Renseignement industriel : « La France a perdu la culture du combat »

- Intelligence économique -

Date de mise en ligne : jeudi 23 avril 2009

Spyworld Actu

Interview de Franck DeCloquement*, spécialiste de l'intelligence économique. Retrouvez les mêmes experts demain : ils se pencheront sur le facteur humain et donneront des conseils pratiques pour les PME-PMI.

La France est-elle une cancre de l'intelligence économique ?

F.D - Le terrain des affrontements plus classiques a laissé place à la guerre économique, mais une grande naïveté reste effectivement prégnante en France. On n'a pas beaucoup l'habitude de voir ces choses-là en face. On a perdu la culture du combat. Pourtant, il est souvent possible de décrypter l'actualité géostratégique. Cela pose parfois un problème éthique : beaucoup d'alliés politiques sont aussi nos adversaires sur le terrain économique. Le message de faible intensité envoyé par Vladimir Poutine sur le gaz peu apparaitre comme un exemple assez clair de ce point de vue.

Beaucoup d'entreprises ont affaire à ce contexte. Les très grosses entreprises mais aussi les PME-PMI (voir interview demain, NDLR).

Pêche-t-on par manque de débrouillardise ?

F.D - Nous sommes dans une société de haute information. Notre capacité à admettre ces affrontements sous-jacents dépend du système de valeurs en place. Au Japon, le MITI emploie des méthodes musclées pour permettre aux entreprises vernaculaires d'exporter. En Chine le principe de la copie ne pose pas les mêmes problèmes qu'en France, les normes culturelles ne sont pas identiques. Nous sommes plus tatillons.

D'autres pays ont complètement intégré dans leur arsenal ces méthodes d'actions qui passent sous les fourches caudines de la loi. Le facteur humain est plus difficile à cerner, à la différence des méthodes d'acquisitions par l'électronique : ces pays sont beaucoup plus offensifs dans leur approche globale. La France se contente bien souvent de se défendre. La réputation est aussi une arme : « Médisez, il en restera toujours quelque chose » disait Beaumarchais.

Les anglo-saxons de manière plus générale sont très forts en matière d'actions d'influence et l'assument beaucoup mieux. Cette philosophie en France n'a jamais eu bonne presse. Résultat : quand certaines méthodologies non conventionnelles d'action s'opèrent, peu arrivent à y lire les actions avisés de la concurrence en sous-main. C'est l'histoire de Gemplus, leader des cartes à puces rachetées par un fond d'investissement proche du Département de la Défense Américaine. L'Etat ne s'en est pas préoccupé à l'époque, faute d'une grille de lecture des événements adaptée. Cela restera pour beaucoup un cas d'école.

Les fonds étrangers sont-ils l'armée de l'ombre ?

F.D - Les fonds souverains sont en effet en première ligne : Gemplus attaquée par un actuariat proche des fonds américains le montre. A fortiori en période de crise, ces fonds profitent de la possibilité d'acquérir des entreprises à moindre coût, trop peu soutenues par les pôles de compétitivité, et démarchent des créateurs en mal de financements. De manière plus générale, les anglos-saxons sont dans une logique d'investissement sur le moyen et le long terme. La France s'enlise souvent dans une logique de court termisme.

On parle d'agents du renseignement récupérés au service du secteur économique ?

F.D - Sous l'ère Clinton, les Etats-Unis ont réorienté l'appareil de renseignement d'état en direction du champ économique. Les spécialistes du renseignement ont fait leur entrée dans les directoires des grandes entreprises stratégiques : aviation, automobile, énergie. La création de « l'Advocacy center » sorte de « war room » a permis très vite de mieux orienter les efforts de conquêtes de marchés au profit des entreprises nationales. C'était d'autant plus facile que la fin de la guerre froide avait laissé les effectifs des différentes agences du renseignement vacants. Il en fut de même en Russie ou de très nombreux spécialistes, du FSB notamment, sont ainsi passés des problématiques militaires aux problématiques plus économiques.

La communication d'influence s'impose aussi là où on ne l'attend pas. Avez-vous des exemples ?

F.D - Il s'agit d'une politique en "mille-feuille" : les liens entre Hollywood et le Pentagone sont connus par exemple. La CIA qui utilise l'actrice de la série culte "Alias" Jennifer Gardner pour promouvoir son image dans une campagne de recrutement, c'est de la politique d'influence intelligente. Les actions d'influences ne sont pas figées, ne viennent pas d'une source et peuvent prendre de multiples formes. On a bien souvent du mal à y voir une action globale. Pour tenter de les décrypter, on utilise en pratique des cartographies et des matrices d'acteurs (sociétales, économiques, médiatiques), puis on les superpose. Ces 3 niveaux de lecture cumulés permettent de mieux lire la logique des événements. Des convergences apparaissent bien souvent, permettant de mettre en lumière des alliés et des contradicteurs afin de déterminer les intentions sous-jacentes.

L'ouvrage de Jacques Myard paru en 2006, La France dans la guerre de l'information, liste toutes les forces en présence et qui peuvent contrer nos intérêts économiques. Beaucoup restent dans l'angélisme quand il est question d'aborder ces sujets. On relie rarement l'échiquier politique, économique, sociétal pour se donner les moyens de lire ce qui se passe. Ce n'est pas toujours évident. L'USAID par exemple, est une organisation très proche du Département de défense américain qui constitue à ce titre un moyen d'influence « soft ». Mais nous sommes encore très frileux et craignons de nous engager sur ce terrain susceptible de blesser nos alliés, qui ne manquent pas de nous tacler dès que leurs intérêts sont en jeu.

La Chine, championne du cyber-espionnage

Des cybercriminels ont eu accès aux documents du projet de l'avion de chasse F-35, le programme d'armement le plus coûteux du Pentagone, a affirmé mardi 21 avril le Wall Street Journal, qui pointe du doigt la Chine. Le 8 avril déjà, le « Wall Street Journal » révélait que des cyber-espions ont pénétré à plusieurs reprises le réseau électrique américain, selon un rapport et des sources au département de la Sécurité intérieure. Qu'ont donc fait les hackers ? « Ils ont laissé derrière eux des programmes qui pourraient être utilisés pour perturber le système et ses contrôles. Ils viennent de Chine, de Russie et d'autres pays. Ils n'ont pas causé de dommages mais pourraient essayer d'agir lors d'une crise ou d'une guerre », écrit le journal. Du côté des ambassades chinoise et russe, on dément véhément qu'il s'agisse de cyber terrorisme d'Etat La main des Etats. Roger Faligot, spécialiste du renseignement et des services secrets chinois, est plus circonspect. Auteur du livre "Les services secrets chinois de Mao aux JO" (éditions du Nouveau Monde) paru en février, il voit "mal des hackers chinois agir à l'insu des autorités". Un rapport de chercheurs canadiens récent a quant à lui révélé une cyber-attaque massive, trouvant son origine en Chine : 1.295 ordinateurs auraient ainsi été infiltrés dont quinze cibles françaises, des "administrations sensibles", dans 103 pays depuis deux ans. Ce rapport met notamment en exergue le rôle du 3e département de l'Armée populaire de libération (APL), qui, selon M. Faligot, compte des "dizaines de milliers d'ingénieurs et de techniciens chargés de la guerre dans le cyber-espace". M. Faligot relève que le rapport canadien situe "une grande partie du dispositif" de cette vague d'attaques informatiques dans l'île méridionale chinoise de Haïnan, une zone dans laquelle un navire espion américain a été récemment harcelé par la marine chinoise.

**Franck DeCloquement et Emmanuel Lehmann ont co-écrit un ouvrage à paraitre en septembre aux éditions Chiron : "Petit traité d'attaques subversives contre les entreprises".*

Post-scriptum :

http://www.usinenouvelle.com/articl...