007, après mon retour en France, j'ai pris la direction de Netasq, acteur majeur de la sécurité des réseaux en Europe, jusqu'à son rachat par le groupe Airbus en 2012. Le pilotage du projet de consolidation avec d'autres acteurs de la filière cybersécurité comme Arkoon et sa filiale SkyRecon, avec les moyens du groupe Airbus et sous la marque Stormshield, m'a permis de lancer une dynamique de croissance et d'innovation profitable qui demeure encore très forte aujourd'hui. Après avoir été nommé à la tête d'Airbus CyberSecurity, j'ai aussi été responsable de la sécurité numérique et de la gouvernance des données pour la division Airbus Defence & Space. Cependant, la tentation de rejoindre un fonds d'investissement qui puisse valoriser mon expertise et mon expérience était forte et l'un de mes projets était de devenir investisseur dans les domaines cyber et data/AI. En effet, l'évolution des montants levées par les start-ups et scales-ups cyber entre 2014 et 2019 a été impressionnante, passant de 2 à 6,7 milliards d'euros (voir graphe ci-dessous).

Durant cette période, de nombreux fonds spécialisés en cyber ont vu le jour, en particulier aux Etats-Unis et en Israël. Il fallait que l'Europe et la France agissent !



Tikehau Capital et l'investissement en cyber

Fin 2018, Tikehau Capital, groupe mondial de gestion d'actifs alternatifs qui gère 51 milliards d'euros d'actifs (au 30/06/2025) a racheté la société de gestion Ace Management, spécialiste des secteurs de l'aéronautique et de la défense afin de renforcer ses activités de private equity. En juin 2019, Tikehau Capital a étoffé sa gamme de fonds spécialisés (transition énergétique, agriculture régénérative, aéronautique & défense et situations spéciales) en annonçant le lancement du premier fonds en France spécialisé dans la cybersécurité. C'était pour moi une excellente occasion d'évoluer vers un nouveau métier tout en restant actif dans le secteur qui me passionne et je n'ai évidemment pas hésité à rejoindre l'équipe lorsque l'opportunité s'est présentée. Notre premier fonds, appelé Brienne III, a collecté 175 millions d'euros et est devenu le plus important spécialisé en cyber en Europe. Nous avons déployé ce premier fonds dans une quinzaine de participations en France et en Europe entre 2019 et 2023. Dans notre stratégie, nous avons été soutenus par divers partenaires et souscripteurs comme EDF, Naval Group, Sopra Steria, Dassault Aviation et le Crédit Agricole ainsi que par Bpifrance et d'autres investisseurs institutionnels et privés. Nous avons signé des conventions de partenariat et des accords avec l'ANSSI, le Ministère des Armées, le Campus Cyber, FIC (Forum InCyber) et le PEC (Pôle d'excellence cyber) avec l'objectif partagé de renforcer la filière cybersécurité en France et en Europe. En 2023, pour accompagner l'évolution du niveau de maturité des sociétés cyber européennes et aussi parce que d'autres fonds spécialisés en cyber et positionnés sur les phases d'amorçage et ce capital risque ont vu le jour avec souvent notre soutien, nous avons lancé le millésime suivant avec une taille cible du double de celle du précédent. Ce nouveau fonds de Growth Equity, appelé Brienne IV, a vocation à investir dans 10 à 15 sociétés avec des tickets significatifs compris entre 10 et 50 millions d'euros et à un niveau de développement assez avancé. Le soutien de la croissance par acquisition au travers de participations ayant le potentiel d'être des plateformes de consolidation est aussi un axe d'investissement. Nous soutenons l'accélération de champions européens de la confiance numérique comme par exemple ChapsVision, FTapi, ProvenRun et Memority en leur apportant non seulement du capital mais aussi du soutien opérationnel et stratégique, à toutes les étapes de leur histoire

La dynamique de l'investissement en cybersécurité est particulièrement forte, avec de belles perspectives, des besoins financiers toujours plus importants et une consolidation qui s'accélère. L'Europe dispose d'un authentique potentiel pour faire émerger plus d'acteurs cyber majeurs au niveau mondial pour garantir son indépendance stratégique. Les initiatives de nombreuses associations françaises et européennes et en particulier d'ECSO (The European Cyber Security Organisation) permettent d'impliquer et de fédérer toujours plus d'acteurs. Notre ambition est de contribuer à l'effort commun de tous les acteurs de la filière cyber européenne pour que l'écosystème continue à prospérer.

TIKEHAU CAPITAL

François LAVASTE
Tikehau Capital
Vice-chair du Board - ECSO (European Cyber Security Organisation)

Créer sa start-up innovante grâce aux financements européens : guide pratique et stratégique

Faire émerger une start-up innovante dans les domaines du numérique, de la cybersécurité ou de l'intelligence artificielle, c'est transformer une intuition en solution concrète, une technologie en produit, une vision en croissance. Ce chemin, complexe mais fécond, nécessite des ressources solides. L'Union européenne (UE), consciente de cet enjeu, propose un ensemble cohérent de financements adaptés aux différentes étapes de développement, depuis la preuve de concept jusqu'à la mise sur le marché.

L'UE vise à renforcer son leadership et son autonomie stratégique en Cybersécurité. L'ANSSI est le Centre français de coordination Cyber (NCC-Cyber) qui a pour mission de rendre visible les dispositifs de soutien financier européens et de développer des programmes nationaux de soutien financier. Il travaille en collaboration avec le Centre européen de compétences en cybersécurité (ECCC) et les autres centres nationaux de coordination membres du réseau. Ainsi, 390 millions d'euros vont être alloués à des appels à projets européens au cours de la période 2025-2027. Chaque entreprise est ainsi invitée à se rapprocher de l'ANSSI (NCC-Cyber). Les programmes européens constituent ainsi une belle opportunité au service de la Cyber et de la souveraineté.

Contrairement aux idées reçues, les PME et start-ups ont toute leur place dans les dispositifs européens de financement de l'innovation. Certaines aides leur sont même réservées.

Pour ce faire l'UE s'est dotée de programmes et d'outils comme Horizon Europe, Europe numérique, Fonds européen de développement régional, le Fonds européen d'investissement (FEI) et Banque européenne d'investissement (BEI), en voici quelques exemples :

1. Explorer l'idée de rupture : EIC Pathfinder (Horizon Europe)

Le programme EIC Pathfinder s'adresse aux projets technologiques encore très en amont (niveaux TRL 1 à 3). Il soutient des idées scientifiques audacieuses susceptibles d'initier de véritables ruptures. Deux modalités s'offrent aux porteurs :

- Pathfinder Open : ouvert à toutes thématiques, il laisse libre cours à la créativité scientifique sans contrainte de sujet.
- Pathfinder Challenges : ciblé sur des défis identifiés par la Commission (ex : IA générative pour le diagnostic médical).

Les financements, pouvant aller jusqu'à 3 millions d'euros, visent à valider la faisabilité scientifique d'un concept au sein de petits consortiums (universités, centres de recherche, PME). La soumission se fait sur le portail Funding & Tenders, avec une évaluation par experts externes. Ce programme constitue une première rampe de lancement pour les projets disruptifs.

2. Valider un prototype : EIC Transition

À mi-chemin entre recherche fondamentale et innovation de marché, EIC Transition permet de franchir le cap critique de la preuve de concept au démonstrateur fonctionnel (TRL 3 à 6). Il finance les activités de maturation technologique, d'expérimentation en conditions réelles et d'étude de faisabilité commerciale.

Ce programme peut accorder jusqu'à 2,5 millions d'euros en subvention pour les projets issus d'un précédent financement européen (EIC Pathfinder, ERC Proof of Concept, FET...). Il est particulièrement adapté à celles et ceux qui envisagent la création d'entreprise ou une première levée de fonds.

3. Accélérer la mise sur le marché : EIC Accelerator

Conçu pour les start-ups et PME en phase de pré-commercialisation (TRL 5 à 9), l'EIC Accelerator est le dispositif le plus ambitieux d'Horizon Europe. Il propose :

- Une subvention allant jusqu'à 2,5 M€, pour le prototypage, les tests, les certifications ou les recrutements stratégiques ;

- Un investissement en equity jusqu'à 15 M€, via le Fonds EIC, permettant d'éviter une dilution excessive du capital lors de la première levée.

Les critères de sélection sont rigoureux : innovation de rupture, impact potentiel à l'échelle européenne, qualité de l'équipe dirigeante, viabilité du modèle économique. Le processus comprend une présélection sur dossier, un pitch vidéo, puis une audition devant un jury. C'est un levier de croissance puissant pour les jeunes entreprises à fort potentiel.

4. Déployer la technologie : Digital Europe Programme (DEP)

Le programme pour une Europe numérique cible le déploiement opérationnel des technologies matures, sans financer la recherche. Il soutient notamment :

- L'intégration de solutions IA, cloud ou cybersécurité dans les secteurs publics et privés ;
- Le développement des compétences numériques via des formations, certifications ou plateformes ;
- La création de Hubs d'innovation numérique (EDIH) pour accompagner les PME dans leur transformation digitale.

Le DEP finance principalement des projets collaboratifs, en consortiums paneuropéens. Une start-up peut y participer comme partenaire ou bénéficiaire final pour tester sa technologie dans plusieurs États membres. L'apport financier peut représenter jusqu'à 50 % des coûts du projet, selon les appels.

5. S'ancrer régionalement : le Fonds européen de développement régional (FEDER)

Le FEDER, géré par les régions françaises dans le cadre de leurs Programmes opérationnels, via les Stratégies de spécialisation intelligentes (S3), constitue une ressource essentielle pour soutenir les infrastructures, l'innovation locale et l'écosystème entrepreneurial.
Les start-ups peuvent y recourir pour cofinancer :

- Des investissements matériels (machines, équipements, infrastructures numériques) ;
- L'aménagement de locaux techniques ou la participation à des pôles de compétitivité ;
- Des actions collectives portées par des incubateurs ou clusters régionaux.

L'intensité de l'aide varie selon les priorités régionales et le degré d'innovation du projet, avec des taux de cofinancement allant jusqu'à 60 % pour certaines catégories d'entreprise.

6. Accéder à l'investissement privé : InvestEU et le Fonds européen d'investissement (FEI)

Le programme InvestEU vise à renforcer l'accès au capital pour les start-ups européennes à fort potentiel. Il ne s'adresse pas directement aux entreprises, mais opère par l'intermédiaire de fonds d'investissement labellisés, souvent gérés par des structures de capital-risque.

Ces fonds, sélectionnés par le Fonds européen d'investissement (FEI), investissent dans des entreprises actives dans des domaines stratégiques, comme les technologies numériques souveraines, l'IA ou les semi-conducteurs. Une start-up en phase d'expansion peut ainsi bénéficier d'un effet de levier public-privé significatif pour sa levée de fonds.

7. Financements d'envergure : le rôle de la Banque européenne d'investissement (BEI)

Bras financier de l'Union européenne, la Banque européenne d'investissement (BEI) joue un rôle capital dans le financement de l'innovation technologique. Elle intervient à trois niveaux :

1. Prêts directs aux entreprises innovantes (généralement à partir de 25 M€), avec des conditions avantageuses ;
2. Lignes de crédit ou garanties à des institutions financières locales, qui répercutent ensuite ces conditions sur les PME ;
3. Co-financement de projets structurants, notamment dans les domaines du cloud, de la cybersécurité ou des infrastructures de données.

La BEI est un acteur central des programmes InvestEU, Horizon Europe ou Connecting Europe Facility, et pilote des instruments ciblés comme InnovFin pour les projets à haut risque technologique.

Pour ce faire, le réseau Enterprise Europe Network (EEN), créé en 2008, a pour mission d'accompagner le développement des PME dans chaque Etat membre. En Europe c'est aussi le cas pour la European CyberSecurity Organisation via des programmes tels que Invest4Cyber et les Cyber Investor Days .

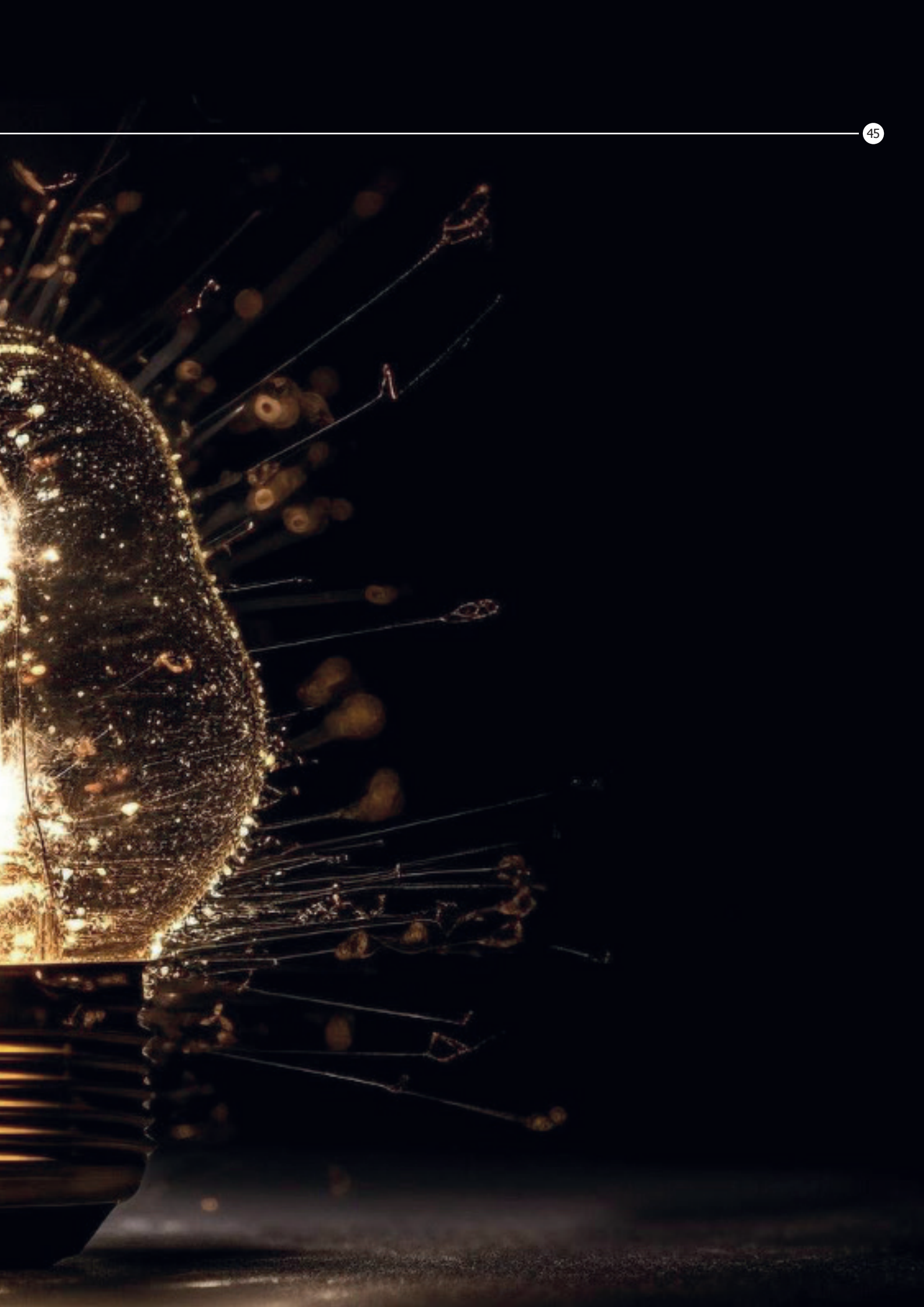
Aussi, même si comme le disait G. Flaubert L'innovation est toujours dangereuse, les fonds européens peuvent être de bons outils pour soutenir et sécuriser votre démarche novatrice !

PÔLE D'EXCELLENCE CYBER

Annie AUDIC
Ambassadrice Europe
Pôle d'excellence cyber

Marine THIEBAUD
Chargée de mission Europe
Pôle d'excellence cyber

PARCOURS INSPIRANTS



Réinventer la croissance des start-up cyber : pour un modèle européen enfin adapté à ses ambitions

Depuis plus de vingt ans, j'évolue dans l'écosystème de la cybersécurité. J'ai cofondé et dirigé plusieurs entreprises technologiques en France, dont Arkoon Network Security, entrée en bourse en 2007 puis cédée à Airbus en 2013, et Sentryo, pionnière de la cybersécurité industrielle, rachetée par Cisco en 2019. Aujourd'hui, je poursuis cet engagement comme investisseur, au sein du fonds Auriga Cyber Ventures et du start-up studio Cygo Entrepreneurs, que nous avons lancé pour accompagner la création de champions européens de la cyber.

Depuis dix ans, j'observe une contradiction persistante. D'un côté, le nombre de start-up créées dans la cybersécurité a fortement augmenté, notamment en France. Mais de l'autre, très peu passent à l'échelle. Presque aucune ne devient un acteur mondial. Et celles qui réussissent sont souvent absorbées prématurément par des groupes américains ou israéliens.

En 2013, dans un livre blanc publié avec l'AFDEL, je soulignais déjà l'impératif d'attirer les investisseurs et de faciliter les cessions, afin d'accélérer les cycles investissement/désinvestissement et permettre à l'écosystème européen de croître. Depuis, des avancées ont eu lieu : les chaînes de financement seed, série A/B/C se sont structurées, la BPI a renforcé son rôle, plusieurs fonds spécialisés sont apparus. Mais un verrou majeur subsiste : les investisseurs en capital-risque manquent de liquidité. Il n'y a pas de marché boursier dynamique pour les valeurs technologiques, et surtout il n'y a pas ou très peu de consolidateurs européens susceptibles d'acheter les start-up dans des conditions satisfaisantes

pour les investisseurs. Les meilleures sont souvent rachetées par des groupes extra-européens, beaucoup stagnent et très peu réussissent à se développer.

L'expérience de Sentryo l'illustre bien. Dès 2014, avec mon associé Laurent Hausermann, nous avons choisi de développer simultanément la France et l'Allemagne, avant d'attaquer les États-Unis après notre deuxième levée de fonds. Cette stratégie s'est avérée pertinente, mais difficile à financer : les cycles de vente dans l'industrie sont longs, les effets de réseau lents à construire. Lorsqu'un groupe comme Cisco s'est intéressé à nous pour compléter son portefeuille IoT industriel, il n'existait aucun acteur européen avec une approche équivalente.

L'histoire d'Arkoon le montre aussi : après une réussite sur le marché français, l'entrée en bourse devait nous permettre de financer le développement européen, tout en offrant une porte de sortie aux investisseurs historiques. Mais nous sommes arrivés trop tard sur un marché déjà dominé par des compétiteurs, et le contexte bousier n'a pas permis de générer la liquidité espérée. La cession à Airbus s'est imposée comme une solution raisonnable.

Dans le capital-risque américain, la règle est claire : « Go big or go home ». L'objectif est de bâtir une entreprise dominante à l'échelle mondiale, rapidement. Ce modèle repose sur un marché homogène, un accès massif au capital, une forte appétence des clients pour l'innovation, et une armée d'acteurs tech prêts à racheter les meilleurs. En Europe, on a tenté d'appliquer ce modèle… sans en réunir les conditions. Résultat : un développement plus lent, des entreprises qui butent sur les frontières intra-européennes, et trop souvent une stagnation sous la taille critique.

Il est temps d'assumer une autre voie. De concevoir un modèle européen, qui transforme la fragmentation du marché en levier stratégique. Cela implique que les start-up soient pensées dès l'origine pour un développement paneuropéen, avec un accompagnement adapté. C'est la démarche que nous mettons en œuvre avec Cygo Entrepreneurs, qui structure ses projets pour se déployer simultanément sur plusieurs marchés. C'est aussi l'ambition d'Auriga Cyber Ventures, lancé avec trois entrepreneurs de la cyber et Auriga Partners, qui accompagne ses participations dans leur exécution multi-pays, en s'appuyant sur les forces locales.

Ce modèle européen doit être frugal, tendre rapidement vers l'équilibre économique, et s'ancrer dans les besoins industriels réels. Il doit privilégier la croissance organique, l'efficacité du modèle économique et la création de valeur concrète. Il ne s'oppose pas à l'ambition internationale, bien au contraire : il lui donne un socle viable.

Lors de la RSA Conference 2025 à San Francisco j'ai encore une fois pris conscience de l'écart entre l'écosystème Américain et le nôtre. La dynamique d'innovation y est fluide, structurée, extraordinairement bien financée. La conférence est une démonstration de puissance collective où start-up, investisseurs, géants de la tech et institutions publiques travaillent ensemble avec une stratégie d'influence claire.

La cybersécurité n'est plus un simple segment de la tech : c'est une brique fondamentale de souveraineté. Il ne suffit plus de créer des start-up. Il faut qu'elles grandissent et pour cela qu'elles aient des débouchés, des financements cohérents, et qu'elles aient accès à un tissu d'acteurs capables de les consolider et de les porter. Cela suppose une véritable politique à l'échelle européenne, où l'institution n'est pas seulement un catalyseur ou un label, mais un stratège doté d'une vision à long terme.

Après vingt ans passés à construire dans la cyber, je crois qu'il est possible de réussir en créant des entreprises sobres, ambitieuses, résolument tournées vers les besoins du terrain. En valorisant la durée, la profondeur technique, la proximité avec les utilisateurs et les spécificités du marché Européen . Et en refusant les modèles importés comme des dogmes.

L'Europe n'a pas besoin de copier. Elle doit oser inventer.

Témoigner de son parcours n'est jamais simple. Mais si je devais transmettre quelques clés à celles et ceux qui s'intéressent à l'innovation, je dirais ceci :

Après une thèse en mathématiques appliquées, et une carrière de chercheuse en traitement du langage naturel, j'ai occupé des postes de direction d'équipes R&D au sein de multinationales comme IBM et Xerox. Durant ma carrière au centre européen de Xerox, j'ai également travaillé trois années durant dans une entité dédiée au transfert des résultats. En 2011, j'ai été appelée par Viseo pour créer leur centre de recherche focalisé sur l'analyse des données, que j'ai ensuite dirigé pendant six ans. En 2018, je me suis rapprochée de la sphère Défense et Sécurité en prenant la direction du département Intelligence de Bertin IT. Le poste que j'occupe aujourd'hui à Inria est la continuité de cette volonté de mettre mes travaux de recherche au service de causes sociétales : médicales d'abord, puis en sécurité-Défense.

J'ai participé à plus de trente projets européens, dont certains en coordination, notamment SAFFRON et Trivallent sur la radicalisation en ligne et les stratégies de contre-discours. J'ai aimé travailler avec des sociologues, des informaticiens, des services de renseignement, des éducateurs de différents pays. La question centrale était déjà la résilience.

J'ai toujours été attirée par la découverte de nouveaux milieux. La confrontation aux autres domaines, pour s'enrichir et être plus pertinent dans ses travaux, est un fil conducteur de ma carrière. Cela passe par l'écoute des besoins — de chercheurs d'autres disciplines, comme des utilisateurs sur le terrain. Il faut savoir dialoguer, expérimenter, accepter de remettre en question sa méthode. Avoir des convictions, mais pas de certitudes.

On peut être excellent d'un point de vue théorique sans aucune curiosité ni ouverture vers le reste du monde. Selon moi, cela rend rapidement la recherche stérile. J'ai aimé démarrer des choses, construire du nouveau, rassembler des gens différents, comprendre les acteurs nécessaires, faire avancer les idées. Créer du lien entre théorie et pratique, entre disciplines, entre personnes.

J'ai eu la chance d'évoluer très tôt dans des univers internationaux. Chez Xerox, il y avait une cinquantaine de nationalités. Les gens célèbres dans leur domaine étaient simples et accessibles. Il n'y avait pas de cloison entre les statuts. C'est là que j'ai appris à écouter des cultures différentes, et que j'ai compris la magie des mélanges. Ces compagnies m'ont aussi appris la rigueur, le management, la communication, et m'ont permis de bâtir un solide réseau international.

Commencer des choses nouvelles ne va pas de soi. On se heurte à des réticences : peur du changement, conformisme, dénigrement. Dans la recherche aussi, la liberté est relative. Pour publier, il faut suivre les modes. Pour obtenir des financements, il faut rentrer dans les cases. En tant que femme, on vous prend souvent moins au sérieux. J'ai entendu que je ne devais pas me maquiller car on me prenait pour une secrétaire.

Les choses ont évolué, pourtant, le numérique compte toujours peu de femmes.

Il n'y a pas de miracle. Pour innover il faut savoir bifurquer, réorienter, apprendre en chemin. Innover, c'est capter des signaux faibles avant les autres. Et quand on est en avance, on n'est pas toujours soutenu. J'ai eu la chance d'être aidée par des personnes qui avaient elles-mêmes créé des choses, qui avaient une ouverture d'esprit, une tolérance pour les profils atypiques. Des gens brillants qui m'ont inspirée par leur modestie, leur vision et leur façon de partager. Pour avancer il faut être soutenu par des personnes qui ont un certain pouvoir.

Un manager m'avait dit : "Il faut accepter une forme de pouvoir car elle donne accès à des informations et à une liberté pour faire ce que tu veux. Trop de pouvoir, tu n'as que les ennuis." J'ai aussi vécu les logiques tribales de la recherche, les jeux de statuts, les règles implicites. Mais j'ai vu des environnements plus ouverts, où seuls comptaient les idées et les qualités de recherche.

J'ai aussi appris à doser la diplomatie. On apprend à dire les choses autrement, à chercher des compromis pour faire passer une idée. Ce n'est pas un échec. C'est un apprentissage. On apprend plus de ses erreurs que de ses réussites. Parce que la réussite flatte l'ego, mais l'erreur, elle, fait grandir.

Certains m'ont dit des années plus tard : "À l'époque on n'y croyait pas, mais avec le recul c'était visionnaire." Ce genre de retour fait chaud au cœur. Il redonne du courage.

J'essaie de rester alignée avec ce que j'aime et ce que je sais faire. Et je me demande : qu'est-ce qui me retient encore ici ? Qu'est-ce qui me permettrait d'aller plus loin ?

Commencer des choses nouvelles demande du courage, mais surtout de croire en leur utilité. Si je devais donner un conseil : soyez curieux. N'ayez pas peur de commencer petit. Osez le mélange. Et surtout, partagez. Toujours.

Quand on m'a proposé de contribuer librement à ce livre blanc, j'ai pris un moment pour repenser au chemin (escarpé) parcouru - non sans un léger vertige. D'abord avec Earthcube, devenue Preligens, où nous avons relevé quelques défis, malgré les difficultés liées aux apprentissages, parfois abrupts, qui accompagnent l'hyper-croissance. Aujourd'hui avec Safran.AI - depuis son intégration au sein du groupe Safran en septembre 2024 - nous poursuivons cette entreprise singulière, toujours avec la même conviction : servir au mieux nos clients et utilisateurs dans un secteur exigeant où l'innovation technologique est à la fois indispensable et contrainte.

Tout a commencé en 2016, à l'initiative de deux co-fondateurs, Arnaud Guérin et Renaud Allioux. Très vite, une équipe (de pionniers, d'aventuriers, de bâtisseurs, etc.) s'est constituée autour d'eux, motivée par une double ambition : innover aussi vite et aussi efficacement que possible dans le domaine de l'intelligence artificielle appliquée à la défense et au renseignement, et démontrer qu'un modèle alternatif de développement pouvait exister, capable de franchir la fameuse « vallée de la mort » et de tenter le « passage à l'échelle », tout en assurant une forme de souveraineté à travers la composition de notre capital. Sur ces derniers aspects, nous devons également beaucoup à Jean-Yves Courtois, dont l'arrivée a été structurante en 2023.

Avec le recul, nous avons dû franchir de nombreuses barrières à l'entrée. Du genre de celles relevant de la sempiternelle formule prêtée généralement à Mark Twain : « Ils ne savaient pas que c'était impossible, alors … » Il a fallu assimiler les codes et les usages propres au secteur, s'approprier un langage parfois abscons fait d'acronymes et d'abréviations - et il faut bien l'avouer, ce fût une forme de reconnaissance, le jour où nous avons pu nous-mêmes bénéficier de cela : TAIIA, TORNADE, etc. Acculturés progressivement par nos interlocuteurs étatiques ou industriels ainsi que par le général (2S) Grégoire de Saint Quentin, que nous avons la chance et le privilège de compter parmi nous depuis 2020, nous avons graduellement compris le rôle, le périmètre, le calendrier ainsi que les éventuelles marges de manœuvre de chacune de nos parties prenantes : opérationnels, responsables capacitaires, architectes, acheteurs, financeurs, etc. Cela a impliqué de naviguer - et on finit par ne plus s'en rendre compte – dans un enchevêtrement de niveaux de décision et de temporalités. En outre, certains défis étaient particulièrement paradoxaux, comme celui de l'habilitation. Véritable quadrature du cercle : une jeune entreprise ne peut être habilitée que si elle en prouve la nécessité, laquelle ne peut être liée qu'à des sujets pour lesquels elle ne peut en connaître que si elle est habilitée. Il en va de même avec certaines homologations.

Fort heureusement - et toujours avec un peu de recul - nous avons eu la chance de bénéficier d'un momentum exceptionnel. La volonté de transformation chez les opérationnels était (et reste !) forte. Le secteur a manifesté une réelle détermination pour voir émerger de nouveaux acteurs. Nos clients et nos utilisateurs ont rapidement compris tout l'intérêt de la « co-construction », appelée

très souvent de leurs vœux afin de pouvoir s'appuyer sur une start-up capable de chercher en permanence l'adéquation entre innovation technologique et besoins opérationnels concrets.

Un constat « stratégique »

Au fil de cette expérience, nous avons mieux saisi pourquoi, dans ce secteur si essentiel de la défense et du renseignement, les grands programmes d'armement - qu'il s'agisse de systèmes d'armes complexes, de plateformes aériennes, navales ou terrestres, ou d'infrastructures critiques - exigent encore une approche traditionnelle et rigoureuse de gestion de projet. Le cycle en V y reste indispensable. C'est lui qui garantit la conformité aux exigences opérationnelles, sécuritaires et réglementaires ou encore de certification et de qualification, dès la conception. Compte tenu de l'ampleur des enjeux stratégiques, financiers, industriels et politiques, il n'y a pas de place pour l'improvisation « en conduite » : il faut une maîtrise du risque à chaque étape, une traçabilité totale des décisions et une validation systématique des jalons, pour livrer aux forces des systèmes robustes, fiables et pérennes.

Dans le même temps, nous avons collectivement observé qu'il faut faire face à une accélération sans précédent de l'innovation technologique, et ceci a été notre « trou de souris », notre « interstice ». Intelligence artificielle, cybersécurité, systèmes autonomes, robotique, … ces technologies évoluent à une vitesse telle que pour rester compétitif et pertinent face à des compétiteurs ou adversaires toujours plus imprévisibles ou réactifs, il devient vital d'intégrer rapidement des solutions nouvelles. C'est dans ce contexte que les approches agiles prennent tout leur sens : elles permettent de développer, tester et ajuster des capacités en cycles courts, en intégrant des retours utilisateurs fréquents et en conservant une capacité d'adaptation permanente face à des besoins opérationnels en constante évolution.

Au fond, c'est cette double logique qu'il faut parvenir à conjuguer efficacement. Une forme de dilemme militaro-industriel. Les grands systèmes ou systèmes de systèmes sont pensés et certifiés sur des cycles longs pour garantir leur interopérabilité et leur solidité. Mais en parallèle de ces structures pérennes, des briques technologiques, des applications logicielles et des services numériques peuvent - et doivent - être développés et intégrés en continu. C'est ce qui permet ou devra permettre, par exemple, d'équiper un sous-marin, un avion de chasse ou une frégate de systèmes de traitement de données en temps réel, de capacités de guerre électronique adaptatives ou de solutions tactiques évolutives, mises à jour au fil de l'innovation, at the speed of relevance.

Pour une ambition renouvelée

Ces deux dynamiques - grands programmes structurants et innovation incrémentale continue - obéissent à des temporalités, des cultures et des gouvernances radicalement différentes. On le vérifie chaque jour : une start-up, aussi innovante et brillante soit-elle, se heurte vite aux contraintes réglementaires, industrielles et commerciales spécifiques à ce secteur. De son côté, un grand groupe industriel, aussi solide et expérimenté soit-il, peine à maintenir l'agilité nécessaire pour développer des solutions en cycles courts et répondre rapidement aux besoins du terrain.

C'est précisément là que notre modèle d'hybridation prend tout son sens. « Pour de vrai ! » Une start-up intégrée au sein d'un grand groupe peut bénéficier du meilleur des deux mondes : un environnement industriel exigeant et sécurisé, des infrastructures d'essais, l'empreinte internationale, une connaissance fine des normes et des circuits institutionnels, tout en conservant sa capacité à expérimenter vite, à prendre des risques technologiques et à s'adapter en continu. Ce positionnement hybride permet de concevoir des modules ou composants technologiques innovants et de les rendre interopérables avec des systèmes sophistiqués développés selon des cycles en V, sans altérer la cohérence et la robustesse des grands programmes. En optimisant les coûts.

Dans un groupe comme Safran, un leader mondial à l'ADN d'équipementier - qui maîtrise des sous-ensembles critiques sans forcément piloter l'ensemble des systèmes - cette approche est particulièrement stratégique. Elle peut permettre de proposer des solutions innovantes, compatibles avec les architectures complexes pilotées par d'autres intégrateurs, et de conserver des positions clés dans des chaînes de valeur toujours plus fragmentées et concurrentielles. C'est à notre sens un levier décisif pour rester pertinents et réactifs dans un environnement où la vitesse d'implémentation des nouvelles technologies est devenue un facteur majeur de succès.

C'est cette vision que nous défendons et que nous mettons en œuvre désormais. Faire de notre start-up intégrée un accélérateur d'innovation pour le groupe, pour être capable de faire le lien entre les besoins opérationnels et les cycles industriels longs, de tester et de valider des technologies en environnement contraint, et d'alimenter en continu les capacités offertes à nos clients et utilisateurs. C'est bien cela que nous voulons réussir ensemble, sans esprit de territorialisme, et c'est ce qui donne tout son sens à notre engagement dans ce secteur si particulier.

De là à y voir une recherche permanente de résonance optimale entre ce que nous souhaitons offrir, même en termes d'organisation, et les besoins de nos clients et utilisateurs - on ne change pas !

De bidouilleur à entrepreneur : mon chemin sans plan tout tracé

Je ne viens pas d'un parcours classique. Je n'ai pas fait de grandes écoles ni suivi de plan de carrière précis. Ce qui m'a toujours guidé, c'est la curiosité, l'envie de comprendre comment les choses fonctionnent — et parfois, l'envie de les faire autrement.

Aujourd'hui, je dirige XXII, une boîte spécialisée dans la vision par ordinateur. Ce n'était pas un objectif écrit à l'avance. C'est plutôt le résultat de plein d'expériences, d'essais, de rencontres... et de pas mal de tâtonnements.

Des débuts bricolés et beaucoup de tests

J'ai toujours aimé bricoler. À 17 ans, je fabriquais dans mon garage des boîtiers pour détecter les radars. C'était un peu artisanal, mais ça marchait. Petit à petit, j'ai ouvert quelques boutiques. C'est comme ça que j'ai rencontré Fabien Pierlot, le fondateur de Coyote, avec qui j'ai bossé sur le signalement participatif sur la route. Ça a bien marché, mais ce n'est pas ce que je retiens le plus. Ce qui m'a marqué, c'est de voir qu'une idée pouvait vraiment changer les habitudes des gens au quotidien.

Une idée qui fait tilt

À l'époque de Coyote, une décision gouvernementale interdit les détecteurs de radars. En discutant avec le ministère de l'Intérieur, on évoque une alternative : afficher les vitesses autorisées en temps réel via GPS. Le problème, c'est qu'aucune base de données centralisée n'existe.

Je pars alors en Israël pour explorer ce que d'autres font en vision par ordinateur. Là-bas, je découvre des technos capables de détecter automatiquement les panneaux de vitesse. C'est la première fois que je me rends compte à quel point l'image peut devenir une source d'info exploitable pour les machines. Ça me reste en tête.

XXII : premières étapes

En 2015, je lance XXII. Au début, on fait de la réalité virtuelle, augmentée, et quelques projets autour de la vision par ordinateur. On propose des services, on répond à des besoins spécifiques. C'est une période super formatrice. Mais au fond de moi, j'ai envie de construire quelque chose de plus stable, de plus long terme.

Changer de cap pour créer CORE

En 2020, je prends une décision un peu radicale : j'arrête les prestations de service pour me concentrer à 100 % sur un produit. Ce sera CORE, une plateforme logicielle de vision par ordinateur.

L'idée, c'est de proposer un outil simple et efficace pour analyser des flux vidéo en temps réel. Pas de gadgets, pas de matériel à vendre. Juste un logiciel utile pour les gens sur le terrain — dans les magasins, les gares, les sites sensibles…

Mon objectif n'est pas de remplacer les humains, mais de les aider à voir plus vite, à repérer ce qui compte, à intervenir au bon moment. C'est ça, pour moi, l'intérêt de la tech : être un appui, pas une fin en soi.

Grandir sans perdre le sens

Depuis, XXII a bien évolué. On a grandi en France, et depuis peu, on essaie de se développer à l'international, notamment aux États-Unis et au Moyen-Orient. Ce sont des marchés exigeants, mais ils partagent les mêmes enjeux : sécurité, supervision, efficacité sur le terrain.

Même en allant plus loin, je tiens à ce qu'on garde nos principes : un produit sobre, utile, respectueux de la vie privée. On essaye de faire les choses proprement, sans en rajouter.

L'équipe et les valeurs qui m'importent

Ce qui compte le plus pour moi aujourd'hui, c'est l'équipe. On vient de parcours très différents, et c'est une richesse. J'essaie de créer un environnement où chacun peut proposer des idées, tester des trucs, apprendre.

Je n'ai pas la science infuse, et je me plante encore souvent. Mais je crois qu'on progresse ensemble, pas à pas. Je parle régulièrement de notre vision, parfois un peu à l'improviste, parce que je pense que la tech doit rester proche des gens, compréhensible et accessible.

Je n'ai pas envie d'une IA toute-puissante. Je veux des outils utiles, concrets, au service des humains. C'est ça qui m'a toujours motivé — et qui continue de me faire avancer.

Olivier Dellenbach, qui êtes-vous ?...

À l'âge de 64 ans, ma carrière dans le domaine du logiciel et de la technologie s'étend sur près de quarante années. J'ai découvert l'informatique durant mes études à Polytechnique et j'ai décidé d'en faire mon métier. À une époque où l'informatique était encore peu répandue dans les écoles, j'ai rapidement été attiré par ce domaine en pleine expansion.

Après avoir obtenu mon diplôme, j'ai travaillé pendant deux années chez GSI, une société de services informatiques. Cette expérience m'a rapidement convaincu que le conseil n'était pas ma vocation. J'ai donc décidé de créer ma propre entreprise, Nat System, spécialisée dans le développement de compilateurs et d'outils technologiques avancés.

Mon travail a rapidement attiré l'attention de Microsoft aux États-Unis, qui nous a sous-traité le développement de compilateurs Pascal et C++. Cette collaboration m'a conduit à passer un an à Seattle pour développer un produit pour eux. De retour en France, j'ai consacré près de huit années à développer notre système d'outils de développement pour les grands comptes, à une époque où les entreprises passaient des architectures mainframe aux architectures PC.

En 1999, après avoir vendu Nat System à un groupe canadien, j'ai été nommé CTO du groupe. Cependant, j'ai rapidement réalisé que travailler au sein d'un grand groupe, même en tant que directeur technique, n'était pas conforme à mes aspirations. J'ai donc décidé de quitter ce poste pour fonder eFront, au début des années 2000, à l'aube de l'ère Internet.

Convaincu que les grands comptes allaient migrer vers des architectures Internet, nous avons développé des outils et des solutions pour faciliter cette transition. Cependant, nous avons rapidement constaté que les entreprises n'étaient pas encore prêtes à refondre leurs applications en client léger. Après une période d'errances, nous avons effectué un pivot stratégique en 2001, en nous concentrant sur le développement d'applications spécifiques. C'est ainsi que nous avons découvert un cas d'usage prometteur dans le logiciel pour le private equity.

En vingt ans, de 1999 à 2019, eFront est devenu le leader mondial dans le domaine du logiciel pour les sociétés de private equity, de gestion de fonds et de capital-risque. Cette entreprise a été vendue à BlackRock en 2019 pour 1,5 milliard d'euros, marquant la fin de ma deuxième aventure professionnelle.

Pour ma troisième aventure, j'avais deux projets en tête. D'une part, ma femme et moi souhaitions investir dans une fondation dédiée au handicap, une cause qui me tient particulièrement à cœur en raison de mon enfant handicapé. D'autre part, je souhaitais redémarrer une nouvelle aventure dans le domaine du logiciel, en essayant de créer un acteur européen majeur dans ce secteur.

Nous avons réconcilié ces deux projets en créant Chapsvision, une entreprise spécialisée dans le traitement de la donnée et l'intelligence artificielle. Ce domaine se prêtait bien à la création d'un gros éditeur de logiciels, avec une forte logique de souveraineté. Il est crucial que la France et l'Europe disposent d'acteurs forts dans cette thématique. Notre fondation « HappyCap Foundation » est aujourd'hui un actionnaire stable de référence, ce qui stabilise le capital de Chapsvision, et elle bénéficie de revenus pour financer ses programmes.

La question de la taille s'est rapidement posée : comment devenir rapidement un acteur important ? Chez eFront, il m'avait fallu vingt ans pour créer une entreprise de dimension internationale, et à mon âge, cela semblait trop long. Il fallait donc raccourcir ce délai. De plus, la technologie évolue si rapidement que les investissements technologiques peuvent devenir obsolètes en vingt ans.

Chez Chapsvision, nous avons adopté un modèle hybride, investissant massivement dans la technologie et développant une plateforme large de traitement massif de données et d'intelligence artificielle. Nous avons ensuite décliné cette plateforme sur divers cas d'usage. Ayant appris chez eFront qu'on ne s'improvise pas spécialiste d'un métier, nous avons choisi d'acheter des sociétés ayant une expertise métier et des accès clients, nous permettant de démarrer rapidement.

En cinq ans, nous avons réalisé une trentaine d'acquisitions, investissant massivement dans notre plateforme technologique. Nous avons remporté le projet OTDH, visant à doter la DGSI et les services de l'État d'une plateforme alternative à Palantir. Nous avons également acquis des sociétés technologiques pour compléter notre offre, ainsi que des sociétés très verticales dans des domaines spécifiques.

Lorsque nous avons commencé à travailler sur le projet OTDH il y a trois ans, je ne connaissais pas du tout le monde de l'État. Ayant toujours travaillé pour des acteurs privés, j'ai dû apprendre les codes et les enjeux de ce nouveau secteur. Pour gérer le risque, nous avons acquis des sociétés proches du régalien, nous basant sur un savoir-faire existant. Sur les trente acquisitions réalisées, une douzaine concernent le monde de la défense, de la police et du renseignement. Nous avons finalement remporté OTDH l'année dernière.

En conclusion, mon parcours professionnel a été marqué par une volonté constante d'innovation et d'adaptation aux évolutions technologiques. Aujourd'hui, avec Chapsvision, nous cherchons à créer un acteur européen majeur dans le domaine du traitement de données et de l'intelligence artificielle, tout en contribuant à des causes qui me sont chères, comme le handicap.

A quoi ressemble votre société aujourd'hui ?

Chapsvision compte 1100 collaborateurs et réalise un chiffre d'affaires de 200 millions d'euros. Environ 40 % de notre chiffre d'affaires provient du secteur régalien, tandis que les 60 % restants proviennent du secteur privé, ce qui constitue un équilibre judicieux.

Notre approche consiste à nous intéresser aux problèmes spécifiques de nos clients, plutôt que de leur imposer des discours technologiques. La technologie doit être perçue comme un support permettant de résoudre les problèmes concrets des clients. Une approche trop technique réduit considérablement les chances de créer de la valeur et de susciter l'intérêt des clients.

D'autre part, la technologie est par nature volatile, tandis que les besoins métiers et les cas d'usage restent relativement stables dans le temps. Cela est particulièrement vrai dans le domaine de l'intelligence artificielle, où 99 % des chefs d'entreprise ou des équipes de management sont convaincus que l'IA représentera un élément de rupture pour eux. Cependant, seuls 3 % à 4 % d'entre eux se considèrent comme matures sur ces sujets. Personnellement, je pense que ce pourcentage est encore plus faible.

Il existe une profusion d'acteurs technologiques qui présentent des technologies avancées, réalisent des preuves de concept et recrutent des data scientists. Cependant, la plupart d'entre eux n'ont aucune idée de la manière d'utiliser ces technologies de façon concrète et de gérer la transformation induite par la technologie. Un acteur qui se contente de présenter une belle technologie a donc peu de chances de passer en production.

Pour avoir un impact réel, il ne s'agit pas de se concentrer sur la technologie en elle-même, mais de vendre des applicatifs que les clients peuvent utiliser et qui, à leur tour, amèneront cette révolution. C'est du moins notre conviction. Dans le petit monde des start-ups, on rencontre trop souvent des personnes qui arrivent avec une technologie qu'ils jugent géniale, mais sans être capables de démontrer la valeur ajoutée qu'ils apportent. Le retour sur investissement (ROI) doit être clairement perçu des deux côtés. En tant que fournisseur de logiciels,

nous vendons un ROI. C'est même le ROI qui déterminera le prix de notre logiciel. Cependant, cette culture n'est pas encore bien ancrée en France, contrairement aux États-Unis.

Si l'on examine pourquoi nos logiciels s'exportent si peu, on constate une habitude française de développer des logiciels avec une culture très technique. Nous vendons ainsi la sophistication et la complexité, ce qui constitue un frein à l'exportation. En vérité, il est impossible de construire un éditeur de logiciels en partant du principe qu'il doit réussir en France. Il faut construire un éditeur de logiciels pour qu'il réussisse mondialement, et ensuite, éventuellement, l'ajuster et l'adapter au marché français. Le contraire est quasiment impossible.

D'une certaine manière, l'État est un acheteur difficile. Il est compliqué de servir l'État en raison des mécanismes d'achat et de la volonté souvent répandue de redévelopper des solutions spécifiques, alors qu'un logiciel standard existant suffirait. C'est une sorte de réflexe pavlovien qui pousse à préférer les systèmes sur mesure. Cela complique l'abord du marché français et incite à développer des solutions spécifiques pour ce marché, ce qui garantit l'échec à l'international.

Actuellement, nous réalisons 15 % de notre chiffre d'affaires aux États-Unis, mais notre objectif est de porter progressivement ce pourcentage à 30 % ou 40 %.

Est-ce qu'un des facteurs de réussite d'une entreprise, ou d'une start-up, n'est pas de comprendre la culture et de comprendre comment s'intégrer dans un marché ?

Je suis convaincu que ce facteur est déterminant. En France, nous observons un nombre excessif de startups tentant de « vendre des glaces en Antarctique ». Notre pays regorge d'énergie et d'une expertise technologique remarquable. Nous disposons de jeunes, talentueux, très bien formés, et d'ingénieurs parmi les meilleurs au monde. Cependant, il est regrettable de constater que ces atouts sont souvent gaspillés.

Ces dernières années, une excitation intense a entouré les startups. Toutefois, sans un mode opératoire solide, le taux d'échec est extrêmement élevé. Un nombre significatif de startups survivent à peine, conservant quelques clients et subsistant grâce à des financements externes, faute d'un modèle de développement viable.

Pour réussir, il est primordial de répondre clairement à la question suivante : quel bénéfice mon produit apporte-t-il aux clients ? Lorsqu'une idée émerge, il ne faut jamais s'auto-convaincre de sa génialité, mais plutôt la tester auprès des futurs clients pour évaluer si ceux-ci en reconnaissent la valeur et sont prêts à y investir. Si la valeur perçue est marginale, les clients ne seront pas disposés à payer cher pour elle.

Ensuite, l'exécution doit être irréprochable : créer une belle histoire est une chose, mais le produit doit impérativement délivrer cette promesse. Enfin, les raisons pour lesquelles les clients français achètent ne sont pas nécessairement les mêmes que celles qui motiveront les clients internationaux à faire de même. Il s'agit ici de marketing produit, un domaine souvent mal maîtrisé par les startups.

De nombreuses startups partent d'une bonne idée, développent un produit, parviennent à conquérir trois ou quatre clients français, et trouvent des investisseurs pour s'internationaliser. Cependant, tout s'arrête là, car le développement à l'international nécessite une expertise spécifique. Il est indispensable de recruter des professionnels compétents dans ce domaine. Sans cela, les fonds des investisseurs sont dilapidés et la startup s'arrête.

Aux États-Unis, il existe un vaste vivier de managers compétents, ayant déjà réussi dans leurs entreprises. Ce type de ressources manque en France. Aujourd'hui, fort de près de quarante années d'expérience, j'ai acquis une vision claire de ce qui fonctionne et de ce qui ne fonctionne pas. Cette connaissance est le fruit de toutes les erreurs possibles et imaginables que j'ai pu commettre au cours de ma carrière.

Cela peut sembler contradictoire : comment sait-on si on est une startup « zombie » qui ferait mieux d'arrêter ou bien si on doit persister parce qu'on est juste en train d'apprendre ?

L'actif principal de l'entrepreneur est son temps. À l'âge de 60 ans, mon principal passif est précisément cette ressource temporelle qui se réduit. Si un jeune entrepreneur consacre cinq années de sa vie à tenter de sauver un projet, même si celui-ci échoue, il aura acquis des compétences précieuses qui lui seront utiles pour ses futures entreprises. Il aura compris ce qui n'a pas fonctionné et pourquoi, ce qui lui permettra de mieux orienter ses prochaines initiatives.

Ensuite, il existe ce que j'appelle le syndrome « Brice de Nice ». Brice, avec sa planche à Nice, attend la vague. Si vous vous trouvez sur un marché petit et sans croissance, vous ne parviendrez à rien. En revanche, si vous êtes sur un marché en pleine expansion, il est crucial de s'accrocher à sa planche et de surfer sur cette vague aussi longtemps que possible.

Ainsi, si vous constatez que vous êtes sur une voie sans issue, il est préférable de ne pas insister. En revanche, si vous êtes sur une tendance porteuse, il est essentiel de vous y accrocher et de tirer parti de cette opportunité.

Qu'est ce qui nous attend pour les 10 ans qui viennent ?

Concernant le monde entrepreneurial, nous traversons une période extrêmement complexe. La France possède un atout majeur : nous sommes reconnus à travers le monde pour la qualité exceptionnelle de nos ingénieurs. En conséquence, de nombreux investisseurs sont enclins à croire en nos histoires technologiques, appréciant notre expertise et notre savoir-faire.

Cependant, notre marché intérieur est profondément déprimé. Les services de l'État manquent cruellement de ressources financières et adoptent une stratégie d'achat qui les pousse à disperser leur budget sur une multitude de projets plutôt que de le concentrer sur

quelques sujets stratégiques. Cette situation me rend assez pessimiste quant à l'avenir immédiat.

En parallèle, une vague absolument extraordinaire est en train de se former : celle de l'intelligence artificielle, avec la « révolution agentique ». Je suis convaincu que de nombreux acteurs vont tenter de surfer sur cette tendance. La première recommandation que je leur adresse est de se tourner vers l'international. Il n'est pas nécessaire de se rendre aux États-Unis pour cela. Il est essentiel de s'établir comme un acteur français souverain, mais de dimension internationale. À mon avis, le modèle industriel à suivre est celui de Dassault.

Quelles sont pour vous les qualités nécessaires pour innover ?

Je perçois l'innovation comme un soutien essentiel à l'entrepreneuriat. L'innovation et l'entrepreneuriat offrent la meilleure impression de liberté que l'on puisse éprouver. Bien que cette liberté soit toujours relative, il est crucial de ressentir que tout est possible et que l'on est entièrement responsable de son propre destin.

Créer ou diriger une entreprise est un sport d'équipe. Plus les collaborateurs sont brillants, plus les chances de succès augmentent. Le rôle de l'entrepreneur est de réunir les talents les plus exceptionnels pour faire aboutir son projet.

L'intelligence réside dans la capacité à reconnaître ce que l'on ignore. La deuxième forme d'intelligence consiste, une fois que l'on a identifié ses propres lacunes, à trouver les experts les plus compétents dans les domaines où l'on est soi-même démuni.

Comme le disait Clémenceau, pour prendre une décision, il est préférable d'être un nombre impair, et trois c'est déjà trop. L'entrepreneuriat est donc également un sport solitaire, où la prise de décision repose souvent sur les épaules d'une seule personne.

L'INNOVATION PAR L'AMIAD

Regard sur l'innovation de rupture, ou comment l'IA de défense bouleverse le champ de bataille

L'intelligence artificielle a parfois été comparée à l'atome. Pas tant pour sa nature que pour son effet. L'atome, on pouvait l'enfermer, le développer en secret, le maîtriser en autonomie. L'IA, elle, est tout l'inverse : elle est fondamentalement ouverte, connectée, dépendante des données, des infrastructures, des usages. Mais ce que ces deux révolutions ont en commun, c'est leur potentiel de transformation absolue et la force de dissuasion qu'elles portent avec elles. Demain, sur le champ de bataille, l'efficacité sera conditionnée par l'intelligence artificielle. Et ceux qui la maîtriseront auront un coup d'avance – comme la dissuasion nucléaire a jadis redéfini l'équilibre des forces.

Il ne s'agit pas là d'une projection lointaine. L'IA est déjà une réalité militaire. Elle est en train de reconfigurer profondément notre manière d'appréhender le combat : du traitement massif des données issues des capteurs à la levée du brouillard de guerre, de la visualisation du théâtre d'opérations à la prise de décision assistée, jusqu'à l'autonomisation progressive des systèmes d'armes. Cette transformation est systémique. Elle repose sur la capacité de la machine à digérer ce que l'humain ne peut plus traiter seul – des millions d'images, une variété de signaux, des déplacements multiples – et à rendre visible l'invisible. Non pas pour marginaliser la décision humaine, mais pour mieux l'éclairer, pour mieux la soutenir.

Cette mutation s'inscrit dans une logique duale. L'IA ne vient pas du militaire. Elle naît dans le civil, dans les laboratoires, les startups, les grandes entreprises du numérique. Et nous devons l'adapter, la militariser, l'outiller pour résister aux contraintes du terrain. Cela impose une réflexion permanente sur l'appropriation de technologies issues d'un monde ouvert, souvent peu conscient des contraintes opérationnelles, pour les adapter à un cadre d'usage critique, souverain et sécurisé. L'IA militaire, ce n'est pas une IA hors-sol. C'est une IA capable de fonctionner dans la poussière, la boue, sous les chocs, dans des environnements où la connectivité n'est pas garantie, où l'adversaire vous écoute, vous observe, vous pirate. Une IA embarquée, robuste et capable de fonctionner avec peu de ressources. Une IA au service de l'efficacité, pas de l'effet de mode.

C’est précisément là que se joue la souveraineté. Car si demain, l’IA structure les systèmes de décision, elle devient un levier de puissance stratégique. Et ce levier, on ne peut pas le confier à d’autres. Ce n’est pas qu’une question de performance – c’est une question de confiance, d’indépendance, de résilience. Il ne s’agit pas de tout internaliser. Mais de comprendre où sont nos dépendances critiques. Et de pouvoir, si nécessaire, tout refaire, tout reconstruire, seuls. Même si c’est moins rapide. Même si c’est moins brillant. Mais librement.
L’innovation militaire, à mes yeux, n’a de sens que si elle est pilotée par le besoin opérationnel. Ce n’est pas une quête de démonstration technologique. C’est une réponse, parfois modeste, mais toujours ciblée, à une problématique concrète du terrain. Une innovation utile, maîtrisée, robuste. Une innovation qui sert, pas qui fascine.

Face à ces enjeux, il nous revient collectivement de tracer une voie exigeante et lucide. L’innovation de défense ne peut être le fruit d’un seul acteur, ni d’une seule vision. Elle demande une articulation fine entre expertise technique, besoin opérationnel et cadre éthique. Cela suppose de croiser les regards, de créer des passerelles durables entre les mondes militaires, industriels, scientifiques et académiques. Car c’est dans cette hybridation, dans cette capacité à conjuguer excellence technologique et finalité stratégique, que se jouent notre crédibilité et notre avance.

L’innovation ne se décrète pas. Elle se construit dans la durée, dans la confrontation des idées, dans la complexité des usages et dans l’exigence des contextes. L’innovation n’est pas une fin mais un chemin.

Bertrand RONDEPIERRE
Directeur
Agence ministérielle pour l’intelligence artificielle de Défense

CONCLUSION

Crédit photo : © Université de Rennes - J.Mignot

Nous espérons vivement que la lecture de cet ouvrage vous aura apporté les enseignements, l'inspiration et les idées qui correspondent à vos attentes. Chacun ayant ses propres aspirations, cet ouvrage peut être lu - et relu - de bien des façons différentes.

Nous tenons à remercier chaleureusement l'ensemble des personnes qui ont contribué à ce livre, pour leur enthousiasme, leur énergie, leur temps, leurs compétences, qui, ensemble, font la valeur et la qualité de l'ouvrage que vous avez entre les mains.

Ce livre est une invitation à agir et nous souhaitons souligner les recommandations suivantes, pour lesquelles nous avons repris les verbatims et remercions tous les auteurs.

1. La réussite passe par la coopération

Tous les parcours inspirants montrent bien que la communauté Cyber est marquée par une grande solidarité et une volonté de collaboration, dans le contexte d'une mission d'intérêt collectif.

La réussite passe par le travail, le sérieux, la rigueur, la passion de l'action : accepter de prendre des risques, oser et expérimenter. Comme l'indique Stéphanie Ledoux, la capacité à apprendre et à coopérer est aussi un facteur clef de succès.

C'est l'alliance réussie entre le ministère des armées, la région Bretagne, les industriels, les académiques et scientifiques (CNRS, INRIA ...) qui fait la force et l'originalité du Pôle d'excellence cyber. Construire des passerelles durables entre les mondes militaire, industriel, scientifique et académique permet de relever de nombreux défis.

2. Faire le pari de la confiance dans l'avenir

Se faire confiance et innover est aussi dans l'ADN de la cyber. L'incertitude caractérise notre époque. Comme l'indique Philippe Silberzahn : « Même si nous ne pouvons plus contrôler l'avenir, nous pouvons contrôler notre façon d'y répondre. Si l'incertitude est anxiogène, cela signifie aussi que l'avenir est ouvert. L'incertitude, c'est aussi l'ouverture et l'opportunité ».

Si les modèles classiques deviennent obsolètes, d'autres les remplacent. « Il ne s'agit plus de chercher la solution idéale en prévoyant l'avenir mais de construire pas à pas des solutions collectives ».

Comme l'explique Benoit Wintrebert, l'innovation, ce n'est pas un simple agencement entre logique d'ingénierie et logique de financement mais une aventure humaine pour construire ces solutions collectives. Diffuser l'innovation cyber, c'est faire le pari de la confiance et partager les émotions pour construire l'avenir ensemble.

3. S'appuyer sur les forces de l'écosystème pour passer à l'échelle

Le livre blanc vise à présenter les principaux dispositifs d'accompagnement utiles pour réussir un parcours d'innovation. Le chemin de l'innovation se construit en marchant avec des mentors. Un créateur entrepreneur ne réussit pas seul : il est accompagné dans cette aventure humaine. Les aspects financiers sont clés : Le Poool, BPI, France 2030, les différents fonds accompagnent ces créations. Comme le rappelle François Lavaste, le passage à l'échelle des PME innovantes nécessite des financements et un environnement favorable, c'est aussi une leçon de l'expérience américaine. Le nombre de startups cyber créées en France et en Europe augmente régulièrement mais très peu passent à l'échelle et beaucoup sont rachetées par des fonds américains. « Il ne suffit pas de créer des startups, il faut qu'elles grandissent, qu'elles aient des débouchés, des financements, qu'elles aient accès à un tissu d'acteurs capable de les porter. » En ce sens tous les témoignages résonnent avec les recommandations du récent rapport de Mario Draghi pour accroitre la compétitivité de l'Europe, renforcer sa base industrielle de défense et relever les défis de la course à l'intelligence artificielle. Cela nécessite de renforcer les investissements dans la capacité d'innovation de l'économie européenne. Du côté des financements publics, l'Europe est au pied du mur pour renforcer son leadership, son autonomie stratégique et sa souveraineté en remédiant à une fragmentation délétère.

4. Rester humble et savoir revenir à l'essentiel

L'innovateur est celui qui a la tête dans les étoiles et les pieds dans la glaise. Les innovateurs n'oublient jamais que la technologie n'a de sens que si elle est toujours considérée au service des clients, pilotée par le besoin.

Comme le rappelle Bertrand Rondepierre, l'innovation, « ce n'est pas une quête de démonstration technologique, c'est une réponse parfois modeste mais toujours ciblée à une problématique de terrain. Une innovation utile, maîtrisée, robuste qui sert et pas qui fascine. »

L'Intelligence Artificielle a commencé à bouleverser le monde du numérique, générant pour la cyber de nouveaux besoins et ouvrant la voie à de nouvelles solutions. Nous avons devant nous un univers rempli d'opportunités. Puisque le contexte que nous traversons constitue un moment propice au changement, alors tâchons de saisir les opportunités !

« Avec le péril croît aussi ce qui sauve » selon le poète allemand Hölderlin.
Ce livre blanc est ainsi une invitation à passer à l'action pour agir ensemble face à la montée des périls, par la confiance et la coopération.

Puisse ce livre servir de guide et d'inspiration à celles et ceux qui souhaitent s'engager dans la voie de l'innovation !

Jean-Luc GIBERNON
Directeur Développement - Sopra Steria

VP Développement industriel
Pôle d'excellence cyber

David ALIS
Président de l'Université de Rennes

VP Recherche
Pôle d'excellence cyber

REMERCIEMENTS

Ce livre blanc est le fruit d'une intelligence collective.
Nous tenons à remercier chaleureusement l'ensemble des contributrices et contributeurs qui ont partagé ici leur expérience, leur vision et parfois leurs doutes – avec sincérité et lucidité. Chacune de ces voix éclaire, à sa manière, les multiples facettes de l'innovation en matière de cybersécurité et d'intelligence artificielle.

Annie AUDIC

PÔLE D'EXCELLENCE CYBER

François BOURRIER SOIFER

SAFRAN AI

Bertrand EMENEUX

AVOXA

Olivier DELLENBACH

CHAPSVISION

William ELDIN

XXII

Olivier EZRATY

Quantum Energy Initiative

Yosra JARRAYA

ASTRAN

Aurélie CLERC

CYGO

Daniel GERGES

LE POOOL

AGENCE INNOVATION DÉFENSE

AID

Agence Defense Innovation

COMCYBER

Commandement de la cyberdéfense

DGA

DGA

Direction Générale de l'Armement

François LAVASTE

TIKEHAU CAPITAL

William LECAT

AURIGA CYBER VENTURES

Stéphanie LEDOUX

ALCYCONIE

Marie PAINDAVOINE

SKYLD

Jean-Nicolas ROBIN

AVOXA

Bertrand RONDEPIERRE

AMIAD

Thierry ROUQUET

ENTREPRENEUR

Frédérique SEGOND

INRIA

Philippe SILBERZAHN

Chercheur - auteur conférencier

Marine THIEBAUD

PÔLE D'EXCELLENCE CYBER

Cyrille VIGNON

GLIMPS

Benoit WINTREBERT

INRIA

PÔLE D'EXCELLENCE
CYBER

www.pole-excellence-cyber.org