Synthèse

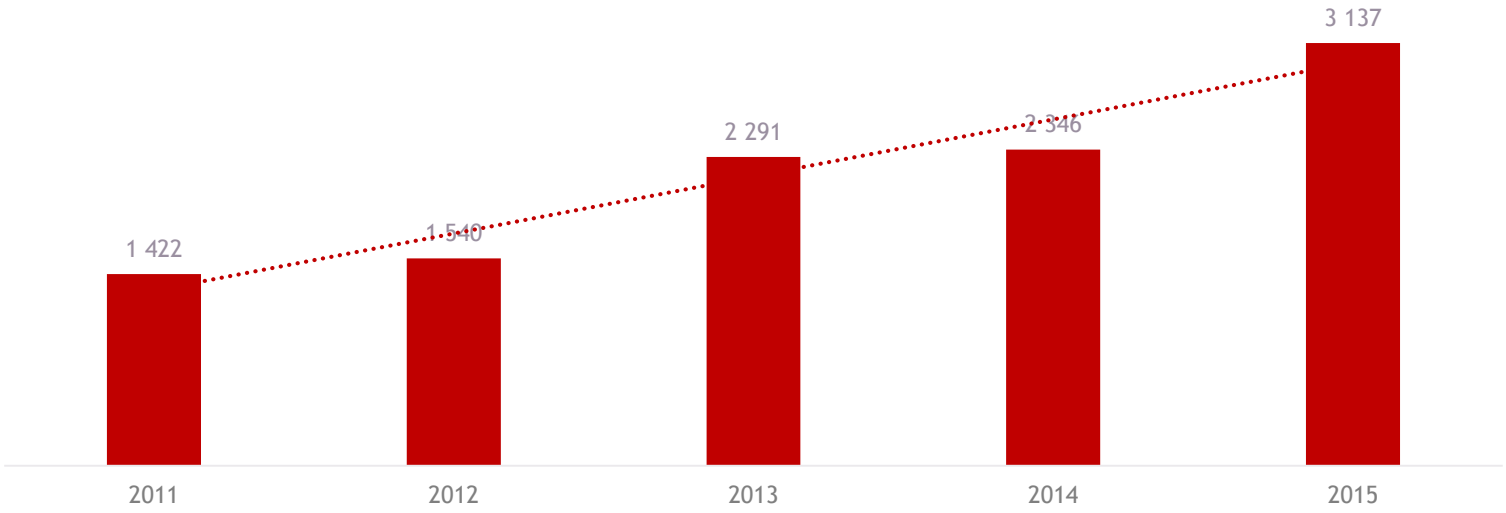
Structure sectorielle de la cyber sécurité

- La filière de la cyber sécurité regroupe des acteurs aux profils divers : groupes industriels diversifiés, start-ups spécialisées ou cabinets de services, etc. Ces acteurs se positionnent sur les trois segments principaux de la filière (édition de logiciels de cyber sécurité et/ou prestation de services dédiés à la cyber sécurité et/ou fabrication de matériel) selon leur cœur de métier, les compétences qu'ils possèdent en interne et leurs capacités d'investissement. Si rares sont les groupes à avoir développé des activités sur l'ensemble des segments, de nombreux acteurs se sont spécialisés soit dans l'édition de logiciels, soit dans la prestation de services dédiés
- Les acteurs du secteur sont essentiellement issus des Etats-Unis, d'Israël ou de France : les deux premiers possèdent une industrie informatique solide et innovante, soutenue par un réseau d'investisseurs privés dynamique et encouragé par un cadre légal propice à l'investissement en capital, le troisième, la France, peut s'appuyer sur l'argument de la « préférence nationale », qui s'impose facilement dans les discours traitant des questions de sécurité
- L'essentiel de la demande, sur le marché français de la cyber sécurité sont des grands comptes (qui sont plus sensibilisés aux questions de cyber sécurité et qui possèdent la trésorerie nécessaire à cet investissement) et des OIV (qui sont soumis à une réglementation précise en matière de sécurité des systèmes d'information). Naturellement, les grands acteurs industriels français issus des secteurs de la télécommunication ou de la défense, ainsi que les SSII nationales, ayant développé des offres transversales en matière de cyber sécurité, apparaissent comme les plus à même de répondre à ces besoins
- Ces acteurs ont construit leur expertise en la matière en développant des compétences en interne ainsi qu'au travers d'opérations de croissance externe, portant sur des acteurs bénéficiant déjà d'une notoriété certaine, au moins sur le marché national. Ils ont aussi noué des partenariats stratégiques avec des acteurs possédant compétences et technologies qu'ils ne peuvent maîtriser ou développer seuls
- Néanmoins, sur ce marché en pleine structuration, un écosystème de start-ups, PME et ETI lutte pour trouver sa place sur le marché hexagonal, s'appuyant sur des architectures organisationnelles moins lourdes et souvent sur un produit phare

Evolution de la demande de cyber sécurité

- Une estimation de la tendance en France

Total des pertes liées à la cyber criminalité en France (1)
(MEUR)



(1) Ont été utilisées les variations annuelles des pertes observées aux Etats-Unis et le calcul des cyber menaces comme % du PIB pour la France en 2014 présentées par MacAfee

Source : Les Echos Etudes, d'après MacAfee - Economic Impacts of Cybercrime et FBI, Internet Crime Complaint (IC3)

- Le taux de croissance annuel moyen constaté aux Etats-Unis est de 22 % depuis 2011 : les pertes constatées, et reportées au FBI, ont ainsi doublé entre 2012 et 2015
- La tendance devrait être similaire en France et le total des pertes en 2015 avoisine les 3 Mds EUR

Synthèse

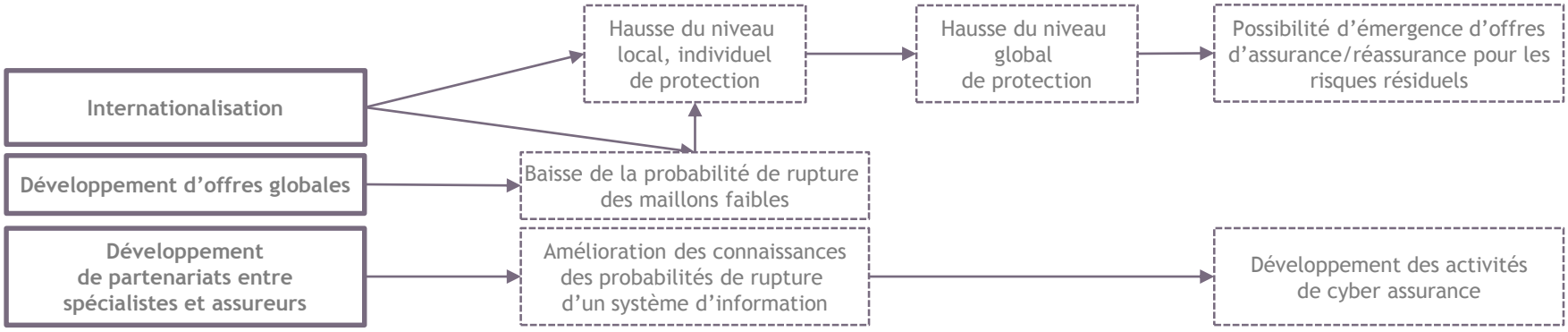
La structuration du marché de la cyber sécurité autour de leaders nationaux

- Le marché français de la cyber sécurité, faisant face à une demande croissante de solutions en matière de cyber protection, tant au niveau national que sur un plan international, s'est progressivement structuré par le biais de grandes tendances :
  - Des impulsions politiques favorables au développement de la filière
  - L'édification de structures de coopération : ces structures, gouvernementales ou non, donnent un cadre commun de références aux divers acteurs du marché, diffusent les bonnes pratiques et permettent les coopérations multilatérales (ou souhaitent le faire)
  - Le rapprochement des acteurs privés via des partenariats commerciaux ou technologiques : ces partenariats bilatéraux permettent notamment aux entreprises qui s'engagent dans cette voie de s'appuyer sur des technologies qu'elles ne maîtrisent pas afin de proposer des offres complètes, ainsi que de profiter d'une base de clientèle existante
  - Des mouvements de croissance externe : les opérations de fusions-acquisitions sur le marché de la cyber sécurité ont connu deux grands mouvements stratégiques depuis le début des années 2000. Les premières opérations de rachat visaient à compléter des technologies, renforcer une offre. A partir de 2012, les opérations de croissance externe ont davantage pour but de renforcer les positions de marchés et interviennent sur des entités de plus large envergure
- Des acteurs de premier plan se dégagent clairement, positionnés de façon stratégique sur le plan des partenariats et ayant racheté des entités déjà établies sur le marché français. Ces acteurs sont des groupes industriels français de la défense et des télécommunications (Airbus, Thales, qui a d'ailleurs repris les activités de cyber sécurité d'Alcatel, Orange, Safran) ainsi que des SSII françaises (Cap Gemini, Atos, CS dans une moindre mesure)
- Les entités de moindre envergure (ETI, PME, start-ups) luttent pour trouver leur place sur ce marché. Elles ont fondé Hexatrust dans cette perspective

Les stratégies poursuivies par les acteurs clés de la cyber sécurité

Les acteurs du marché français de la cyber sécurité mènent des actions stratégiques afin de consolider leurs positions sur le marché :

- L'**internationalisation** est fortement recherchée par les entreprises françaises du secteur, qui peuvent bénéficier des effets d'une relative « préférence nationale », tant qu'elles restent à l'intérieur des frontières de l'Hexagone. Cet effet ne leur permet cependant pas d'atteindre une taille critique, propice aux efforts de R&D et à la densification de l'offre. Les jeunes entreprises françaises peuvent néanmoins avoir du mal à s'exporter, puisqu'elles se confrontent rapidement à des entités américaines ou israéliennes, qui peuvent s'appuyer (entre autres) sur des investissements privés beaucoup plus importants. Ce mouvement d'internationalisation pousse, en premier lieu, les entreprises de l'Hexagone vers les Etats-Unis, où elles vont pouvoir gagner en légitimité, se rapprocher de la frontière technologique et bénéficier d'externalités positives propres aux centres technologiques de premiers plans. Enfin, cette croissance peut être tirée par la demande, puisque les clients internationaux des solutions de cyber sécurité sont en attentes de solutions globales au niveau local. Ainsi, plusieurs entreprises françaises ont ouverts des SOC ou des filiales pour suivre les marchés de leurs clients
- La tendance au **développement d'offres « globales »**, c'est-à-dire des solutions sur l'ensemble de la chaîne de valeurs, est à relier avec ce dernier point. Les acteurs du secteur tendent à se positionner sur l'ensemble des segments du marché, de l'édition de logiciels à l'aide à l'exploitation. Un symptôme de cette tendance est l'ouverture de nombreux **SOC**, en Europe et dans le monde. Ces offres « tout en un » permettent à certains acteurs de rééquilibrer les rapports de force qui les unissent à de potentiels intégrateurs et qui sont également les prescripteurs des clients finaux
- Le développement d'offres « globales » peut aussi se comprendre comme un mouvement de diversification, **d'ouverture de marché**, puisque un certain nombre de ces offres sont destinées aux **PME et ETI**, qui ne possèdent ni les moyens ni les compétences pour gérer des partenaires divers et des solutions complexes



Source : Les Echos Etudes