



**ERIC GAILLAT EST LE CO-FONDATEUR DES FONDS DE CAPITAL-INVESTISSEMENT CALAO FINANCE.**

## CYBERSÉCURITÉ, UNE ACTIVITÉ TRANSVERSE

Calao Finance investit dans le secteur de la cybersécurité et travaille au lancement d'un nouveau fonds professionnel de capital-investissement (FCPR) dédié aux *start-up* et PME de cet univers. Éric Gaillat, cofondateur de la société de gestion, explique les caractéristiques de ce support d'investissement et les enjeux dans ce domaine de la cybersécurité. L'aéronautique et la défense sont particulièrement concernées du fait du caractère sensible des activités.

Son parcours est celui d'un entrepreneur financier. Il a démarré sa carrière dans la banque d'affaires en 1993 à la banque du Phénix (direction des affaires financières) où il traite des opérations de LBO, avant d'être fondé de pouvoir et co-manager du fonds Phénix Mezzanine. Puis, il a été conseil auprès des associés gérants de la Banque Arjil (Groupe Lagardère). Eric Gaillat a par la suite une carrière d'entrepreneur avec la co-présidence d'Ipen Group (plates-formes d'échange pour banque d'affaires) et de BusinessAngels.com. Il est, en 2000, vice-président de l'*European Business Angels Network* à Bruxelles, l'ancêtre du phénomène du *crowdfunding*. En 2002, il rejoint les fonds Alto Invest comme directeur associé, qu'il quitte en 2010 pour lancer Calao Finance.

Eric Gaillat est par ailleurs président du club du Haut de Bilan du Centre des professions financières et auditeur de l'Institut des Hautes études de la défense nationale (secrétariat général de la défense et de la sécurité nationale).

### Quel est le métier de Calao Finance?

Calao Finance est une société de gestion indépendante dédiée au capital-investissement, agréée par l'AMF. Notre métier est de détecter des PME avec un potentiel de croissance, de les financer et de les accompagner afin d'accélérer leur développement. À un terme de six à huit ans, l'objectif est de céder ces participations avec plus-values. Nous apportons aux PME un financement adapté en capital (actions) ou en quasi fonds propres (obligations convertibles et outils financiers assimilés). Nous veillons à éviter les secteurs subventionnés par le secteur public ou les collectivités locales, car la pérennité de ces financements n'est pas de mise sur plusieurs années et ce, quels que soient les secteurs d'activité aidés et leur enjeu. Les fonds que nous gérons ou conseillons participent au financement de plus d'une cinquantaine d'entreprises employant au total près de 4000 salariés pour un chiffre d'affaires 2015 agrégé d'environ 700 M€.

Nous avons une approche thématique de l'investissement avec des équipes d'experts dédiés. Nous traitons plus particulièrement deux univers, l'art de vivre qui regroupe souvent des activités BtoC dans le luxe, le bien-être ou le *digital media*, et celui des activités stratégiques qui concerne des PME plutôt BtoB et comprend la cybersécurité.

### Pourquoi avez-vous retenu la cybersécurité et comment envisagez-vous l'avenir du secteur?

La cybersécurité et ce qui y contribue sont des secteurs que nous suivons depuis plusieurs années et dont nous observons le développement exponentiel. La France et l'Europe disposent d'ailleurs d'entreprises aux hautes compétences sur ce secteur, *start-up* et

PME, qui sont reconnues pour la qualité de leurs ingénieurs et de leur recherche.

Depuis une dizaine d'années, la cybersécurité est identifiée comme le moyen de se protéger des risques de piratage de données de toutes sortes, d'ailleurs renforcés avec le *Cloud* et les objets connectés. Mais ce n'est pas tout.

À cette vulnérabilité des données s'ajoute maintenant la nécessité de protéger le fonctionnement intrinsèque d'une part exponentielle des activités économiques (paralysie des systèmes ou prise de contrôle) qui utilisent le numérique pour gérer toutes leurs activités avec des automates industriels: transport et logistique, exploitation gazière et pétrolière, distribution d'eau, services financiers, etc. Bref la cybersécurité est devenue un sujet transversal à tous les secteurs économiques.

### La cybersécurité concerne-t-elle aussi l'aéronautique et le secteur de la défense?

La cybersécurité est omniprésente dans tous les secteurs, dans la banque et la finance bien évidemment, mais aussi, bien sûr, dans ce qui touche aux domaines de l'aéronautique et de la défense. À titre d'illustration, nous pouvons citer une de nos participations qui est justement à la frontière de ces univers, Apissys, basée en Haute-Savoie et qui intervient dans le domaine des cartes de conversion de données ultrarapides et de traitement de signaux à très haute vitesse pour les marchés de la défense et de l'aérospatial. Apissys répond ainsi aux besoins croissants de conversion d'un signal réel (type radar) en valeurs numériques pouvant être traitées par ordinateur. Ces besoins sont particulièrement complexes pour les applications ▶

- de défense, par exemple dans la guerre électronique où l'extrême rapidité est nécessaire pour décrypter un signal et son origine, que ce soit pour les avions ou les bateaux. Dans ce type d'application, la sécurité numérique est évidemment clé.

### **Qu'est ce qui caractérise l'investissement dans la cybersécurité ?**

Tout d'abord, à la différence d'autres secteurs d'activités, investir dans la cybersécurité nécessite objectivement une expertise pointue car le sujet est extrêmement technique. C'est pour cela que nous avons constitué une équipe d'experts (*seniors advisors*) de haut niveau mêlant des ingénieurs, des mathématiciens et aussi des praticiens des *business* de la sécurité, comme Yves Véret, Sébastien Héon (par ailleurs *Cybersecurity expert* de la SCOR) ou Jérôme de Labriffe pour le *big data*.

Ensuite, tout en définissant un ensemble de secteurs cibles, il faut rester pragmatique car prétendre que les tendances sectorielles définies aujourd'hui seront identiques dans un an ou deux ans n'a pas de sens au vu du développement de cet univers et des interactions multiples. Il faut donc être aussi en veille et réflexion sur les applications futures. Nous avons ainsi l'organisateur du Forum international de la cybersécurité (FIC), Guillaume Tissier, directeur général de CEIS, comme *Senior advisor*, ce qui nous permet d'avoir une vision assez large des évolutions en cours.

Enfin, outre des ressources financières nécessaires au développement, les entreprises de ces secteurs sont souvent jeunes et, au-delà des technologies qu'elles maîtrisent, elles ont des besoins d'assurances par exemple en termes de marketing et de commercial, notamment pour mieux cerner le marché potentiel. En clair, il faut parfois les aider à définir leur gamme et vendre leurs applications afin, par exemple, qu'elles soient adaptées à des demandes complexes mais aussi courantes (démultiplier les clients via des déclinaisons). Bref, il faut être un investisseur entrepreneur : financer et accompagner.

### **Quelles sont les principales caractéristiques de votre fonds « cybersécurité » ?**

Il s'agit d'un fonds professionnel de capital-investissement (NDLR : à ne pas confondre avec un FCPI, Fonds commun de placement Innovation) dont la politique d'investissement se caractérise par une approche financière d'investisseur et opérationnelle de développeur, à la manière d'un incubateur/accélérateur. Nous déploierons une démarche réactive avec des prises de participations minoritaires dans des délais rapides, ayant éventuellement vocation à devenir majoritaires.

Ce fonds vise à devenir actif et structurant sur le domaine de la

**La plupart de ces sociétés [de cybersécurité] se survalorisent. Cela s'explique notamment par le regard porté vers les valorisations américaines où le marché potentiel est évidemment beaucoup plus important. Également, les acteurs du secteur savent qu'il y a du potentiel dans leurs activités et parfois font monter les enchères ! Sur ce sujet nous « rééquilibrons » la négociation.**

cybersécurité, en France et en Allemagne notamment. Nous nous adressons à des investisseurs français ou européens ; l'équipe investissant à titre personnel avec des intérêts en ligne avec ceux des autres investisseurs et un *hurdle*<sup>1</sup> de 8 %.

Comme évoqué, nous nous appuyons sur une équipe d'experts robustes et le fonds dispose d'un comité stratégique visant à définir et actualiser les axes de développement prioritaires et à apporter un regard extérieur pertinent sur la stratégie du fonds.

### **Quelles sont les cibles d'investissement ?**

Nous avons identifié de nombreuses PME en Europe relevant de cet écosystème et ciblé quatre principaux axes : l'identité numérique et ses applications ; la protection des réseaux ; la vulnérabilité et le comportement des systèmes et, enfin, la surveillance des menaces et de la sécurité grâce aux *big data*.

### **Quel est le profil des investisseurs du fonds ?**

Il s'agit d'investisseurs dits avertis ou professionnels (le fonds n'est pas ouvert au grand public), plutôt des grands comptes et des *family offices*. Pour les industriels du secteur, un tel fonds permet également de suivre l'évolution de l'écosystème, voire identifier des synergies avec leurs propres activités.

Il est à noter que ce fonds est éligible au dispositif dit *corporate venture* de la loi de finance rectificative 2015, dont le détail sera précisé par décret. Ce dispositif vise à inciter les entreprises à allouer une

partie de leur trésorerie dans des fonds d'investissement comme le nôtre et de pouvoir amortir comptablement cet investissement sur cinq ans, ce qui est évidemment un gain substantiel.

### Comment fonctionne ce FPCR sur le plan financier?

Le fonds interviendra principalement en fonds propres et quasi-fonds propres dans des opérations de capital-risque et de capital-développement. L'objectif est de rester au capital entre six et huit ans, et cela peut aller jusqu'à dix ans, avec des sorties effectuées soit à l'occasion d'une fusion, par cotation boursière, par la reprise de participation par un autre fonds, ou encore lors d'un LBO du management.

Un premier *closing* d'une trentaine de millions d'euros est en cours et nous visons cent à cent cinquante millions pour une vingtaine de cibles.

### Qu'en est-il de la valorisation des entreprises de la cybersécurité?

C'est une bonne question. Beaucoup de ces sociétés ont tendance à se survaloriser. Cela s'explique notamment par le regard porté vers les valorisations américaines où le marché potentiel est évidemment beaucoup plus important. Les acteurs du secteur savent aussi qu'il y a du potentiel dans leurs activités et font parfois monter les enchères! Sur ce sujet, nous « rééquilibrons » la négociation par l'accompagnement que nous apportons aux niveaux de nos experts. En clair, les contacts et autres ouvertures que nous apportons se valorisent aussi. Il ne faut pas oublier une grande règle du capital-investissement : la plus-value future se fait souvent à l'entrée, par une négociation équilibrée, et moins à la sortie en pariant sur des multiples élevés de valorisation à terme.

### Quel est le sort des sociétés après le départ du capital-risqueur?

Notre rôle consiste à consolider ces *start-up* et PME dans leur métier pour les transformer en ETI. Pour certaines, l'avenir se concrétisera par une entrée en Bourse, une fusion avec un autre acteur, l'arrivée d'un autre fonds d'investissement et, pour d'autres, elles pourront s'adosser à un groupe. Dans ce dernier cas, nous considérons qu'il faut leur laisser leur liberté d'action et ne pas les enfermer dans un univers bureaucratique. Selon nous, l'avenir de ces sociétés n'est pas d'être intégré à de grands groupes. Il est très important que ces PME conservent un esprit de jeune société innovante et réactive, comme c'est le cas aux États-Unis.



Les besoins en matière de sécurité et de traçabilité sont amenés à connaître des développements sans précédent dans les années à venir.

### Donc, pour vous, la cybersécurité est un secteur extrêmement porteur?

Oui, sans aucun doute. Les développements numériques actuels sont sources de profits importants mais aussi de risques systémiques majeurs pour l'ensemble de l'économie mondiale.

Dans ce cadre, la nécessité de solutions de « confiance » devient prioritaire pour tous les secteurs économiques, sans quoi les bénéfices économiques de la transformation numérique peuvent être rapidement impactés. Tout ce qui concerne la sécurité numérique, ou y contribue, fait dorénavant partie des secteurs unanimement reconnus comme porteurs de croissance à l'échelle mondiale. Les besoins en matière de sécurité et de traçabilité sont amenés à connaître des développements sans précédent dans les années à venir.

En moins de deux ans, cette thématique d'investissement est passée du stade de la « niche sectorielle » à un « *mega trend* ». Le marché de la cybersécurité est actuellement estimé à 4 milliards d'euros en France et deux faits réglementaire et économique accéléreront son développement dans le secteur financier. D'une part, les entreprises, notamment les banques, en tant qu'organisme d'importance vitale, vont rapidement être obligées d'appliquer des normes de protection définies par l'Agence nationale pour la sécurité des systèmes d'information (ANSSI)<sup>(2)</sup> et, d'autre part, les compagnies d'assurance travaillent d'ores et déjà la manière d'inclure, dans leurs tarifications, la question de la protection des entreprises dans les contrats d'assurance des sociétés. L'assurance comme la réassurance sont concernées. ■

Achevé de rédiger le 29 février 2016.

(1) Hurdle : taux de rendement minimum pour l'investisseur, avant que ne soit déclenché l'intéressement de l'équipe de gestion.

(2) ANSSI : [www.ssi.gov.fr](http://www.ssi.gov.fr). Voir aussi à ce sujet l'étude du Cigref (Club informatique des grandes entreprises françaises) et Futuribles « Entreprises et cyber sécurité à l'horizon 2020 ». Janvier 2015.