AFDEL

Les éditeurs de logiciels
et solutions internet

LIVRE BLANC

CYBER-SÉCURITÉ :
HISSER LES ACTEURS FRANÇAIS AU NIVEAU DE LA COMPÉTITION MONDIALE

JUIN 2014

SOMMAIRE


CYBER
ATTACK
SYSTEMS
ATTACKS
INFRASTRUCTURES
CYBERTERRORISTS
SYSTEM
NETWORK
WATER
CRITICAL
COMPUTER
CYBERWARFARE
CYBER-ATTACKS
INFRASTRUCTURE
TRANSPORTATION
CONTROL
DEVICES
DATA
FACTOR
GOVERNMENT
SECURITY
FEAR
TARGET
DAMAGE
HACKERS
CYBERTERRORISM
PHYSICAL
ENERGY
NETWORKS
CONFLICT
SOFTWARE
REGION
CAUSING
MALICIOUS
SHUT
ANOTHER
SEEN
CERTAIN
ACCESS
INSTALLATIONS
CAUSE
MINUTES
EQUIPMENT
POWER
OPPONENT
DISRUPT
ATTACKED
TARGETS
MAKING
IMPEDE
MONEY
USUALLY
SPECTACULAR
PROFESSIONAL
POLITICAL
CIVILIAN
VULNERABILITY
INFORMATION
FACILITIES
GRIDS
HARD
CODE
INDIVIDUALS
EVEN

EDITO

Thierry Rouquet

Président de la Commission Cyber-sécurité de l'AFDEL

La structuration d'une filière industrielle forte, permettant de maitriser les technologies de cyber-sécurité, est devenue un élément déterminant pour l'autonomie stratégique de la France. En réponse à ce défi, le Gouvernement a décidé en octobre 2013 de consacrer l'un des 34 plans de reconquête industrielle à la cyber-sécurité et il a validé la feuille de route attachée à ce plan au début du mois de juin 2014.

Les buts et les missions de cette feuille de route sont clairs :

- la sécurisation des infrastructures critiques ;
- le développement de la demande en solutions de cyber-sécurité de confiance ;
- le développement d'offres de confiance pour les besoins de la France ;
- l'organisation de la conquête des marchés à l'étranger ;
- le renforcement des entreprises nationales du secteur ;
- la consolidation du tissu industriel trop dispersé (plus de 600 acteurs) pour éviter l'éparpillement.

Si l'AFDEL soutient pleinement la poursuite de ces objectifs, elle souhaite aussi faire entendre la position étayée des éditeurs de logiciels et solutions Internet concernant le plan industriel « Cyber-sécurité » (plan n°33), porteur d'une vision cohérente mais, finalement, stato-centrée des enjeux de la cyber-sécurité.

En l'état, l'AFDEL juge que le plan a davantage pour effet de permettre à des acteurs privés de s'affranchir des « forces du marché » que de les doter de la capacité à s'y adapter et à en profiter. La nécessité d'établir une zone « de confiance », c'est-à-dire un marché pertinent, suffisamment large pour justifier une «base industrielle forte» est, par ailleurs, ignorée.

La France peine aujourd'hui à mettre en œuvre un modèle industriel de la cyber-sécurité au-delà du secteur de la Défense. Tel que défini jusqu'à présent, le soutien des pouvoirs publics aux entreprises de cyber-sécurité reste ambivalent et entraine des conséquences en demi-teinte sur leur dynamique de croissance.

1 Une filière industrielle française trop faible à l'international

La sécurité des systèmes d'information : de la menace aux risques.

Le développement exponentiel et l'ouverture des systèmes d'information, le Cloud computing, l'explosion de la mobilité, le BYOD (Bring Your Own Device), ont généré un niveau de risque cyber-sécuritaire inédit et parfois insoupçonné. La nécessaire ouverture des systèmes de pilotage et de contrôle des processus industriels ou de distribution d'énergie (SCADA) met en évidence la vulnérabilité de ces systèmes et les risques associés. L'avènement annoncé de l'Internet des Objets fera passer l'acuité de ce problème à un niveau encore supérieur.
L'affaire PRISM mais aussi, plus récemment, la polémique en France née de l'article 20 de la Loi de Programmation Militaire (LPM), relatif à la surveillance électronique, rend visible l'activisme des agences gouvernementales et met en lumière le caractère géostratégique et les enjeux de souveraineté de la cyber-défense.

Des protagonistes d'ordre différent sont concernés :

- **les Etats** et tous les acteurs publics ou privés qui ont la responsabilité de gérer des infrastructures vitales pour le pays ;
- **les entreprises** dont le niveau de dépendance aux technologies de l'information est de plus en plus important et qui font face à une concurrence de plus en plus globale ;
- **les individus** dont les données personnelles sont de plus en plus souvent digitales, et qui se posent des questions fondamentales de protection de la vie privée.

Les menaces sont elles-mêmes multiformes : espionnage, déstabilisation, atteinte à la réputation, vol, etc. Pour les entreprises et les Etats, elles sont le plus souvent ciblées. Leurs origines varient et leurs auteurs jouissent d'une forme d'impunité en raison des difficultés à les identifier et à les localiser. Certaines attaques récentes ont eu un retentissement très important qu'il s'agisse du vol de 40 millions de numéros de carte de crédit chez TARGET (second distributeur américain) ou du vol de données client à l'éditeur Adobe ou à l'opérateur Orange.

Les logiciels de cyber-sécurité : un maillon critique de la chaine de sécurité

La protection passe par des mesures organisationnelles en matière de traitement de l'information, par la diffusion de bonnes pratiques en matière de gestion des systèmes d'information et, enfin, par la mise en œuvre de moyens de contrôle, de défense et de surveillance fondés sur des logiciels spécialisés. Ceux-ci relèvent des grandes catégories suivantes :

- **La mise en place d'architectures sécurisés** : segmentation (firewalling), VPN (réseau virtuel), proxys, etc… ;
- **La protection des systèmes et des applications contre les malwares** (virus, spams,…) : IPS, antivirus, Firewalls applicatifs, etc… ;
- **La protection de l'information** : chiffrement, contrôle d'accès, etc… ;
- **Le contrôle des utilisateurs et des utilisations** : gestions des identités et des accès, authentification, filtrage des URL, contrôle des périphériques et des applications, etc… ;
- **La supervision, l'audit de détection de vulnérabilité en amont et l'analyse à posteriori** ;
- **La gouvernance et de la gestion des risques**.

Ces produits peuvent être délivrés sous la forme de logiciels traditionnels, d'appliances (boitiers) et, de plus en plus, sous celle de services cloud. La qualité de ces composants, leur bonne utilisation et la confiance que les acteurs leur accordent contribuent largement au développement de l'économie numérique.

Une domination sans partage

Or, le secteur des logiciels de cyber-sécurité est actuellement dominé par des entreprises américaines et israéliennes. Celles-ci bénéficient d'un écosystème exceptionnel en Californie du Nord et dans la région de Tel Aviv où les startups de la cyber-sécurité foisonnent aux côtés de grandes entreprises. **Dans un cas comme dans l'autre, les pouvoirs publics ont su attirer investisseurs, entrepreneurs et chercheurs** pour enclencher un cercle vertueux dont le résultat est un leadership technologique et une domination commerciale mondiale. Non seulement il s'agit d'un des secteurs les plus dynamiques du domaine des technologies, fortement créateur d'emplois qualifiés, mais c'est aussi un formidable moyen d'influence géopolitique. C'est, enfin, un moyen très efficace de développement des compétences indispensables pour exister dans un monde ou la cyber-sécurité déterminera les rapports de force dans les conflits de demain.

Une Europe en ordre dispersée, une France concentrée sur ses besoins domestiques

Dans le même temps, dans le monde de l'« après Snowden », la plupart des individus manifestent une grande inquiétude face à des déclarations du type de celle de l'ancien Directeur de la CIA, David Petraueus, au sujet de la manière dont pourraient être surveillées les nouvelles « smart homes », dans lesquelles les objets connectés se multiplieront.

" Items of interest will be located, identified, monitored,and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters - all connected to the next-generation internet using abundant, low-cost, and high-power computing, " Petraeus said, " the latter now going to cloud computing, in many areas greater and greater supercomputing, and,ultimately, heading to quantum computing. "

Source : www.wired.com/dangerroom/2012/03/petraeus-tv-remote/

Face à cette situation, l'Europe agit en ordre dispersé, chaque pays ayant sa propre stratégie. **La France fait preuve d'un volontarisme remarquable et les pouvoirs publics semblent avoir pris la mesure des enjeux. Mais, ce volontarisme se traduit malheureusement par une vision restrictive, voire protectionniste du rôle des « industriels », éditeurs de solutions de sécurité que l'on voudrait cantonner à la satisfaction de marchés domestiques de niche quand il faudrait en faire des éléments actifs d'une stratégie d'influence ambitieuse**. L'analyse de la mondialisation devrait au contraire conduire la volonté publique à attirer les acteurs privés et, ainsi, à dynamiser un véritable écosystème dont émergerait des acteurs de dimension européenne ou mondiale.

Le plan cyber-sécurité de la nouvelle France industrielle (plan 33) propose de façon louable différentes mesures visant à bâtir un « socle industriel » dans le domaine de la cyber-sécurité. Mais, la situation est telle que ces mesures ne suffiront pas à doter le pays de la capacité d'exister, c'est-à-dire à détenir une autonomie stratégique suffisante, dans le monde cyber-sécuritaire d'aujourd'hui et de demain. Non seulement elles ne suffiront pas à assurer de façon pérenne la sécurité des entreprises et des administrations françaises mais, en outre, comme tout se tient, elles ne permettront pas de créer des emplois sur le marché national et de rayonner sur les marchés internationaux.

Pour l'AFDEL, il est donc urgent et essentiel que s'ouvre un dialogue avec les différentes parties prenantes, afin de définir et de mettre en œuvre une politique industrielle de la cyber-sécurité à l'ambition renouvelée.

2 Standards et qualifications : une offre encore trop peu lisible

Comme les autres logiciels, ceux qui sont spécialisés dans la cyber-sécurité se caractérisent d'abord par des critères technico-fonctionnels (fonctionnalités d'administration, capacité à s'intégrer dans l'infrastructure existante…), par des critères économiques (coût d'acquisition, de mise en œuvre et d'opération) et par des critères liés à l'éditeur lui-même (pérennité, stratégie, moyens, canaux de vente, services…).

A cet ensemble de critères « classiques », il convient d'en ajouter deux, plus difficilement objectivables. Le premier concerne la qualité de la solution en termes de sécurité alors que le second concerne la confiance dans l'impossibilité de contourner la solution.

L'offre technologique est-elle adaptée aux risques ?

L'acheteur doit pouvoir bénéficier de **la preuve que la solution remplit effectivement ses objectifs de sécurité** et en particulier qu'elle est capable de résister au niveau de menace pour lequel elle est conçue.

C'est l'objet des standards internationaux qui permettent de certifier que les caractéristiques d'un produit de sécurité sont bien en rapport avec le niveau de sensibilité des éléments qu'il protège (Critères Communs EAL (ISO 15408), FIPS_140). Bien que coûteuse et relativement lourde, l'obtention de ces certifications sur un périmètre représentatif de l'utilisation réelle du produit est un critère important de choix d'un produit de sécurité.

La solution de sécurité peut également être évaluée par des approches spécifiques à base de tests de pénétration ou de tests à l'état de l'art. Des sociétés spécialisées, comme la société américaine NSS, réalisent de telles évaluations à la demande des éditeurs ou des clients finaux. Ces dernières sont couteuses et doivent être réalisées de manière récurrente pour correspondre en permanence à l'évolution des menaces et de la solution elle-même.

L'offre technologique est-elle digne de confiance ou est-elle contournable ?

Dans le même temps, l'acheteur est en droit d'attendre **que la solution de sécurité soit exempte de moyens de détournement**, qu'il s'agisse de portes dérobées dans les composants de chiffrement qui pourraient être utilisées pour faire fuir de l'information ou de vulnérabilités intentionnellement maintenues dans un logiciel afin de permettre l'exécution d'un malware donnant accès aux ressources que la solution prétend protéger.

Suite aux révélations d'E. Snowden, la presse a largement relayé l'information selon laquelle la NSA imposerait couramment aux éditeurs et aux constructeurs américains la mise en place de moyens de détournement dans les composants de sécurité et d'infrastructure, facilitant ainsi considérablement sa capacité d'interception.

En pratique, et au-delà de ces assertions, l'assurance que la solution est exempte de moyens de détournement ne peut être établie que sur la base d'un examen approfondi du logiciel

(reverse engineering, audit du code source) et sur celle d'un contrôle strict de son processus d'industrialisation. Or, **il n'existe pas de standard internationaux en la matière et cette « garantie » ne peut être donnée que par l'éditeur lui-même ou par un tiers « de confiance »**.

En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) assure le processus de qualification des produits de sécurité en se fondant sur des évaluations dont la profondeur varie en fonction du niveau de sensibilité des éléments à protéger. Cette qualification s'appuie, d'une part, sur la certification critères communs de la solution dans un cadre d'utilisation réel et, d'autre part, sur des exigences complémentaires notamment en matière de cryptographie. C'est donc l'ANSSI qui atteste à la fois de la pertinence de la solution dans un contexte donné et de la confiance que peuvent lui accorder ses utilisateurs. **Pour l'éditeur, le processus de qualification est particulièrement engageant, car il doit donner accès à des éléments très sensibles allant jusqu'au code source. En pratique, en France, seuls les éditeurs français sont susceptibles d'accepter cette contrainte.**

Des solutions technologiques différentes retenues selon les enjeux

Sur le terrain, différentes catégories de solutions de cyber-sécurité sont déployées et mises en œuvre :

- Celles qui sont destinées à **la protection des systèmes gouvernementaux** et qui doivent obligatoirement être qualifiées pour les systèmes et les données « classifiés » (Confidentiel Défense, Secret Défense). Elles sont vendues en faible quantité et à des prix élevés par les industriels de Défense, à l'abri de la concurrence internationale. Leur qualité première est d'être agréée pour l'utilisation qui en est faite, et elles n'ont pas à répondre aux contraintes d'évolution rapide des produits commerciaux. Ce faisant, elles peuvent se permettre d'imposer des contraintes fortes d'utilisation, justifiées par les enjeux de sécurité. **Leur modèle économique diffère radicalement de celui des solutions commerciales puisque la R&D est financée sur des fonds publics et que, le nombre de clients potentiels est très limité.**
- Celles qui sont destinées à **la protection des infrastructures et des données dites « sensibles »**, bien que non classifiées, des entreprises et administration qui gèrent des infrastructures critiques. Celles-ci doivent, en application du Référentiel Général de Sécurité édité par l'ANSSI, être qualifiées (niveau standard) pour attester à la fois de leur robustesse en matière de sécurité et de leur niveau de confiance. Par définition, il s'agit d'un marché limité à la France et à sa zone d'influence/de confiance qui, bien que plus important que le précédent, reste de taille modeste. En outre, **ces entités ne choisissent de se conformer aux exigences du RGS en retenant des solutions qualifiées que si ces dernières restent concurrentielles (prix, performances, fonctionnalités) par rapport à l'offre du marché.**
- Celles qui, représentant l'immense majorité du marché, sont destinées au **marché global des entreprises et des administrations**, grandes ou petites. En fonction du contexte et de leur culture, **a majorité des clients optera pour une solution de sécurité en fonction de sa simplicité de mise en œuvre et d'intégration, de son niveau technologique, de son rapport prix/performance et de la réputation de son éditeur**. Une partie d'entre eux, souvent les plus sensibilisés aux risques, prendront également en compte les critères de certification (EAL, IPS), voire la qualification ANSSI.

Au total, l'offre française intègre peu de standard et se fonde sur une qualification ANSSI qui la limite au marché hexagonal.

Le caractère subjectif de la confiance

La notion de « confiance » dans une solution de sécurité recoupe trois notions dont l'importance relative dépend de la nature et de la criticité des infrastructures ou des informations protégés :

- Sa « **compétitivité** » qui regroupe à la fois les aspects de fonctionnalité, d'exploitabilité ou d'intégrabilité complétés par la pérennité et la qualité de service ;
- Sa « **sécurité** » qui caractérise la capacité de la solution à assurer la protection contre le type de menace pour laquelle elle est conçue ;
- Son « **intégrité** » qui caractérise l'absence de moyens de contournement, que ces moyens soient insérés par l'éditeur lui-même ou sur demande expresse d'un acteur tiers, (par exemple la NSA dans le cas d'un acteur d'origine américaine.)

La « compétitivité » est facilement évaluée par les acheteurs selon une grille de lecture équivalente à celles des autres solutions IT. La « sécurité » peut également se mesurer de manière objective au moyen de la conformité aux standards ou d'évaluations spécifiques. L'« intégrité », en revanche, ne s'évalue que de manière relative, par rapport à la réputation de l'éditeur lui-même, à son pays d'origine, voire à une qualification nationale dont la valeur se limite aux frontières du pays.


PASSWORT
123456

3 Le marché de la cyber-sécurité déjà aligné sur la dynamique des sociétés d'hyper-croissance

A l'exception des produits gouvernementaux qui s'adressent à un marché domestique étroit, très réglementé et peu concurrentiel, **le marché des logiciels de cyber-sécurité est donc un marché mondial extrêmement concurrentiel dans lequel, comme pour les autres logiciels d'infrastructure, les mots clés sont : investissement, innovation, internationalisation**. Il s'agit d'un marché horizontal dans lequel il n'y a pas, à l'exception de certains segments, de spécificités « régionales » en matière technico-fonctionnelle.

Un marché mondial engagé dans la course à la taille critique

Les acteurs de ce marché mondialisé sont :

1. Les grands éditeurs de solutions d'infrastructure (système, réseau, middleware) : Microsoft, isco, EMC, IBM, Intel, HP Oracle… Ils intègrent en permanence des mécanismes et des solutions de sécurité dans leurs offres, produits et services et, à cette fin, mettent en œuvre un modèle de développement fondé sur l'acquisition de sociétés technologiques.

Exemple d'acquisitions récentes (en milliards de dollars –B$) :

Acquéreur	Cible	Valorisation
Cisco	SourceFire	B$ 2,7
Dell	SonicWall	B$ 1,2
Intel	McAfee	B$ 7,7

2. Les « pure players » internationaux qui, à l'image de Symantec, RSA, ChekPoint ou Fortinet s'appuient sur des offres leaders dans les segments matures de la cyber-sécurité (antivirus et firewalls par exemple), ainsi que sur des marques et des réseaux de vente mondiaux. Ceux-ci, tirant partie de réserves de cash très importantes, se développent également par acquisition de sociétés spécialisées qui leur permettent d'élargir leur offre, et à qui ils apportent de la notoriété et un accès démultiplié au marché.

3. Les très nombreuses sociétés spécialisées dans une technologie ou dans une solution innovante, dont la vocation est d'être rachetée par l'un des acteurs précédents ou, plus rarement, de devenir un acteur de la catégorie 2.

Certaines de ces sociétés connaissent des succès remarquables et deviennent en quelques années des leaders mondiaux avec des revenus de plusieurs centaines de millions de dollars et des capitalisations boursières de plusieurs milliards.

L'apparition rapide de leaders mondiaux

Le contexte boursier aux Etats Unis et les progrès réalisés dans la prise de conscience des risques cyber-sécuritaires entretiennent une importante dynamique d'investissement dans les startups positionnées sur ces technologies.

Les schéma de développement sont toujours plus ou moins les mêmes : innovation technologique et/ou marketing, levée de fond successives de plusieurs dizaines de millions de dollars, arrivée d'équipe de dirigeants très expérimentés et projection très rapide à l'international. En 5 ans, celles qui réussissent sont rachetées ou introduites en bourse pour plusieurs milliard de dollars. Elles y trouvent les ressources qui leur permettent d'accélérer leur développement international et d'atteindre la taille critique.

Le secteur de la protection réseau (Firewall) est caractéristique de ce modèle de croissance.

Au tournant des années 2000, le segment était largement dominé par la société israélo-américaine Checkpoint qui vendait des Firewalls logiciels à installer sur des serveurs. Créée en 1997, la société Netscreen fut la première à intégrer le proposer le Firewall sous la forme d'une appliance (le logiciel firewall est intégré dans un boitier). Elle connut en quelques années une croissance ultra rapide, lourdement financé par des investisseurs en capital-risque. En 2002, année de de son introduction sur le Nasdaq (pour lever 160M$) son chiffre d'affaire dépassait les 100M$. Deux ans plus tard, en 2004, Netscreen était rachetée par Juniper pour presque 4B$.

Peu après, Fortinet, créé en 2000, eu l'idée d'intégrer non seulement le firewall mais aussi l'antivirus dans l'appliance pour réaliser la détection de virus « à la volée » (appliance UTM). Cette innovation incrémentale, valorisée par une forte agressivité commerciale et une projection très rapide à l'international, fut la base de sa réussite exceptionnelle. En 2009 la société réalisait déjà un chiffre d'affaires proche de 300 M$. Sa capitalisation boursière est aujourd'hui d'environ 3,5B$.

A son tour, Palo Alto Networks, créé en 2005 par un vétéran de Checkpoint et de Netscreen, proposa une appliance Firewall capable de reconnaitre les applications communiquant sur le réseau et permettant, ainsi, de les contrôler. Son succès fut fulgurant. En 2012, la société réalisait un CA de 180 M$. Elle est entrée en bourse cette même année, réalisant au passage une levée de 260M$. Sa capitalisation tangente désormais les 3 B$.

Plus récemment encore, FireEye, introduisit une appliance de détection des malwares (Advanced Malware Detection). Portée par une croissance météorique, la société est rentrée en bourse fin 2013 réalisant à cette occasion une augmentation de capital de plus de 300 M$ lui permettantd'acquérir un leader historique du secteur quelques semaines plus tard : la société Mandiant.
La capitalisation boursière de FireEye est aujourd'hui proche de 5B$.

Au travers d'innovations incrémentales, d'une exécution remarquable et d'une utilisation exceptionnelle des mécanismes de financement, ces entreprises sont devenues en quelques années des leaders mondiaux dans le même segment de marché. Il est intéressant de noter qu'elles généraient à peu près toutes un chiffre d'affaire de l'ordre de 100M$ au moment de leur introduction en bourse, qu'elles parvenaient juste à l'équilibre financier, voire qu'elles généraient des pertes (abyssales dans le cas de FireEye) et qu'elles étaient déjà lourdement financées, plus ou moins par les mêmes investisseurs en capital-risque.

Ayant atteint une taille critique, installé leur marque, crée leurs réseaux de vente et pénétré les principaux marchés internationaux, elles transforment leur modèle d'hyper croissance en un modèle d'optimisation dans lequel elles privilégient la génération de cash-flow.

Leurs actionnaires y trouvent leur compte, et réinvestissent dans les entreprises du même type tant le modèle est performant. Leurs clients y trouvent aussi leur compte car, lorsque le marché devient mature, ils disposent de fournisseurs solides, capables de faire évoluer leurs offres en permanence pour répondre tant à l'évolution de leurs infrastructures et de leurs usages qu'au développement de la menace.

4 Une industrie française fragmentée et faiblement attractive pour l'investissement privé

La France compte un nombre important d'éditeurs de logiciels de cyber-sécurité dans tous les grands segments du marché. Leurs solutions, déployées dans de grandes entreprises, ont fait la preuve de leur qualité fonctionnelle. Pour autant, seuls quelques éditeurs ont des CA supérieurs à 10M€ ; la grande majorité d'entre eux peinant à atteindre les 5 M€ de CA. Ces chiffres rendent compte d'une réalité industrielle peu enviable : les PME françaises du logiciel mettent beaucoup de temps à se développer, sont centrées sur le marché domestique et n'atteignent jamais la taille critique.

Les éditeurs Français de la cyber-sécurité (*)

		Chiffre d'affaires				
Thème	**Segments / produits**	**< 3M€**	**5<<10M€**	**10<<20 M€**	**20<<30M€**	**>30M€**
Protection des infrastructures fixes & mobiles	Firewall/ Détection d'intrusion / réseau privé virtuels / Protection contre le déni de service / protection des postes de travail et des serveurs / contrôle d'accès au réseau	The greenbow Seclab 6cure		Ercom	Arkoon-Netasq (Airbus Defence & Space)	Thalès e-security
Protection des applications & des utilisateurs	Firewall Applicatifs / "Deep packet Inspection"/ détection des malware / passerelle mail et web		Vade Retro Olfeo	Denyall-Beeware Qosmos		
Protection des données	Chiffrement / Prévention de la fuite de donnée	Cryptolog Prim'X				
Gestion des identités et des utilisateurs	Système d' authentification / Gestion des accès aux applications / Gestion des comptes à privilèges/ Infrastructure à clé publiques	Netheos InWebo Brainwave LoginPeople Usercube Kleverware	Wallix	Dictao Open Trust Evidian (Bull) Ilex		Gemalto (BU sécurité)
Supervision Audit	Système de gestion des événements de sécurité / scanner de vulnérabilité	Itrust Vigie (GFI Info)				

(*) Hors produits gouvernementaux, hors protection des systèmes transactionnels bancaires, hors carte à puce

Les sociétés appartenant à des grands groupes sont soulignées

Classement réalisé sur la base des travaux de R.Rocroy pour Hexatrust

Si cette situation s'apparente à celle que connaissent les autres compartiments du logiciel d'infrastructure, les conséquences sont encore plus préoccupantes car **la maitrise de ces technologies représente un enjeu de souveraineté**. Le paysage industriel français reste particulièrement fragmenté, et sa capacité à relever les défis de demain demeure beaucoup trop faible.

Pas de modèle industriel français au-delà du secteur de la Défense

Il n'existe pas de « modèle français » des solutions de cyber-sécurité pour servir de modèle de croissance aux éditeurs hexagonaux ou aux investisseurs. Et, il n'y a pas non plus, à l'exception peut-être de Gemalto et de Morpho, de « consolidateur » français susceptible d'acquérir des sociétés de technologie innovantes en les faisant bénéficier de leurs marques, de leurs canaux et de leurs modèles d'affaire.

Les groupes de Défense, s'ils bénéficient de la taille, de la structure financière et d'une vraie culture de la sécurité des systèmes d'information critiques et des produits gouvernementaux, ne disposent pas de marques reconnues sur ces segments de marché (hors Défense). Ils ne disposent ni des canaux de vente ni de la culture du management propre à l'industrie du logiciel. Ils définissent des stratégies fondées sur le retour sur investissement sur la base des cashflow, là ou un investisseur en capital-risque aura pour objectif de réaliser une plus-value actionnariale. **Or, si ce mode de raisonnement est bien adapté au monde industriel, il ne l'est pas pour des sociétés technologiques en forte croissance.**

Une faible attractivité pour l'investisseur privé

L'accès à l'investissement en fonds propres est restreint par le cadre qui est proposé aux investisseurs. Il est pourtant indispensable de disposer au bon moment d'importants moyens en capital pour industrialiser la solution et exploiter la fenêtre d'opportunité permettant d'accéder rapidement aux principaux marchés mondiaux (Etats-Unis, Europe). Pour l'éditeur, il s'agit d'acquérir de la visibilité auprès des influenceurs, de nouer des partenariats stratégiques avec certains acteurs de l'écosystème, de mettre en place des canaux de vente et de signer les premiers clients dans les marchés visés.

Ces investissements très importants, qui visent à favoriser une croissance la plus rapide possible au dépend d'un équilibre économique qui sera recherché ultérieurement, lorsque la taille critique sera atteinte, sont le propre des investisseurs en capital-risque. Mais ces derniers se montrent particulièrement frileux vis-à-vis des sociétés françaises de la cyber-sécurité, **notamment parce que leurs options de sortie du capital après quelques années sont restreintes** :

- Les possibilités de cession de l'entreprise seront limitées par la volonté (légitime) des pouvoirs publics de conserver le caractère français d'une entreprise dont les solutions sont jugées « sensibles », utilisant pour cela sa capacité de contrôle des investissements étrangers. Cela aura pour effet de limiter les prétendants à l'acquisition à des acteurs français (fort peu nombreux) et, à la rigueur, européens, réduisant considérablement le potentiel de plus-value de l'investisseur ;
- Les introductions en bourse restent exceptionnelles dans le secteur (aucune depuis Arkoon Network Security en 2007) et les performances passées du marché Alternext ne leur permettent pas, de toute façon, d'espérer un gain à la hauteur du risque. **A cet égard l'initiative de l'AFDEL en faveur de la création d'un NASDAQ européen pour les valeurs technologiques trouve tout son sens.**

Pour un investisseur prêt à investir dans une entreprise française, il est indiscutablement plus opportun d'investir dans le commerce électronique ou dans un site de social networking, dont les modèles de succès sont connus, plutôt que dans la cyber-sécurité.

Il est vrai qu'en France, l'accès à des sources de financement pour de la R&D est relativement facile s'agissant de financement public, et les programmes de type PIA, Rapid ou FUI sont reconnus pour leur efficacité. En revanche, l'accès à des financements privés est beaucoup plus difficile. Or, si les investissements publics ont un rôle important à jouer, notamment pour soutenir le financement de la R&D, **ils ne peuvent se substituer à des fonds privés, dont les capacités sont infiniment supérieures, pour financer la croissance et le développement international.**

Le soutien ambivalent des pouvoirs publics

La magnitude des révélations d'E.Snowden et l'actualité de l'activité malicieuse conduit légitimement les pouvoirs publics à favoriser l'émergence de solutions « de confiance », d'abord et avant tout pour les opérateurs d'infrastructures critiques mais aussi avec l'espoir que celles-ci soient adoptées par les autres acteurs économiques.

Les pouvoirs publics font preuve d'un réel volontarisme, notamment au travers de l'ANSSI, en matière de structuration et de croissance de la filière française de produits de sécurité. Ce volontarisme se traduit, au travers du processus de qualification, par une définition stricte des exigences de sécurité, appuyée par un cadre réglementaire destiné à favoriser le développement de solutions de confiance pour les entités gouvernementales, les opérateurs d'importance vitale et les entreprises en général. **Un tel contexte présente des avantages certains pour les éditeurs nationaux**. Le label « solution de confiance française» les avantage face à des concurrents souvent beaucoup plus puissants qu'eux mais qui ne peuvent assurer le même niveau de conformité. Il se traduit aussi par des aides directes en faveur des projets de R&D innovants (FUI / Rapid…), ainsi que par un certain activisme destiné à favoriser la consolidation du secteur. **Pour autant, cette démarche peine à prendre en compte les réalités et de la dynamique économique du secteur.**

Les conséquences en demi-teinte de ce soutien sur la dynamique de croissance des éditeurs

Ce volontarisme, bien qu'il permette à beaucoup des acteurs de la cyber-sécurité d'exister, engendre donc des conséquences négatives s'agissant de favoriser l'émergence d'acteurs de taille internationale :

- **Il pousse les éditeurs à concentrer leurs efforts sur la conformité au référentiel défini par l'ANSSI pour accéder aux marchés « sensibles » alors que leurs ressources (forcément limitées) pourraient parfois être mieux employées à la conquête de nouveaux marchés.** Cela est d'autant plus vrai que, l'Europe de la cyber-sécurité n'existant pas, ce référentiel n'a de valeur qu'en France ;
- Surtout, comme nous l'avons vu précédemment, **il limite considérablement les options capitalistiques et donc les capacités de financement de la croissance.**

Les attentes des clients français plutôt susceptibles d'adopter des solutions de dimension internationale

Les entreprises françaises, en particulier les grandes qui se déploient largement à l'international au travers de filiales, privilégieront les éditeurs présents directement ou indirectement dans les principales régions qui abritent leurs filiales. Pour elles, la capacité à disposer du même service dans les principales zones géographiques quel que soit le fuseau horaire est un « must ». Or, indépendamment de la qualité de leurs solutions, les éditeurs français ont, pour la plupart, des difficultés à assurer cette couverture, ce qui les disqualifie aux yeux de ces clients qui devraient pourtant être leurs premières références au service d'une stratégie de conquête.

5 Le succès des modèles américain et israélien

Le modèle éprouvé des startups technologiques

Comme pour le reste des logiciels d'infrastructure, les principaux pôles de développement des solutions de cyber-sécurité sont les Etats-Unis, notamment la Californie du Nord qui regroupe les trois quarts des startups du domaine, et la région de Tel Aviv, en Israël. En Europe, les acteurs principaux sont le Royaume-Uni et l'Allemagne.

Sans surprise, le succès des entreprises de ces écosystèmes se fondent sur :

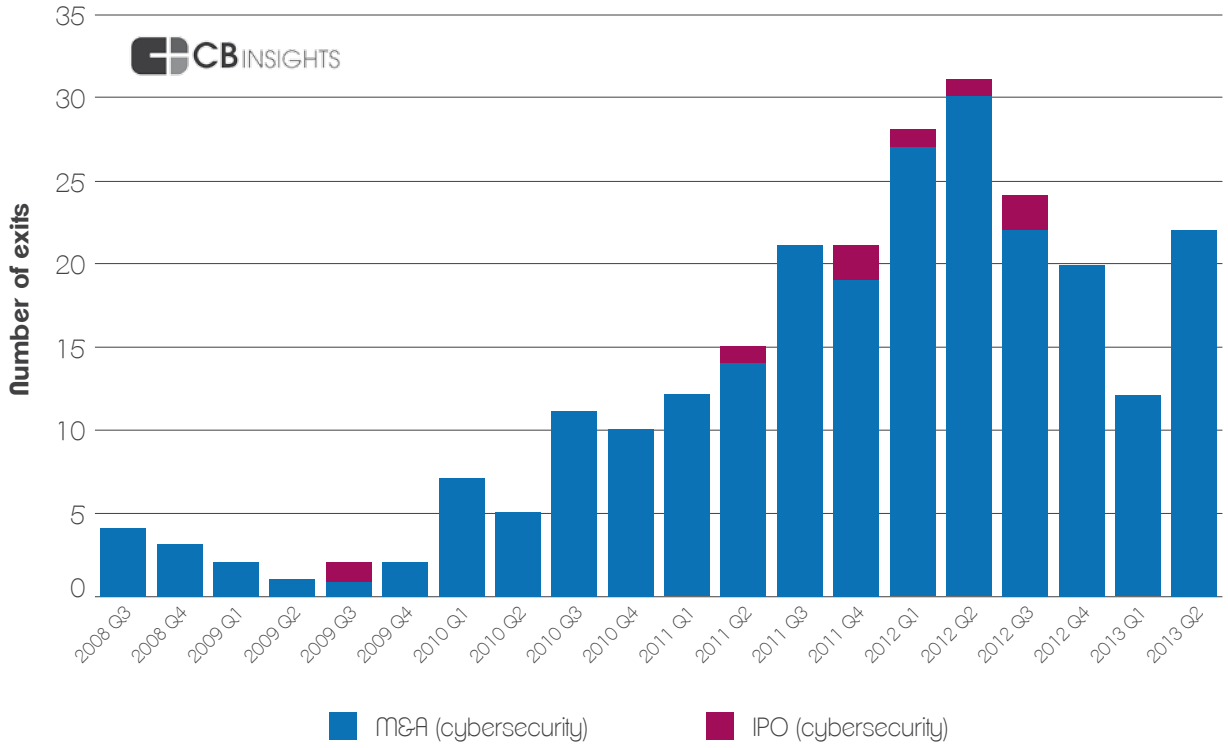
- **Une projection très rapide sur le marché international.** Leur priorité est le marché américain, de loin le plus important et le plus réactif en termes d'appétence pour les solutions innovantes. **Il s'agit d'un passage obligé pour acquérir, auprès des analystes internationaux et de l'écosystème, la visibilité et la notoriété nécessaires au succès, y compris en Europe.**
- **Un accès facilité et massif aux financements en fonds propres** (sans lequel le point précèdent est impossible) **grâce à un cadre très favorable aux investissements en capital**, permettant notamment des possibilités de sortie sous la forme de cession ou d'IPO (introduction en bourse) pour les investisseurs ;
- **Un écosystème riche** de sociétés de technologie, d'investisseurs et de compétences **dont la densité ne cesse de croitre** ;
- **La présence d'acteurs de consolidation** dont la stratégie d'innovation passe clairement par les acquisitions technologiques ;
- La disponibilité d'**équipes de management expérimentées et une très forte culture entrepreneuriale.**

Tant aux Etats-Unis qu'en Israël, les autorités jouent le rôle de catalyseur et optimisent l'effet de levier massif de l'investissement privé. Leur objectif est de créer une filière regroupant toutes les compétences techniques, marketings et managériales, en contact permanent avec les investisseurs privés et les centres de recherches. La dynamique vertueuse qui en découle s'illustre par le réinvestissement des plus-values générées dans de nouvelles entreprises du même secteur et par l'émergence progressive de leaders jouant un rôle de consolidateur. L'ensemble contribue à la création d'emploi spécialisé, de savoir-faire et d'expertise « cyber » non dé-localisables.

Des marchés très dynamiques

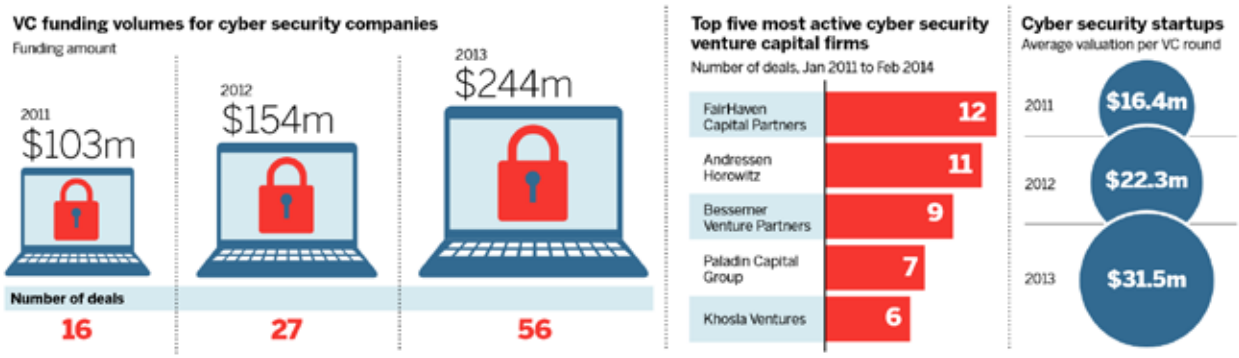
La cyber-sécurité est devenue un des secteurs les plus dynamiques de la Silicon Valley. Les méthodes de protection traditionnelles comme les anti-virus ou les Firewalls ayant montré leurs limites contre les attaques de nouvelle génération, des centaines de startups proposent de nouvelles approches de la protection et attirent des millions de dollars d'investissement. **En 2013, le montant des investissements en capital-risque dans les sociétés de la cyber-sécurité a atteint 1,7 B$** (source : CB Insight). Le dynamisme du marché se traduit par des introductions en bourse pour des valorisations supérieure à un milliard de dollars et par un grand nombre d'opérations de fusion-acquisition initiées par des majors de l'IT (Cisco, Juniper, EMC…) ou par des entreprises du secteur ayant trouvé en bourse les moyens de financer ces transactions.

Le tableau ci-après présente le nombre de transaction dans le secteur depuis 2008 :



Source : CB Insights

D'après PrivCo, un organisme d'étude spécialisé, les financements initiaux (*early stage funding*) du secteur ont bondi de 60% en 2013 et le nombre de startups financées a doublé, alors même que ces sociétés n'ont presque pas réalisé de chiffre d'affaire.



Source PrivCo

Le secteur israélien de la cyber-sécurité affiche lui aussi un niveau record de transactions, que ce soit en matière de financement de startups innovantes, d'opérations de fusion-acquisition ou d'introduction en bourse. Ce secteur est tiré par des pionniers comme CheckPoint, Imperva et même RSA racheté en 2006 par EMC. Il compte un nombre impressionnant de startups prometteuses, parmi lesquelles Seculert, Votiro et Covertix, primées cette année à la RSA conférence de San Francisco, ou encore Cyvera un pionnier de la détection des malware récemment rachetée par Palo Alto Networks. **Les investisseurs du monde entier, s'y précipitent pour profiter des effets de levier financier en matière de fusion-acquisition, voire d'introduction en bourse, de la « silicon valley Israélienne ».**

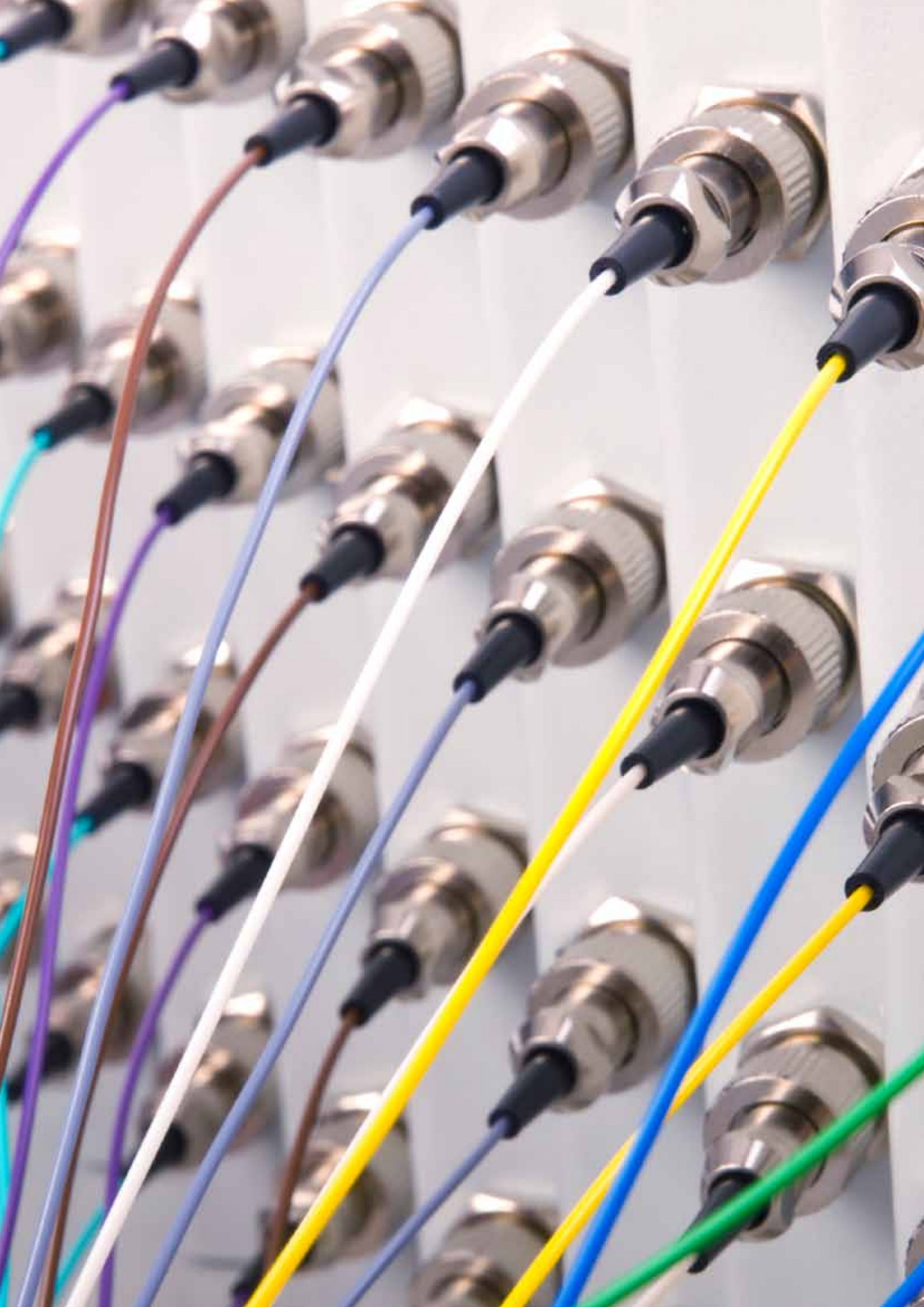
Les pouvoirs publics favorisent le processus, au travers d'investissements publics et de collaborations entre la recherche publique et le privé mais, surtout, en mettant en place un cadre attractif pour les investisseurs privés. Cela concerne à la fois le cadre fiscal, boursier mais aussi l'assurance que les options de sorties des investisseurs ne seront pas limitées (sauf dans certains cas très particuliers).

Les transactions dans la high-tech israélienne

En milliards de dollars (y compris sciences de la vie)

« LES ÉCHOS » / IDÉ / SOURCE : PWC / PHOTO : SHUTTERSTOCK

La création progressive d'une telle filière en France, et l'arrivée massive d'investisseurs privés, 'accompagnerait inévitablement du rachat de sociétés par des acteurs étrangers, mais **elle accélèrerait le développement permanent d'un savoir-faire technique et entrepreneurial jusqu'à permettre l'émergence d'acteurs capables, à leur tour, de consolider des acteurs étrangers.**



6 Hisser les acteurs français au niveau de la compétition mondiale

Le marché des logiciels de cyber-sécurité est, à l'image du marché du Logiciel en général, un marché mondial. Il est tiré par l'innovation, par les évolutions technologiques, par la diffusion des usages et, surtout, par l'évolution extrêmement rapide de la menace. Compte tenu des enjeux et de l'intensité concurrentielle, **les capacités d'investissement des acteurs et les effets d'échelle sont essentiels.**

Dans le même temps, les composants logiciels et matériels qui permettent d'assurer la sécurité des systèmes d'information et de communication des infrastructures critiques représentent un enjeu crucial pour la France. Ils doivent non seulement être à l'état de l'art en terme technico-fonctionnel mais également apporter la preuve qu'ils sont exempts de moyens de détournement, l'affaire Snowden ayant mis en évidence la propension des services américains à imposer à certains fournisseurs de tels moyens.

Les donneurs d'ordre doivent choisir entre des solutions promues par des entreprise mondialisées (ou en voie de mondialisation), disposant de moyens considérables mais qui risquent de comporter des moyens de détournement, ou des solutions « de confiance », venant de petites sociétés françaises aux capacités financières faibles et présentant donc un risque d'exécution et de pérennité.

Le volontarisme des pouvoirs publics permet de faire vivre un certain nombre d'acteurs au travers d'une définition contraignante des exigences en matière de sécurité. **Il manque cependant du réalisme économique qui lui permettrait hisser ces acteurs au niveau de la compétition mondiale et de doter la France de la « base industrielle solide » qu'ils appellent de leurs vœux.**

A cet égard, la feuille de route du plan cyber-sécurité de la nouvelle France industrielle, résultat des travaux du « groupe 33 » piloté par l'ANSSI, propose une série de chantiers dont les objectifs sont louables mais dont l'efficacité globale risque d'être fragilisée par la non prise en compte de deux ressorts essentiels à l'avènement d'une véritable politique industrielle dans ce domaine.

Plan industriel « Cyber-sécurité » : l'AFDEL souhaite une stratégie davantage tournée vers la conquête de l'international.

Elle se **focalise sur la nationalité des entreprises, au lieu de se focaliser sur le développement d'un écosystème dont le centre de gravité serait en France.**

Pour financer de vrais projets de croissance avec un potentiel international il faut attirer des investisseurs privés en leur permettant de rendre facilement liquide leur investissement, soit au travers d'une introduction en bourse, ce qui implique l'existence d'une place de marché européenne, soit en autorisant que certaines des plus belles entreprises nationales aillent se coter aux Etats-Unis.
Il nous faut donc changer de paradigme et autoriser que ces entreprises puissent être des cibles

d'acquisition par des acteurs étrangers. Tant que cela ne sera pas le cas, le nombre très limité d'acquéreurs tirera à la baisse la plus-value potentielle pour les investisseurs en capital-risque et ceux-ci continueront à orienter leurs investissements vers d'autres secteurs, dans lesquels leur capacité ne sera pas bridée.

Certes, la perspective de voir une entreprise technologique de la cyber-sécurité ayant bénéficié d'un environnement national favorable pour se lancer (formation, aide à l'innovation, support de ses premiers clients…) lever des fonds auprès d'investisseurs et se faire racheter par un acteur étranger paraît aujourd'hui encore peu intuitive. Elle ne l'est pas moins que de voir la même entreprise incapable de créer et d'exploiter suffisamment rapidement un avantage concurrentiel par manque de capacité de financement. En effet, dans cette dernière hypothèse, l'entreprise finira immanquablement par végéter. **Elle perdra sa compétitivité vis-à-vis d'acteurs mieux dotés et finira par être incapable de satisfaire les clients sensibles que cette politique de contrôle des investissements était supposée protéger.**

A l'inverse, le développement d'un environnement initial véritablement favorable (innovation, compétences, esprit entrepreneurial, cadre fiscal) encouragera les investisseurs à réinvestir majoritairement leurs plus-values dans de jeunes entreprises de la cyber-sécurité issues du même « écosystème ». Au final, le processus est vertueux. Quand bien même une partie des entreprises passerait sous pavillon étranger, leur centre de R&D restera en France pour être au cœur de l''écosystème ainsi créé. Surtout, ce processus sublimant l'entrepreneuriat et l'innovation incitera les meilleurs éléments à créer leur propre affaire ou à en rejoindre une autre à un stade initial. Il aboutira ainsi au développement rapide d'un écosystème de plus en plus solide et dynamique dont, émergeront des champions nationaux qui, à leur tour, deviendront des consolidateurs internationaux.

Ceci nécessite une volonté politique forte (au-delà de l'ANSSI), un peu d'argent public pour initier le processus (il est déjà là) et des compétences techniques, marketing et entrepreneuriales qui existent et qui se renforceront au fur et à mesure qu'elles se confronteront à un marché mondial.

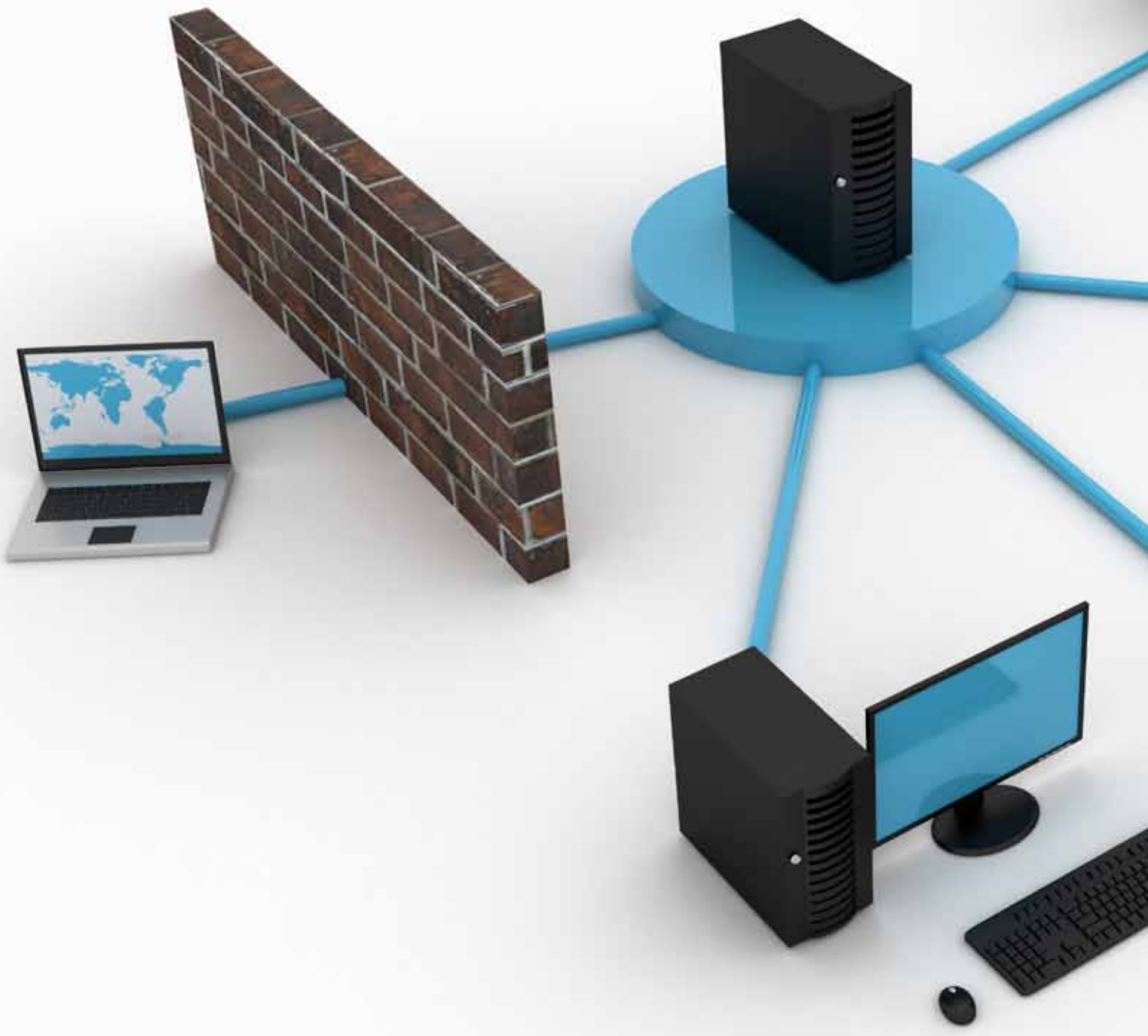
Prendre le risque (calculé) de la « confiance européenne »

La définition restrictive de la notion de « confiance », actuellement en vigueur, est, paradoxalement, susceptible de desservir l'intérêt national. Le périmètre « géopolitique » au sein duquel la notion de confiance des solutions de sécurité pourrait être partagée et dans lequel il serait possible d'envisager la constitution de la « base industrielle forte » que les autorités appellent de leurs vœux doit désormais déborder des strictes frontières de l'Hexagone. A l'évidence le marché français est bien trop restreint et aucun pays tiers n'accepte de se ranger à une définition unilatérale de la confiance.

Il faut donc prendre le risque d'élargir notre définition et de tenter d'y rallier d'autre pays pour créer un marché suffisamment large. L'Europe des vingt-huit n'est sans doute pas un périmètre adapté dans un premier temps car insuffisamment homogène, mais la constitution d'un premier noyau dur, au premier rang duquel devrait figurer l'Allemagne, pourrait être recherchée.

Sans doute cela impliquera-t-il des compromis de part et d'autre, mais si nous avons naturellement besoin de technologies de confiance pour protéger nos intérêts vitaux, celles-ci doivent être compétitives pour satisfaire les besoins de nos entreprises. Pour cela il faut, d'une part, créer avec nos partenaires européens, un grand marché « domestique » et, d'autre part, prendre la véritable mesure des besoins d'investissements, c'est-à-dire rendre attractive la cyber-sécurité française et européenne aux yeux des investisseurs privés.

Enfin, dans le monde multipolaire de la cyber-sécurité nous devons disposer d'entreprises leaders dans quelques segments afin d'exister pleinement dans le jeu des rapports de force entre puissances « cyber ». **A cet égard la conquête de parts de marché doit être reconnue comme un objectif stratégique de la stratégie de cyber-sécurité des pouvoirs publics.**



7. Les recommandations de l'AFDEL

Un marché Franco-Allemand des solutions de confiance

Il faut convenir d'une action concertée des pouvoirs publics et du secteur privé pour approcher nos équivalents outre-Rhin et **convenir avec eux d'une définition commune de ce que doit être une solution de confiance pour nos infrastructures critiques et nos entreprises. Cela passe par la mise en place d'un processus de qualification commun** qui devrait associer étroitement les acteurs du secteur et être conduit par des cabinets indépendants (type CESTI) labélisés par les pouvoirs publics des différents pays.

Il faut en parallèle favoriser les initiatives Franco-Allemandes en terme de collaborations R&D, partenariats stratégiques entre les entreprises et attirer l'investissement privé sur ce type de projet en abondant par exemple les fonds privés via la BPI et son équivalent allemand.

Focaliser les interventions des pouvoirs publics sur l'effet de levier attendu

Les dispositifs d'aide français et européens sont efficaces. Mais, **ils se focalisent en général sur l'innovation technologique sans se préoccuper sérieusement du potentiel de développement et de la capacité d'exécution de l'entreprise aidée** : moyens humains, savoir-faire marketing, leadership, apacité à attirer des investisseurs… Si l'attribution de ces aides a un effet indéniable pour « booster » l'innovation, leur «retour sur inversement sociétal » est réduit lorsque les projets de R&D financés n'ont pas la capacité d'exécution requise pour valoriser commercialement la technologie, et en tirer les dividendes en terme d'emploi mais aussi d'influence internationale.

Il faut **focaliser les aides sur les projets disposant d'un vrai potentiel pour attirer des investisseurs et encourager les développements à l'international** en reconsidérant la manière dont celles-ci sont attribuées.

Attirer l'investissement privé

La capacité d'attraction des investisseurs français et étranger dans les technologies de cyber-sécurité est la clé du succès. Investir dans les startups de la cyber-sécurité en France doit devenir un « must » pour les investisseurs en capital-risque spécialisés dans les technologies.

Le plan industriel « Cyber-sécurité » prévoit la création de fonds d'investissement « cyber ». **Mais, le schéma retenu se limite à des ressources (semi) publiques, donc très limitées en quantité et mobilisées sur la base d'une logique différant significativement de celle d'un investisseur.**

Sur ce point précis, il convient de souligner que l'expérience et l'expertise des participants du groupe n°33 ne couvrent pas le financement en fond propre (VC, bourse) des sociétés de technologie. Or, les ordres de grandeur retenus par le groupe de travail (quelques millions d'euros) ne correspondent pas aux ordres de grandeurs permettant de développer des écosystèmes IT compétitifs.

Selon l'AFDEL, il conviendrait de définir une stratégie permettant d'attirer les investisseurs étrangers, européens en priorité, en les incitant à investir dans la cyber d'origine française; reconnue pour la qualité de sa R&D, le talent des équipes mobilisées et un environnement « business friendly ». Cela suppose d'accepter « les règles du marché » (sorties, fiscalité, attitude générale des pouvoirs publics...) tout en jouant avec elles.

Pour cela, il est essentiel d'encourager les innovations qui ont un potentiel d'applicabilité à court et moyen terme, d'aider à grandir les entrepreneurs de talent et de développer le savoir-faire business (marketing, international) propre à l'industrie du logiciel. Il faut aussi **abandonner l'idée de contrôler les cessions des entreprises du secteur de la cyber-sécurité pour favoriser les sorties des investisseurs et accélérer le cycle investissement/désinvestissement qui permettra de construire un véritable écosystème de chercheurs, ingénieurs, investisseurs et entrepreneurs de classe mondiale**. C'est cet écosystème qui finira par constituer la fameuse « base industrielle » dont nous avons besoin.

Donner la priorité aux PME technologiques et aux startups

Le couple startup technologique/ investisseur en capital est clé pour adopter une position offensive dans le domaine des solutions de cyber sécurité. Dans un marché tiré par l'innovation, les grands groupes n'ont ni l'agilité ni le modèle économique requis pour faire émerger des champions. Contraints par la recherche d'un retour sur investissement sous la forme de cashflow, dans l'impossibilité de valoriser leurs investissements sous forme de valeur actionnariale compte tenu de leur taille ils ne peuvent pas consentir les investissements nécessaires pour des projets risqués. Au-delà de la posture qui consiste à jouer sur la proximité sécurité et défense la solution ne viendra à l'évidence pas des grands groupes même si ceux-ci ont un rôle à jouer notamment dans le domaine des services.

L'AFDEL est volontaire pour travailler au côté des pouvoirs publics, des représentants des laboratoires, de ceux des investisseurs en capital-risque et des organismes de financement public sur ces sujets et initier un dialogue avec les associations professionnelles outre-Rhin.

À Propos de l'AFDEL

L'Association Française des éditeurs de Logiciels et Solutions Internet, AFDEL, a pour vocation de rassembler les éditeurs et sociétés Internet autour d'un esprit de communauté et d'être le porte-parole de l'industrie numérique en France. L'AFDEL est le représentant de la profession d'éditeur de logiciels et de services Internet en France.

Elle compte aujourd'hui plus de 350 membres (CA global : 8,5 Mds€) répartis dans toute la France : grands groupes de dimension internationale dont les premiers français (60 % du Top 100 France en CA), PME et Start-ups.

De statut loi de 1901, l'AFDEL contribue au développement de ses membres en défendant les intérêts de la profession, en organisant l'échange des bonnes pratiques entre ses adhérents, en mettant à leur disposition un ensemble de services dédiés et en favorisant les synergies d'action entre eux.

L'AFDEL est membre de deux fédérations professionnelles, la FIEEC pour les synergies métier et la CINOV au titre de la convention collective CINOV-Syntec. Elle participe ainsi à la gestion de la convention collective CINOV-Syntec et de l'offre de formation de branche. Elle participe également aux travaux du Medef.

En région, l'AFDEL s'appuie sur le dynamisme des nombreux clusters avec lesquels elle a noué des partenariats dans l'intérêt de ses membres communs.

350 acteurs du logiciel, du Saas et de l'internet

4D
A2IA SA
ACTIVNETWORKS
AD SCIENCE
ADDENDA SOFTWARE
ADEQUASYS FRANCE
ADLER TECHNOLOGIES
ADWAYS
AGENCE FRANCAISE INFORMATIQUE
AGILIENCE
AKIO SOFTWARE
AKUITEO
ALCUIN
ALPHA CENTAURI
ALPHA SYSTEM
ALTAVEN
ALTISYS
AMADEUS FRANCE SA
AMALTO TECHNOLOGIES
AMETHYSTE
ANAKEEN
ANAPLAN FRANCE SAS
ANTELINK
ANTENIA
APLON FRANCE
APPLIDGET
APPS PANEL
ARCAD SOFTWARE - QUADRA SA
ARCADE
ARKOON NETWORK SECURITY
ARPEGE
ARTWAY MANAGEMENT
ASP FRANCE
AS-TECH SOLUTIONS
ASTON ITRADE FINANCE
ATRIL/POWERLING
AURA EQUIPEMENTS
AVANTEAM
AVENCIS
AXALOT
AZENDOO
BACKELITE
BEE WARE
BERGER LEVRAULT
BIBOARD
BIG5MEDIA
BILOG
BIX SOFTWARE
BLUEPIM
BONITASOFT
CABINET LEFEBVRE DISTRIBUTION
CASHSOLVE
CASSIOPAE
CD-ADAPCO
CEGEDIM ACTIV
CEGID
CENTURION TECHNOLOGIES
CERTICORPS
CGSI
CLARITEAM
CLEVER TECHNOLOGIES
CLIK'N DO ID CONTACT
CLIRIS
COCPIT
CO-DECISION TECHNOLOGY
CODINGAME
COHERIS
COMPARIO
CONCERTEO
COSYTEC
COZY CLOUD
CREATIVE IT
CROSSING-TECH
CYBERTRONIQUE
CYNAPSYS TECHNOLOGIE
DAESIGN
DASSAULT SYSTEMES
DATA
DATA CONCEPT
DATAKIT
DDS LOGISTICS
DENSITY
DENY ALL
DIALONICS
DIMELO
DISTRITEN SARL
EASIWARE
EASY VISTA
E-ATTESTATIONS.COM
ECO-LOGICIELS
EDICIA
EGYLIS
EL2I INFORMATIQUE
ELAB SAS
ELCIMAÏ FINANCIAL SOFTWARE
ELIADIS
EMAILSTRATEGIE
ENERGIENCY
EPTICA
ESI GROUP
EUCLEAD
EURECIA
EURODECISION
EVEA CONSEIL
EXTENSO PARTNER
FINANCE ACTIVE
FITNET APPLICATION
FLEXERA SOFTWARE LIMITED
FLEX-SERVICES
FLUOREM
FLUXOD
FOLLOW THE SUN
GB AND SMITH
GBM SYSTEMS
GENESE INFORMATIQUE
GLOBALLIANCE
GOLAEM
GOOGLE FRANCE
HBS RESEARCH
HEDERA TECHNOLOGY
HOLY-DIS
HORIZONTAL SOFTWARE
IBIZA SOFTWARE SAS
IDM WEB
IKO SYSTEM
IMMO-ONE
INCENTEEV
INNOVIT
INTEMPORA
INTERSEC
INTERSYSTEMS FRANCE
INTRASEC
INVOKE
IN-WEBO TECHNOLOGIES
IPLUS CONCEPT
IP-MEDIA
IRIUM SOFTWARE GROUP
IS2T
ISAGRI
ISATECH
ISEEDS SOFTWARE
ISOTOOLS
ISSENDIS
ITESOFT
ITFORCE
ITN
ITRUST
ITTIAM SYSTEMS EUROPE
IVALUA
IXIN
JALIOS
JAXIO
JLB INFORMATIQUE
JVS - MAIRISTEM SAS
KAYENTIS
KIMOCE
KITRY
KLEVERWARE
KOSMOS
KRONO-SAFE
LA NETSCOUADE
LASCOM
LE MEDIA
LEGAL SUITE
LEVEL5
LIGNE BLEUE CYBER
LMBA
LOCALEO SAS
LOGICIEL SERVICE ENTREPRISE
LPDR INGENIERIE
LSI-SUD
LUCCA
MATRIX
MEGA INTERNATIONAL
METNEXT
MICROLOGICIEL
MICROSOFT FRANCE
MIXVIBES
MOBYDOC
MOMINDUM
MOVIE SOLUTIONS
MP CONCEPT
MPHASIS WYDE
NAVIDIS
NEED SOLUTIONS
NEEVA
NELL'ARMONIA
NEOCASE SOFTWARE
NEOFI SOLUTIONS
NEOLANE
NEOTIC
NEOTYS
NETIKA SOLUTIONS
IMMOBILIERES
NEWRON SYSTEM
NLIIVE
NOVAXEL
OBEO
OCI URBANISME
ONE2TEAM
ONESCIENCE
OODRIVE
OPENDATASOFT
OPTIS
OR SYSTEM
ORDIMEGA - NOTA-PME
ORFEO
ORONE FRANCE
OXYAD SOFTWARE
PENBASE
PLANISWARE
PMSIPILOT
POM MONITORING
PRAXEDO
PREDICSIS
PRINCEPS
PROTYS
PUBLISOFT
QOSGUARD
QUALIAC
QUOTIUM TECHNOLOGIES
RESTLET
REWARD PROCESS
RIFT TECHNOLOGIES
ROOTSYSTEM
RUN MY PROCESS
SAASVALUE
SAGE
SALESFORCE.COM
SALVIA DEVELOPPEMENT
SAP FRANCE
SATELIX
SATELLIZ
SCAN & TARGET
SEAL - EVENT CATALYST
SEED4SOFT
SENSIO
SERENEO
SERENSIA
SERIOUS FACTORY
SERVICEPILOT TECHNOLOGIES
SERVICES MANAGEMENT SYSTEMS
SHAREWIZME
SHORTWAYS SAS
SI WEB
SICEM
SIDETRADE
SILKAN SA
SIMPLICITE SOFTWARE
SINEQUA
SIVEO
SLG SA
SMARTCO
SMARTESTING
SMARTFOCUS
SMARTPANDA NETWORK
SNEG
SOFT FLUENT
SOFTSECUR-IT
SOFTWARE CONTINTUITY
SONARSOURCE
SOYATEC
SPARKOM
SPOTTER
SQUID SOLUTIONS
STG INTERACTIVE
STRATOCORE
STREAMWIDE
SYDEV
SYNERTRADE
SYSGROVE
SYSTMG
SYSTRAN
TACTINEO
TALEND
TALENTSOFT
TALIANCE
TEEMEO
TELAMON
TELELOGOS
TELEMETRIS
THE GREAT FACTORY
THEGREENBOW
TOLEDE
TOPSYS
TORRENVAL VENTURES
TOUSCOPROD
TRACE ONE
TRAINING ORCHESTRA
TRF RETAIL
TRF RETAIL (SC. METHODE)
TRIBOFILM INDUSTRIES SAS
TRIIPTIC SAS
TRUST2CLOUD
UB PARTNER SAS
UBIKOD
UCATCHIT
USERCUBE
VAL SOLUTIONS SAS
VERTEEGO
VERTICAL M2M
VIAVOO
VISATIV
VOCAZA
W4 GLOBAL
WEBALLWIN
WEBCASTORY
WEBISTEM
WEEO GROUP
WIBU-SYSTEMS SARL
WINSOFT INTERNATIONAL
WOMUP SAS
WOOXO
XAGA NETWORK
XCOMPONENT
YOSATIS
YSEOP

Le document de positionnement de l'AFDEL sur le développement de la filière industrielle de cyber-sécurité en France est le produit des travaux de sa Commission « Cyber-sécurité ».

Direction : **Thierry Rouquet**, entrepreneur dans les technologies de cyber-sécurité, ancien Président d'Arkoon Network Security

Coordination : **Emmanuel Lempert**, AFDEL

Contributeurs : **Jacques Sebag**, CEO de Deny All,
Jérôme Chappe, Directeur Général de TheGreenBow,
Olivier Arous, Marketing & Business Development Director chez Bee Ware

Design et communication : **Fabrice Larrue** et **Justine Reverdiau**

Association Française des Editeurs de Logiciels et Solutions Internet
11-17 rue de l'Amiral Hamelin, 75016 Paris

Téléphone : 01 49 53 05 89
Email : info@afdel.fr
www.afdel.fr