Petit-déjeuner au restaurant du sénat

LE COMITÉ STRATÉGIQUE DE FILIÈRE (CSF) POUR LES INDUSTRIES DE SÉCURITÉ

Intervenant : Monsieur Marc Darmon
Directeur général adjoint de Thales

le 13 février 2019

L'industrie de sécurité est une filière d'excellence, parmi lesquels grands industriels français, leaders mondiaux, start up, beaucoup d'ETI, PME et laboratoires s'appuient, d'où son élévation au titre de « filière stratégique ».
La croissance du marché vient de celle des menaces et de la nécessité de faire face au terrorisme et aux cyber attaques. C'est une industrie qui repose sur un marché qui n'est pas mûr : les industriels fournisseurs se répartissent en 2000 entreprises, et des clients souvent perdus quand il s'agit de savoir comment se protéger. Beaucoup d'enjeux sont présents à la structuration de la filière et à son renforcement.
Elle comprend 25 milliards de chiffre d'affaire en 3 tiers :

- 1/3 = domaine de la cybersécurité qui va croissant, protection contre le cyber pollution, cyber espionnage et cyber sabotage.
- 1/3 = d'autres solutions numériques : vidéos de protection intelligente, gestion d'accès, identité numérique etc..
- 1/3 = solutions physiques : protection des personnes, bâtiments.

La haute technologie va croissante et son poids est conséquent : elle est désormais omniprésente. Pourtant beaucoup d'investissements et particulièrement régaliens, vont principalement sur les sujets physiques.

Avec plus de 50% à l'exportation c'est une des filières les plus performantes à cet endroit, mais c'est aussi inquiétant : les investissements nationaux sont beaucoup plus faibles qu'à l'exportation. Dans le domaine de la défense, quand il s'agit de convaincre un client étranger des performances des systèmes français, on les amène en France. Dans le domaine de la sécurité les grands industriels français, amènent les clients potentiels là où il y a les belles références, à l'étranger. L'équilibre entre personnels et technologie n'est pas le même en France. La filière englobe donc la cyber sécurité avec une continuité entre les domaines de la cybersécurité, l'identité numérique, le reste des technologies numériques et la sécurité (contrôle d'accès et vidéo-protection) et les services de sécurité physique. Du fait de cette continuité, une seule filière, contrairement aux autres plans précédents, comme le plan Montebourg, où il y en avait plusieurs.

Bilan du COFIS : créé fin 2013 avec un paradigme particulier : il regroupe Etat, utilisateurs et industries. Seulement 5% du chiffre d'affaire des industriels est fait par les administrations. Le vrai besoin de sécurité se trouve auprès des entreprises, des grands opérateurs et des PME, qui eux aussi ont besoin de se sécuriser physiquement et de protéger leur cyber espace. Il est donc nécessaire de dialoguer avec l'Etat acteur mais aussi avec les utilisateurs qui expriment leurs besoins. C'était un pilier important du COFIS et c'est une des choses qui a le moins bien marché. En revanche, le travail fait avec les industriels autour des technologies de ruptures et leur impact sur les nouvelles offres a bien marché. Le COFIS est arrivé à un niveau de frustration des industriels très élevé : les projets initiés et discutés ont accouché d'une souris. Le programme démonstrateur paraissait fédérateur pour montrer aux administrations et industriels ce qui était possible, mais a été extrêmement sous financé, avec une partie remboursable insupportable pour les PME, et il n'y a eu aucune cohérence entre ces quelques démonstrateurs et la vraie politique d'achat de l'administration. Par exemple il y a eu deux démonstrateurs autour des communications sécurisées et spécifiques basées sur des technologies modernes : en France, la Gendarmerie a le système RUBIS, la police le système ACROPOL, basés sur des technologies anciennes. Les nouvelles technologies 4G permettent de faire beaucoup plus. Du fait d'un désaccord entre Thalès et Airbus, deux démonstrateurs ont été créés, avec chacun un écosystème de PME, et auraient dû être la base des futurs investissements :

- L'un montrant comment, en partant d'un réseau existant, on peut le faire évoluer sur la 4G et obtenir des services complémentaires.

- Le second : comment, en partant de zéro construire un réseau High Tech mais répondant aux vrais besoins spécifiques des policiers : appel de groupe, sécurité, vidéo protégée etc.

Mais le programme de rénovation au niveau national au ministère de l'intérieur est découpé en 7-8 lots : aucune des 20 entreprises présentes dans les démonstrateurs n'a été choisie. C'est incohérent avec le travail effectué en amont et démontre une dichotomie systémique qui se retrouve dans tout le travaille du COFIS depuis sa création : la politique publique n'est pas cohérente avec les ambitions.

Les comités stratégiques de filière ne comprennent pas le domaine de la sécurité quand ils apparaissent initialement en 2017. Le principe est très concret et pragmatique : sur chaque filière on signe un contrat de filière, ce qui signifie que cette dernière est organisée autour de quelques projets et sur chaque projet un contrat de filière est signé entre les ministères correspondants et l'industrie, dont le rôle de chacun est défini. Les industries s'engagent par exemple à l'embauche, construction d'usines, non-délocalisation, et les ministères s'engagent aussi par exemple à être un client exemplaire, à avoir des actions règlementaires, fiscales, flechage de budget de R&D. C'est comme ça que fonctionnent les filières, avec ce schéma de contrat de filière très motivant.
En novembre 2018, deux nouvelles filières sont lancées en plus des 15 déjà existantes :

- 1 autour des infrastructures numériques et du soutien de déploiement de la 5G
- 1 autre autour de l'industrie de la sécurité et de la cyber sécurité

Parmi les 15 premières 5 ou 6 n'ont pas encore signé de contrat de filière. Leur ambition est claire et les moyens sont définis de manière précise.
Nous proposons une concentration sur 5 projets visibles, facilement descriptibles et dans lesquels on puisse faire se regrouper tous les industriels, est mise en place. Ils ne recouvrent pas toutes les industries mais sont relativement couvrants et clairs :

1) souveraineté numérique : être capable d'offrir aux administrations et aux grandes entreprises des solutions de Cloud nationales qui protègent autant qu'elles peuvent du Cloud Act. En France, nous avons des offres de cloud public, privé ou hybride extrêmement performants qui peuvent servir de socle à une solution nationale permettant de stocker des données dans un Cloud français (OVH, Dassault, Thales, Atos, Orange...).

2) sécurité des territoires : ainsi que celle des grandes infrastructures et des villes : système autour de la sécurité des vidéos surveillance. C'est un domaine réglementé, avec beaucoup d'énergies en France en termes de solutions qui nécessite une convergence des opérateurs qui mettent en place, mais aussi une convergence des acteurs qui agissent derrière le système. De plus, ce n'est pas parce que les technologies sont là que les considérations éthiques sont remises en question.

3) sécurité des JO 2024 et des grands événements : ce sont des événements sans précédent en termes de sécurité et de nombres de personnes, de sites, de visiteurs. Ils entrainent un enchevêtrement de responsabilités entre collectivités locales, comités d'organisation, polices nationale et municipale et avec des risques de tous types. Le système industriel français comprend un grand nombre de capacités et de références (Atos, Thales...)

4) identité numérique : nous avons des leaders mondiaux, IDEMIA, Gemalto, ArianeGroup, et pourtant la France est probablement le pays d'Europe le plus en retard sur ce sujet. Pour renforcer les industriels tout en améliorant la situation française, il faut un projet clair dans lequel les industriels s'engagent à beaucoup de choses.

5) cyber sécurité : ensemble de projets dont ressources humaines, sensibilisation aux besoins de se protéger, à des règles d'hygiène...

Les chefs de projets de chacun de ces 5 projets ont été nommés (tous des industriels) dans le but de fédérer l'industrie. Le CSF est donc plus concret que le COFIS.
Il s'agit de faire croître la population d'ingénieurs, le chiffre d'affaire de la filière dans un rapport deux. Le comité réunit une douzaine de personnes, 6-7 industriels couvrant l'industrie, un représentant des utilisateurs (président du CDSE) et des représentants de l'Etat (Bercy, intérieur, SGDSN) puis des représentants et partenaires sociaux.

Réponses aux questions :

1) La plupart des grands groupes sont européens et coopèrent beaucoup au sein de l'Europe qui est forcément parti prenante de ça. Il y a des projets de financement de la part de l'UE autour des sujets de sécurité, le problème de cet axe financement R&D de l'Europe c'est qu'il est très lourd et pénalisant, et qu'il y a peu d'efficacité avec les règles de coopération à plusieurs industriels et pays. En termes d'exigence de cyber sécurité, toutes les administrations et nations ne se valent pas : très élevé en France et la coopération

européenne doit éviter une nivèlement par le bas. Donc ça freine toute coopération sérieuse pour l'instant.

2) Quelques coopérations avec le ministère des Armées sont présentes dans les travaux du COFIS autour de l'analyse des technologies critiques. C'est un travail initié avec le process du ministère des armées mais il n'est pas représenté dans le CSF en tant que tel.

3) Dans les 5 projets identifiés, il n'y a que de projet pouvant fédérer et créer un partenariat Etat-industrie clair, donc le sujet de la thématique des radiocommunications sécurisées n'est pas conservé.

4) L'ingénierie française est qualifiée, tirée par l'High Tech : vidéo protection, villes intelligentes etc. La France a toujours été forte en sciences dures, ce qui provient de deux choses : la qualité de l'enseignement supérieure et le crédit impôt recherche. Ce qui fait qu'on a parmi les meilleurs ingénieurs au monde et la capacité de maintenir les meilleures qualités d'ingénierie en France sans délocalisation.

Globalement, ce n'est sûrement pas à cause des syndicats qu'il y a du retard en terme d'équipement technologique, mais à cause de l'ensemble des clients, industriels, des réseaux de transport, de télécoms etc. C'est dû à un échec de mode de sensibilisation: la sécurité est souvent vue comme une contrainte.

5) La sécurité des infrastructures va être traitée dans le volet de sécurité des territoires et va l'équilibrer entre le côté numérique et le côté physique.

6) Aucune grande entreprise ne bascule intégralement sur le Cloud. Elles utilisent plusieurs solutions de Cloud : probablement des offres publiques américaines, mais pas uniquement : les Clouds privés nationaux et souverains existent aussi. On ne saura pas créer un Cloud unique capable de concurrencer Amazon. Mais on peut s'appuyer sur certains qui existent en ajoutant des solutions complémentaires supérieures déjà existantes.

7) Les règles éthiques des pays dans lesquels on vend sont respectées. Le CSF ne peut pas espérer croître dans ce domaine sans une forte considération étique. L'intelligence artificielle va être intégrée dans la plupart des solutions. Il est indispensable qu'elle soit prédictible et répétable afin que la machine ne décide pas seule. Les solutions techniques doivent être suffisamment comprises et expliquée pour qu'on puisse les maitriser. Il s'agit d'adopter une étique de comportement mais aussi une éthique du produit.

8) Il ne faut pas rationaliser et supprimer le foisonnement de grands groupes, PME, ETI et Start up. Ce qu'offrent les entreprises est extrêmement varié et peu clair pour des clients qui ne savent pas ce qu'ils veulent, d'où une caractéristique de « marché pas mûr ». Il ne s'agit pas de structurer l'industries en coupes réglées.

9) Comment être meilleur en standardisation ? On peut demander un soutien sur une normalisation sur un point précis dans un contrat Etat-industrie. Mais le comité de filière n'est pas fait pour qu'on réfléchisse là à un sujet d'éthique : on se concentre sur le fait de travailler sur le sujet industriel.

HAUT COMITÉ POUR LA RÉSILIENCE NATIONALE
40 bis rue Fabert - 75007 Paris
Tel : +33 (0)1 49 52 94 28
Fax : +33 (0)1 47 20 75 27
www.hcfrn.org