Vincibilis

28 novembre 2011

QUI SONT LES ESPIONS INDUSTRIELS ?

- CONNAITRE SON ENNEMI -

Par Alexandre LIENARD

« Connais ton ennemi comme tu te connais toi-même !»

(Maître Sun Tzu, l'Art de la Guerre).

L'espionnage économico-industriel est une réalité

Lorsque nous animons des séminaires consacrés à l'espionnage industriel ou lorsque nous rencontrons des chefs d'entreprises, nous sommes toujours très étonnés de constater à quel point les premières minutes de discussion sont difficiles lorsque l'on aborde notre métier : la lutte contre l'espionnage économico-industriel.

Il est vrai que bon nombre de personnes, même les plus imaginatives sont septiques quand il s'agit de déterminer si l'espionnage économique est un mythe ou une réalité. Les « *non believers* » de la chose argumentent généralement leurs propos en criant haut et fort que seules les grandes entreprises sont victimes de faits d'espionnage industriel ; en bref, le haut de panier ! Seulement il y a plusieurs mais.

Tout d'abord définissons ce qu'est l'espionnage industriel. L'espionnage se définit comme étant la captation d'informations à l'insu de la personne (morale ou physique) ciblée. En y ajoutant le mot économique, l'on peut dire que l'espionnage économique est la captation d'informations plutôt sensibles à l'insu d'une personne (morale ou physique) dans un contexte économique ou industriel. L'espionnage en général se fait via plusieurs méthodes : l'effraction, le vol, la manipulation de personnes et la surveillance discrète, voire furtive, de personnes et de biens.

En y regardant de plus près et en évitant la pensée unique qui consiste à croire que les faits d'espionnage relèvent d'opérations à la James Bond, l'on constate que toute une série de faits qui pourraient se retrouver dans des faits divers ou devant n'importe quel cour de justice civile, constituent aussi des faits d'espionnage économique. C'est vrai pour l'employé indélicat qui part à la concurrence avec des secrets commerciaux ou industriels, cela est vrai aussi pour un commercial qui sauvegarde la base de données clients au cas où il serait licencié et bien entendu pour les partenaires qui ne respectent pas le cas de contrats de collaboration en éventant certaines données sur le marché. Il ne faut donc pas uniquement avoir été suivi, espionné par un détective, filoché par un concurrent ou manipulé avec de la fausse information ou encore écouté téléphoniquement pour être victime d'actes d'espionnage économique.

Quant au fait que seuls quelques grands groupes sont ciblés ou victimes, il y a matière à mettre quelques bémols. Tout d'abord, et de source policière, bon nombre de victimes ne déposent pas plainte : probablement la crainte d'avoir leur image de marque, leur notoriété mises à mal. Ensuite, peu d'entreprises ont les moyens de détecter les faits d'espionnage commis que ce soit en interne ou depuis l'extérieur, que ce soit par le biais de vol informatique ou pire par le biais de recrutement de sources

humaines internes. Bref, à détection impossible, dépôt de plainte impossible aussi. Enfin, ne pas compter avec les PME pour tout ce qui touche de près ou de loin à l'espionnage économique c'est oublier que les PME sont régulièrement les sous-traitants de grands groupes et ce, pour tous les métiers : comptabilité, mis à disposition de ressources informatiques, usinage, travaux divers, transformation de matières premières… Et celui qui est le maillon le plus faible dans la chaîne de la sécurité est toujours visé en premier lieu de part sa nature vulnérable.

L'espionnage industriel est bien une réalité. Tout le monde est concerné : du citoyen à au cadre, en passant par l'employé ou le fonctionnaire ! Car oui, le service public est aussi un maillon faible dans la chaîne de la sécurité. Vous me direz « Quoi ? Une administration espionnée dans un contexte économique ? Est-il devenu fou ? N'est-ce pas le pré carré de l'Etat et de ses services d'espionnage ? » Et moi de vous répondre que non, je ne suis pas fou et qu'il existe des cas d'espionnage économique pour lesquels des administrations spécialisées dans le support à l'exportation se sont vues pillées, informatiquement parlant, des données et des secrets de fabrication de leurs administrés. Certains fonctionnaires dans les finances publiques se font aussi « tamponner » afin d'obtenir du renseignement fiscal ; renseignement exploitable et crucial lors d'approche concurrentielle offensive. Qui ne rêve pas d'obtenir la liste clients de ses concurrents ? Ces listes sont souvent disponibles notamment sous forme de listing TVA.

Les origines de l'espionnage industriel

Loin de moi l'idée de débattre sur le premier fait d'espionnage économique connu. J'imagine que les premiers commerçants devaient déjà être tentés de subtiliser l'information à leurs si dérangeants concurrents. J'imagine aussi que la guerre a toujours été un prétexte à la conquête économique, depuis la nuit des temps l'homme espionne. Ce point n'évoque donc pas le côté originel au premier sens du terme mais bien ce qui pousse les uns et les autres à s'espionner dans la conquête des marchés, aussi petits ou grands fussent-ils.

A mon sens, il y a trois grandes raisons qui déclenchent un processus d'espionnage économique. Bien entendu l'envie de savoir et de connaître les forces et les faiblesses de l'autre sont légitimes et je dirais même normal. Mais fondamentalement, réalisés par des services d'états pour par le secteur privé, les faits d'espionnage sont mus par la volonté de conserver un avantage stratégique ou la volonté d'en acquérir un nouveau – sans trop se fatiguer, sans trop investir. C'est réellement cela qui motive l'entrepreneur, le cadre ou l'homme d'affaires à passer à l'acte ou à demander l'aide

de spécialistes pour capter de l'information sensible. Le dernier déclencheur, et non des moindres, c'est la volonté de nuire voire de détruire.

Un cas marquant m'a ainsi été un jour rapporté. Un chef d'entreprise dans le secteur de l'agro-alimentaire avait été la victime d'un fait de piratage informatique qui avait débouché sur le vol d'informations sensibles et stratégiques. Conformément à notre définition ci-haut, cet acte est bien considéré comme de l'espionnage industriel. Toutes les données de productions, les « secrets maison », la stratégie commerciale et le respect des quotas « bio » avaient ainsi été dérobés par un employé malveillant. Ce dernier, activiste « vert » avéré et patenté, avait eu la « bonne » idée de modifier certains fichiers concernant les quotas « bio » pour en avertir l'agence de surveillance alimentaire et ainsi déclencher une inspection qui m'a été commentée comme musclée, presque anti-démocratique. Je vous passe les détails sordides mais aujourd'hui la société est fermée : après la cessation de paiement qu'a entraînée la perte de notoriété et la non possibilité de livrer les fournisseurs sans l'avis favorable de l'agence alimentaire. Le bilan de l'histoire est lourd car ce sont des dizaines d'hectares qui ont dû être revendus, une dizaine d'emplois perdus et un chef d'entreprise qui sanglote presque encore aujourd'hui quand il évoque sa terrible mésaventure d'espionnage dont il a été victime. L'activiste est, quant à lui, employé dans une ONG traitant d'écologie. Le crime paie finalement.

Chute du mur de Berlin et ère de l'information

Voilà certainement les deux facteurs qui ont fait exploser l'habitude de certains à faire appel à de l'espionnage industriel. S'il est vrai que la course à l'armement a favorisé la lutte entre l'Est et l'Ouest pour la suprématie de l'Espace, la stratégie de conquête et d'occupation du terrain était avant tout économique. Nos joyeux espions n'ont pas eu le choix lors de la chute du mur de Berlin. Il leur a fallu se reconvertir vers d'autres métiers.

Aujourd'hui la plupart du budget alloué aux services de renseignement occidentaux sert à lutter contre le terrorisme. La protection du patrimoine économique est devenu le parent pauvre de la grande famille du renseignement. Mais cela est uniquement vrai en Occident. La Chine, par exemple, alloue en fait peu de budget à la lutte contre le terrorisme. Le renseignement militaire est utilisé pour assurer la souveraineté de l'Etat. Les services de sécurité eux luttent pour la sécurité intérieure politiquement et idéologiquement. Mais, la Chine a une toute autre facette et sa compréhension des frontières ne se limite pas aux frontières physiques mais bien aussi aux frontières économiques virtuelles et mouvantes. Ainsi les services de renseignement extérieurs

mènent des opérations d'espionnage économique et les services de sécurité intérieurs surveillent et espionnent les étrangers venus faire des affaires chez eux. On ne compte plus les histoires racontées par des commerciaux internationaux ou cadres du grand export qui disent avoir été victime de faits troublants lors de leur arrivée à l'aéroport de Pékin : ordinateur confisqué durant quelques dizaines de minutes, téléphone portable pris puis rendu avec une mémoire vidée… et je ne parle pas de ceux qui ont eu le sentiment d'avoir été suivi, écouté au téléphone à l'hôtel ou encore celui qui s'est couché la nuit dans sa suite avec l'étrange impression que la chambre avait été visitée pendant que par magie une beauté chinoise lui avait renversé un verre de champagne alors qu'il payait l'addition au bar du *business lounge* et l'avait retardé d'une bonne heure. Rentré seul dans sa chambre d'hôtel après s'être fait télescopé amoureusement de la sorte, étrange. Oui, la Chine investit dans le renseignement économique et capitalise sur son besoin non encore avéré de lutte contre le terrorisme. Et pendant cela à Paris, Londres ou Bruxelles le budget part en écoutes téléphoniques et en traducteurs farsi/anglais ou arabe/français, en sécurisation d'opérations dans des cités ou personne n'ose plus mettre un pied. Et lorsque l'on arrive à « loger » un groupe d'étudiant chinois occupés à voler des secrets industriels, l'on évoque encore le spectre de l'espionnage chinois sans jamais se dire que des occidentaux oeuvrent peut-être parfois sans le savoir pour des intérêts chinois. J'arrête là côté géopolitique car je n'en ai que de maigres, très maigres compétences. Cela étant posé, je reviendrai à la Chine plus tard dans le document.

Qui fait les opérations d'espionnage ?

Ce qui est certain c'est que l'espionnage économique s'est internationalisé avec la mondialisation des échanges. Tout le monde est exposé et tout le monde en fait. Intéressons-nous à ceux que l'on appelle dans le jargon les opérateurs. Les opérateurs sont les personnes qui vont au contact, celle qui vont chercher le renseignement là où il se trouve. Et je dis bien *renseignement* au singulier. Dans la communauté de l'espionnage trois canaux principaux sont utilisés pour collecter du renseignement :

- le canal humain (HUMINT),
- le canal « sources ouvertes » (OSINT),
- le canal « électronique » (SIGNINT).

Nous pouvons donc déjà découper les opérateurs en trois catégories principales. Généralement les opérateurs faisant de l'humain ne font que cela, les spécialistes des sources ouvertes et publiques travaillent comme documentalistes et mieux ne vaut pas

laisser les opérateurs techniques faire de l'humain tellement leur quotient social est proche de zéro.

Dans le monde de l'espionnage industriel, la découpe est la même et j'illustre ces catégories en fonction de trois grandes familles :

- les opérateurs « HUMINT » : ils volent les informations physiquement ou les font voler en recrutant dans le monde de la criminalité, ils manipulent des personnes détenant des secrets industriels, ils recrutent des sources dans les entreprises et organisations qui les intéressent directement et indirectement ; ils se basent souvent sur le travail des opérateurs OSINT et recrutent parfois les « techniciens » ;
- les opérateurs « OSINT » : ils interrogent les bases de données, les sources publiques, réalisent des cartographies, analysent les faits intéressants et montent les scénarii et les légendes[1] ;
- enfin la grande famille des techniciens qui regroupe les pirates informatiques, les spécialistes de l'écoute téléphonique, les poseurs de micro, les as du labo, les fous de l'électronique.

Il existe bien sûr plusieurs types de commanditaires. Les institutions, les entreprises et même certains hommes politiques intéressés d'aider leurs amis font souvent appel à ces hommes de l'ombre.

Quatre grandes catégories de « fournisseurs » de service d'espionnage industriel existent :

- les services d'Etat : services secrets, services de renseignement, services de police et bureaux militaires etc.,
- les cabinets d'intelligence économique : courtiers en informations, gestionnaires de risques, officines, entreprise de due diligence etc.,
- les espions indépendants : retraités de services spéciaux ou de services de police, aventuriers, activistes en tout genre etc.,
- les espions qui le sont « sans le savoir » : employés indélicats, personnes malveillantes, personnes manipulées etc

Selon le FBI, plus de 100 pays attaquent et espionnent régulièrement les entreprises américaines. Les services d'Etat sont très actifs dans le cadre de l'espionnage industriel. Bien sûr je parle avant tout de services offensifs. Les services de contre-

[1] Une légende se compose des éléments d'identité que l'on donne à un espion. Il s'agit d'une "histoire", d'un "passé" prévu pour la mission de renseignement.

espionnage sont souvent de la partie aussi mais leur approche est plus défensive. Certains pays comme les Etats-Unis, la Chine, la Russie ou même la France, mandatés par le pouvoir politique ou par le gouvernement pour assister une entrepris nationale stratégique, fournissent des services d'espionnage économique dans la sacro-sainte lutte pour la suprématie économique. Les cibles sont généralement de grandes entreprises, des entreprises à haut potentiel technologique ou encore certaines organisations non gouvernementales comme Greenpeace qui perturbent parfois les activités de mastodontes du secteur de l'énergie.

Depuis le milieu des années 90, une nouvelle « race » d'espions a fait surface sur le marché. Les cabinets d'intelligence économique qui communiquent généralement sur l'axe « gestion des risques » - « sécurité économique », offrent généralement et sous le manteau des services offensifs de recherche et de captation d'informations. Si les cabinets anglo-saxons qui détiennent une grande partie du marché mondial sont très présents sur le marché de l'espionnage industriel, il faut aussi compter avec les nouveaux arrivants comme certains cabinets français, suisses ou encore allemands.

Les espions indépendants, sorte de mercenaires de l'information, n'ont par essence que peu de contacts directs avec les commanditaires. On imagine mal qu'ils puissent communiquer par le biais d'un site Internet en mettant en avant leurs particulières compétences : « Bienvenue sur le site Internet de Mr X, expert en vol d'informations, en manipulation et en extorsion ! » Non, cela ne se passe pas comme cela. Certains d'entre eux bénéficient d'un bon réseau de relations souvent issu de leur carrière passée ; ceux-là travaillent en direct pour quelques grandes entreprises ou « groupes d'intérêt ». Mais la plupart d'entre eux travaillent en sous-traitance pour les cabinets d'intelligence économique ou même parfois pour certains services officiels.

Les espions que je qualifie de « sans le savoir » ne savent pas toujours qu'ils sont « espions » et n'ont souvent pas de « savoir » particulier en la matière. C'est probablement la catégorie qui est la plus représentée sur le marché de l'espionnage économique. Souvent présents en interne dans les entreprises ciblées leurs actions sont motivées par l'envie de nuire, l'envie de se venger ou simplement le besoin de lucre. Ils sont susceptibles de fournir du renseignement à la concurrence dans une démarche proactive. Ils volent l'information et tentent de la vendre au plus offrant, au plus « compréhensif ».

Les services officiels, tout comme les cabinets d'intelligence économique, n'aiment pas apparaître dans les opérations d'espionnage industriel ; c'est pourquoi, au final, ce

sont souvent les petits opérateurs qui réalisent les missions. Cela pose bien entendu des lourds problèmes de fiabilité.

Le métier de l'espionnage économique c'est avant tout savoir recruter me disait un jour un ancien fonctionnaire du contre espionnage. Cela est vrai pour les trois premières catégories de « fournisseurs ». De là provient toute la difficulté de tracer un fait d'espionnage. Si l'on prend l'exemple de l'affaire RENAULT qui a fait grand bruit en France en 2011 (et qui continue d'ailleurs d'exciter les journalistes et experts du secteur), on peut constater la cascade d'opérateurs, de contacts et de fournisseurs qui ont été mis en action pour monter la manipulation. Tout le monde semble avoir joué sur le terrain ou plutôt devrais-je dire que les services de renseignement (en démarche défensive pour la D.C.R.I.[2]), une société de sécurité privée (GEOS), un opérateur « HUMINT » (le fameux salarié de GEOS qui aurait fait cavalier seul), des opérateurs « SIGNINT » (les pirates informatiques ayant soi-disant craqué les comptes en banque) et les sources internes (dont le « corbeau » et le directeur de la sécurité) ont été présents sur le champ de bataille !

Et tout ce beau monde agit souvent sous couverture. Ainsi quelques métiers sont idéals quand ils sont utilisés comme couverture :

- les journalistes,
- les spécialistes « communication »,
- les lobbyistes,
- les recruteurs et chasseurs de tête,
- …

Historiquement parlant les journalistes sont des sources voire des opérateurs de choix pour les services de renseignement. Utilisés dans la plupart des conflits durant la période dite de la Guerre Froide pour couvrir l'actualité, certains journalistes échangeaient l'information avec les services de renseignements. Depuis que la guerre économique fait rage, et surtout en période de crise, certains journalistes spécialisés travaillent en couverture pour les services de renseignement publics.

Ces mêmes journalistes sont maintenant régulièrement approchés par les cabinets d'intelligence économique. La capacité qu'a le journaliste de capter de l'information « off the record » est grande. Cette information est bien souvent cruciale dans le cadre d'une opération d'espionnage industriel car elle permet d'aller directement au cœur du problème, de connaître certaines faiblesses.

[2] Direction Centrale du Renseignement Intérieur. La D.C.R.I. a été créée en juillet 2008 et regroupe l'ancienne D.S.T. (Direction de la Surveillance du Territoire) et les anciens R.G. (Renseignements Généraux).

Bien loin de moi l'idée de mettre toute la population journalistique dans le même sac. Cela dit, puisque les journalistes connaissent depuis une dizaine d'années un effondrement de leur pouvoir d'achat (salaires), et une baisse des budgets alloués (paiement de sources, frais de voyages, notes de frais), certains sont tentés par l'argent facile que peuvent offrir les commanditaires de missions d'espionnage industriel.

Les entreprises de communication sont aussi de parfaites couvertures. Il existe, par exemple à Bruxelles, une entreprise de communication basée près de la Commission Européenne qui réalise *en façade* des sites Internet et des communiqués de presse. Cette entreprise a d'autres activités dont la surveillance de certains fonctionnaires ou élus européens et la collecte d'informations stratégiques. Cette entreprise a donc pignon-sur-rue et n'a jamais été inquiétée pour ses activités connexes illégales.

Les bureau de lobbyistes sont aussi souvent utilisés comme couverture car une société qui fait appel à un bureau vendant des services d'influence est bien obligée de se mettre à nu ne fût-ce que pour contextualiser sa demande. Certains lobbyistes jouent double jeu et commettent des actes qui pourraient être qualifiés d'espionnage industriel.

Mais que cherchent les espions ?

Il faut bien se rendre à l'évidence, l'information est devenue un facteur clef de succès dans les affaires. Celui qui maîtrise l'information contrôle une bonne partie du processus d'accès au marché ou d'encerclement de ce dernier. « *Information is power* » disent-les Américains.

Que ce soit dans le but de nuire ou de capturer de l'information, que ce soit via l'utilisation des moyens technologiques ou des moyens humains, le but est toujours d'obtenir une information importante, stratégique. Cela ne veut pas nécessairement dire que l'information a été identifiée comme sensible chez la cible ou même qu'elle le soit réellement. L'importance de l'information, son caractère stratégique et/ou sensible est défini généralement par le donneur d'ordre, la personne ou l'organisation qui commandite l'espionnage.

Les moyens les plus communément utilisés !

Il existe pléthore de techniques utilisées par les espions industriels, l'on peut à titre d'exemples énumérer les moyens suivants :

- Le piratage informatique
- L'intrusion physique
- La pose d'outils de surveillance
- Les interviews sous faux-pavillons
- Le recrutement offensif de personnes clefs
- La corruption
- Le recrutement de sources internes
- Le recrutement de sources externes
- Les visites d'entreprises
- …

Le piratage informatique tend à se généraliser dans les opérations d'espionnage industriel ; en effet commander un piratage informatique ne coûte pas trop cher, il laisse peu de traces lorsque les attaques sont bien faites, il n'y a pas de contacts directs et physiques avec la cible. Le piratage informatique ne demande donc pas de budgets trop conséquents et les risques de se faire prendre sont très faibles. Encore faut-il que l'information soit existante ou disponible. Le piratage est tout autant utilisé par le secteur privé que par le secteur public. En Belgique, la Sûreté de l'Etat peut légalement faire appel à des spécialistes pour « investiguer » numériquement parlant.

L'intrusion physique reste une technique « sûre » pour les espions industriels. Si elle expose le contrevenant à des risques physiques très clairs (être pris sur le fait, arrestation, flagrant délit, répression physique directe…), elle donne cependant des résultats probants car l'opérateur, s'il est doué en « ouverture fine », est quasiment assuré de trouver ce qu'il cherche. Et « *last but not least* », l'opérateur peut maquiller son méfait en simple vol qualifié, ce qui brouille les pistes et l'identification formelle d'un acte d'espionnage. Il arrive aussi parfois que les commanditaires recrutent des voleurs spécialisés ou de la petite délinquance pour commettre les effractions et les vols. Ainsi nous avons eu affaire à un cas ou une petite bande de voleurs avait été recrutée par le crime organisé pour voler des ordinateurs portables des cadres d'une entreprise active dans le domaine de la gestion des déchets. Ce sont plus de dix portables qui ont été volés dans le métro, les voitures, au domicile et en vol-à-la-tire.

La pose d'outils de surveillance se généralise elle aussi. Il s'agit ici de pose de micros, de caméra-espions ou encore de traceur GPS pour suivre quelqu'un sans avoir

à le « filocher » constamment. Ces outils permettent de limiter les risques de flagrants délits à l'acte de pose en lui-même. C'est sans doute l'émergence des « spyshop » - commerces vendant des outils d'espionnage et de contre espionnage – sur l'Internet qui généralise le recours à ce type de matériel. Si auparavant l'utilisation de ces outils était réservée aux services de renseignement publics, le secteur privé s'est emparé de ces technologies qui sont très abordables d'un point de vue retour sur investissement « information volée vs prix d'achat du matériel et coût de l'opération ». Habituellement les micros sont posés dans des endroits stratégiques : salles de réunion, salles de meeting, logiciels d'écoute dans le téléphone portable, salles de conférence, chambres d'hôtels et véhicules de dirigeants. Les caméras sont utilisées dans les mêmes lieux et parfois à distance pour les plus performante (longue distance, mode nuit, canon d'écoute longue distance intégré). De nouvelles générations de micros ou caméras espions dissimulés dans des stylos, boutons de manchette, montres, lunettes et encore bien d'autres ustensiles de la vie courante font surface sur le marché et sont généralement utilisés lors d'interview et de rencontres. Ce matériel devient alors un support important pour les opérateurs « HUMINT » qui conserve une trace de leurs manipulation et recrutement de sources.

Les interviews sous faux-pavillons sont utilisées dans plusieurs cas majeurs comme le recrutement de personnel ou l'interview journalistique. Intéressons-nous aux faux recrutements. Cette technique, utilisée au départ surtout dans le monde de l'aéronautique, consiste à monter une manipulation de fausse interview d'un cadre ou d'une ressource clef d'un concurrent. Quelques sociétés de recrutement jouent le jeu avec des cabinets d'intelligence économique et pousse le vice jusqu'à faire paraître des annonces dans la presse. Une fois le candidat ciblé ferré par l'appât, un spécialiste intervient sous fausse identité pour soutirer l'information sur la cible. Cette technique est redoutable car lors des rendez-vous finaux (c'est rarement au premier rendez-vous que le candidat s'épanche) le candidat est en confiance et il arrive un moment où il doit rentrer en détail sur ce qu'il a fait dans l'entreprise. Une fois l'information obtenue l'opérateur principal « démonte » (jargon du milieu) la mission en avertissant le candidat qu'au final il n'a pas été sélectionné. Certaines PME sont devenues les spécialistes de ce genre de manipulations et tout en sachant qu'ils sont en zone grise (illégale quand même) ils ignorent faire de l'espionnage industriel.

Une technique plus classique, elle aussi liée au recrutement, est utilisée depuis la nuit des temps : le recrutement de personnes clefs chez un concurrent ou un partenaire. C'est probablement le cas où les plaintes – pour concurrence déloyale notamment – sont les plus fréquentes. Le dernier cas en date est celui de l'affaire

SEAGATE/WESTERN DIGITAL où un important dédommagement a été accordé (en attendant l'appel) à l'entreprise victime du fait d'espionnage industriel.

Lorsque l'on parle de corruption pour obtenir du renseignement, on pense tout de suite à l'Afrique et à la Russie. C'est en tout cas le constat que nous faisons lorsque nous évoquons la corruption avec nos interlocuteurs. Cela dit, la corruption n'est pas le pré carré des fonctionnaires. Des actes de corruption internes peuvent aussi être réalisés pour obtenir l'information désirée. Ainsi les femmes de ménages qui «ouvrent » les bureaux le soir à quelques inconnus qui vont « chipoter » dans le bureau de la direction ou du laboratoire R&D, existent bel et bien. Et même si cela ressemble à un scénario de polar sachez que quelques banques d'affaires ont déjà été victimes, en tout cas pour ce qui concerne les faits avérés et jugés. Je n'ose même pas imaginer ce qui n'a pas été détecté ou ce qui a été laissé sous silence dans le monde industriel. La corruption c'est aussi le fait de rémunérer un « client » pour récupérer de l'information sur la concurrence. Cette technique est utilisée dans les métiers du service. Mais revenons à la corruption de fonctionnaire. Certains espions entretiennent des liens forts et financiers avec des employés d'administration. Contre monnaie sonnante et trébuchante, ils font l'acquisition de données fiscales, juridiques ou encore financières. Les opérateurs téléphoniques ne sont pas en reste non plus : recruter un agent « dormant » qui travaille au sein d'une *hotline* chez un opérateur peut servir à récupérer bon nombre de données en ce compris la liste des appels téléphoniques émis et reçus par la cible. Intéressant non ? Oui, mais tout à fait illégal et punissable par la loi. De plus, ce risque est incontrôlable puisque l'information est disponible chez un tiers hors du périmètre de sécurité de l'entreprise ou l'organisation victime.

L'argent n'est pas l'unique motivation des gens qui trahissent. Qu'ils aient la volonté ou la conscience de trahir ou pas, les sources internes restent le terrain de jeux le plus performant pour les opérateurs « HUMINT ». La manipulation est un véritable métier qui demande des compétences particulières et une aisance à déterminer ce que la source est capable de faire et sous quel prétexte. Cependant il y a une différence fondamentale entre l'espionnage privé et l'espionnage public pour ce genre d'opération. Mis à part dans le cas d'actes de terrorisme ou de menaces imminentes, les services de renseignement publics ont le temps. A contrario, les services de renseignement privé sont tenus d'obtenir des résultats et souvent à moindres coûts s'ils veulent conserver leur marge. Le recrutement de sources dormantes su le long terme est plutôt utilisé par le secteur public qui peut se permettre de capitaliser sur le renseignement futur. Pour ce qui concerne le recrutement de sources directes (directement concernée par la mission), cela se fait généralement lors de mise en situations extra-professionnelles de la source ciblée. Affronter une source directement

et d'une manière frontale ne fonctionne que dans peu de cas. Les opérateurs montent donc des scénarii et des légendes complexes pour atteindre leur cible. Travailler sur les passions, les hobbies et les problèmes des gens peut ainsi furtivement amener au contact et au recrutement final de la source.

Les visites d'entreprise sont souvent un prétexte utilisé pour dérober de l'information. Un des mes contacts officiels m'a rapporté, un jour, une bien étrange histoire. Une délégation d'entrepreneurs coréens (du Sud) était venue en visite économique dans l'Est de la France. Tout semblait bien se passer. Les entrepreneurs régionaux avaient de bonnes raisons de croire que des contrats allaient se signer et que de juteux partenariats allaient naître. La chambre de commerce locale avait organisé des visites d'entreprises pour montrer le savoir-faire des entreprises françaises et leur haut niveau technologique.

La D.S.T. [3] avait eu l'idée de dépêcher deux de ses spécialistes pour d'une part prendre de l'information sur les coréens et d'autre part sécuriser au minimum les visites d'entreprises. En effet, quelques entreprises visitées étaient stratégiques de par leurs relations avec l'industrie de l'armement. Deux hommes d'affaires coréens semblaient se comporter d'une manière étrange. Ne respectant pas les consignes de sécurité industrielle, l'un d'entre eux s'était retrouvé dans un zone non prévue au programme de la visite (il s'agissait du local à poubelles) et l'autre avait malencontreusement trempé sa cravate dans un bain chimique. Quelle ne fût pas la surprise des deux policiers quand ils constatèrent que l'indélicat coréen ne voulait ni jeter sa cravate ni la faire passer par la case nettoyage à sec !

Les soupçons étant trop grands, les policiers décidèrent de confisquer la cravate et de la faire analyser à Paris. La cravate était d'un tissu spécial qui avait des propriétés particulières spongieuses, était capable de retenir la matière dans laquelle elle avait été trempée. Le bain chimique comprenait un des secrets de fabrication de l'entreprise ciblée.

Bien entendu, cet exemple sent le scénario de série B. C'est d'ailleurs, je pense, un cas d'école dans certaines formations policières. Cependant d'autres faits m'ont été rapportés. Du visiteur qui prend des photos avec son téléphone portable à celui qui « oubli » un dictaphone dissimulé dans un classeur dans une salle de réunion, les exemples de vol d'informations sont légions lors de visite d'entreprises. Identifier certains produits, capturer de l'information papier, lire les destinataires et les expéditeurs sur des bordereaux collés sur des palettes ou encore prendre des photos

[3] Direction de la Surveillance du Territoire (ajourd'hui devenue la D.C.R.I.)

d'endroits stratégique : voilà ce que cherchent les espions industriels lors de visites d'entreprise.

Les scénarii sont aussi très divers. Bien sûr la difficulté c'est de rentrer dans l'entreprise mais un fournisseur, un client ou un prospect complice peut permettre d'ouvrir la porte de l'entreprise.

Comment se protéger efficacement ?

Le maître-mot c'est bien entendu la prévention. Avoir une démarche « curative » lorsqu'un fait d'espionnage est décelé n'amène pas à l'évitement ! La gestion efficace des risques amène quatre types de traitement du risque :

- réduction du risque : application de mesures appropriées, correctives ou de mitigation,
- acceptation du risque : avec objectivité et en connaissance de cause,
- annulation du risque : interdiction d'actions susceptibles d'engendrer le risque,
- transfert du risque : vers un tiers comme un assureur ou un fournisseur.

Toute la difficulté, face aux risques d'espionnage industriel, réside dans le fait de prendre la bonne décision. Cette décision est toujours fonction et en relation directe avec la nature des activités de l'entreprise et plus particulièrement avec la nature critique de certains domaines d'activités.

La réduction des risques d'espionnage industriel consiste essentiellement à tout faire pour que l'entreprise ne fasse pas l'objet d'un vol d'information, d'un acte d'espionnage. Parmi les mesures appropriées, l'on peut se concentrer sur la sécurité de l'information en rédigeant les procédure idoines et en mettant les systèmes de protection nécessaires pour éviter au maximum les dégâts en cas de crise.

L'acceptation des risques d'espionnage industriel consiste à accepter le risque tel qu'il est et à attendre que le fait survienne ou ne survienne pas d'ailleurs. C'est un choix, pour ma part je ne conseille cette approche que rarement. La prise de risque est toujours calculée sur le facteur « mesures de mitigation/ coûts du risque avérés ». Au décideur de faire le pari de ne pas se faire espionner. Cela dit, il faut toujours prendre en compte le fait qu'en cas d'espionnage, les mesures de réponses ou les mesures correctives peuvent avoir un coup variable. Il faut aussi prendre en compte le fait que l'acte d'espionnage sera peut-être découvert avec retard et même peut-être jamais.

La meilleure stratégie consiste bien évidemment à annuler les risques d'espionnage industriel. Cela est vrai dans un monde théorique car on ne peut pas présager de la survenance des attaques ni même contrôler les assaillant potentiels. Le décideur peut faire le choix de tendre vers l'annulation qui devient alors un objectif continu et jamais atteint (sauf en cas de cessation d'activités).

Le transfert de risques d'espionnage industriel est quasiment impossible. Bien sûr l'on peut se prémunir contre le vol et transférer le risque d'effraction ou de perte de données vers un assureur. Cela dit, le risque ne disparaît pas et les risques connexes comme la perte de confiance, d'image de marque et de notoriété augmentent au fur et à mesure que le risque d'espionnage industriel est « financièrement » couvert. Reste à dire qu'il y a une possibilité de transfert vers les autorités publiques en s'adjoignant de l'aide de services de contre espionnage, la gestion du risque est ainsi transférée ; seulement cela ne concerne que les industries particulières de la défense, du nucléaire ou de l'aérospatiale.

Le meilleur conseil que je puisse vous donner en matière de lutte contre l'espionnage industriel est de sensibiliser vos personnels. Pour ce faire il vous faudra au préalable :

- comprendre votre environnement et son exposition aux risques d'espionnage industriel,
- détecter vos faiblesses,
- évaluer les menaces potentielles,
- prendre les mesures adéquates de gestion des risques,
- gérer vos risques de manière itérative,
- veiller sur les menaces et dangers qui pèsent sur votre organisation,
- conscientiser les personnes clefs de l'entreprise et obtenir le feu vert du management,
- informer et sensibiliser à fréquence régulière tous les maillons de l'entreprise et ses partenaires d'affaires.

Pour conclure

Vous l'avez constaté, l'espionnage économique est une réalité. Il existe pléthores de raisons qui font qu'un commanditaire fasse appel à des opérateurs d'espionnage économique. Personne n'est épargné par l'espionnage industriel et tout le monde y est exposé. Le renseignement économique s'est privatisé et cela ne va pas aller en s'améliorant. Les techniques d'espionnage évoluent en fonction de la facilitation d'accès aux outils d'espionnage et à l'offre grandissante sur le marché.

Sachez que l'espionnage économique est un crime et que la « légitime défense » économique n'existe pas. Répondre à un acte d'espionnage ne doit pas se faire en utilisant les mêmes armes que vos assaillants même si la tentation est grande. Plus vos procédures d'accès à l'information seront strictes et plus les moyens de protéger votre entreprise seront efficaces, plus les opérateurs d'espionnage économique seront face à des difficultés et certains d'entre eux jetteront l'éponge avant même d'avoir tenté un piratage informatique ou une effraction. La principale faille étant humaine (lors de manipulation ou de corruption par exemple), il est nécessaire d'investir sur les moyens humains et le seul moyen est de conscientiser votre personnel et vos partenaires.

En cas de soupçon, faites appel au service de police ou au service de renseignement adéquat. N'ayez pas peur de mettre la confidence les services officiels qui se chargeront de qualifier la menace ; ces hommes sont des professionnels et ne vous pousseront pas à porter plainte si cela engage la continuité de vos activités. Les faits d'espionnage relèvent d'un monde obscur et ne s'improvise pas qui veut « contre espion ».

Notre offre

Le Réseau Vincibilis est composé d'experts en contre espionnage et en sécurité économique. Quelques uns de nos membres ont géré des faits d'espionnage dans leur carrière publique.

Nous offrons des services de détection de menaces, d'identification des risques et des diagnostics précis pour évaluer votre exposition aux risques d'espionnage. Nous assurons aussi des services de support à l'action juridique et sommes capables de dépêcher nos experts sur le terrain pour vous aider à protéger votre entreprise.

FIN.