DIX OUTILS DE LA GUERRE ÉCONOMIQUE

Lorsqu'il s'agit de faire la guerre à la concurrence, les entreprises disposent d'une palette étendue de moyens. Révision de l'arsenal.

PAR MEHDI ATMANI, CLÉMENT BÜRGE, RINNY GREMAUD ET JULIE ZAUGG
ILLUSTRATIONS : LAURENT CILLUFFO

1 LE VOL À L'ANCIENNE

Li-Li avait 22 ans lorsqu'elle a été arrêtée en avril 2005. Cette étudiante chinoise venait d'entamer un stage auprès de l'équipementier automobile français Valeo. Elle en a profité pour voler des centaines de fichiers informatiques contenant des données confidentielles. À son domicile, les enquêteurs ont retrouvé des messages encryptés en provenance de Chine, ainsi que six ordinateurs et deux disques durs ultra-puissants.

Ce cas est loin d'être isolé. Un dimanche de septembre 2011, un employé de l'usine Converteam, filiale française de General Electric, tombe sur M. Dai, un stagiaire chinois, en train de photographier sous toutes ses coutures un prototype de moteur à grande vitesse pour bateaux. Cet opérateur bobinier de 45 ans, originaire de la province de Shandong, était venu passer trois mois dans la firme française qui équipe notamment la marine. Le lendemain, il est placé en garde à vue et renvoyé dans son pays.

Ces deux exemples illustrent la technique dite du « stagiaire chinois », un classique de l'espionnage industriel. Car si les entreprises sont aujourd'hui, à juste titre, très préoccupées par le potentiel hacking de leur réseau informatique, le vol physique de données reste une réalité, et une menace importante. « Les visites d'usines sont particulièrement propices à cela, indique Edward M. Roche, qui a publié plusieurs ouvrages sur l'espionnage industriel. Un observateur avisé pourra par exemple repérer la température et le niveau de pression utilisé pour produire des puces informatiques rien qu'en passant à côté des machines utilisées pour les générer. » Une entreprise française s'est fait voler la formule d'un liquide breveté par un membre d'une délégation chinoise qui a trempé sa cravate dedans lors d'une visite d'usine, selon un rapport des services de renseignement qui a fuité.

Certaines entreprises n'hésitent pas à engager des détectives privés. À la fin des années 90, Nestlé a mandaté le cabinet Beckett Brown International pour obtenir des informations sur les nouveaux produits et les résultats financiers de Mars. L'agence a notamment placé l'un de ses hommes au sein du conglomérat américain en le faisant passer pour un nettoyeur. Cela a permis au groupe veveysan de récolter des listes d'appels téléphoniques, des relevés de comptes bancaires, des fiches de salaire et des détails sur les déplacements des employés de Mars. En 2001, Procter & Gamble a engagé des hommes de main chargés de fouiller dans les poubelles de son concurrent Unilever pour en savoir plus sur ses projets en matière de shampooings. Ils ont récolté près de 80 pages de documents confidentiels.

2 L'EFFRACTION NUMÉRIQUE

La version moderne du vol d'informations sensibles a la forme d'un acronyme : APT, pour Advanced Persistent Threat. « Une APT exige un degré élevé de dissimulation sur une longue période, explique Pascal Junod, expert en cryptographie et professeur à la Haute école d'ingénierie et de gestion du canton de Vaud (HEIG-VD). Le but d'une telle attaque est de placer du code malveillant personnalisé sur un ou plusieurs ordinateurs. » Du code pour exécuter des tâches sur de longues périodes, avec une discrétion maximale.

Ainsi, un vol de données peut se dérouler sur plusieurs mois, voire des années, sans être détecté. « Un hack est découvert au bout de 260 jours en moyenne », affirme Alexandre Vautravers, collaborateur scientifique au Global Studies Institute de l'Université de Genève et spécialiste des questions de sécurité.

Et c'est ce qui est arrivé à Ruag, le géant de l'armement suisse actuellement détenu à 100% par la Confédération (lire en p. 45). Rendu public en mai 2016, le rapport d'enquête laisse entendre que la présence de codes malicieux dans le système informatique de Ruag remontait à septembre 2014 au moins, et qu'ils avaient pour objectif d'aspirer des informations sensibles. Lesquelles ? « Nous ne le savons pas précisément, affirme aujourd'hui encore un porte-parole de Ruag. Nous savons seulement que 20 gigabytes de données ont été affectées, et qu'il ne s'agit pas d'informations mettant en péril la sécurité nationale. »

Mais quid de celles liées à ses activités commerciales ? La nature du code utilisé semble pointer vers la Russie. Quant à savoir si les données volées pourraient servir à une entreprise concurrente, l'enquête, qui se poursuit, ne le révélera sans doute jamais. Les auteurs de telles infractions sont rarement identifiés, sans même parler de leurs commanditaires.

Le hacking, à des fins d'espionnage industriel ou de guerre économique, est une pratique encore trop récente pour être abondamment documentée. Elle se différencie des actes de sabotage informatique, telles les attaques par déni de service (DDoS), du vol de mots de passe et de numéros de cartes de crédit, ou encore du vol pur et simple d'argent, qui sont des opérations spectaculaires et souvent les plus médiatisées.

« UN VOL DE DONNÉES PEUT SE DÉROULER SUR PLUSIEURS MOIS, VOIRE DES ANNÉES, SANS ÊTRE DÉTECTÉ. »

Les spécialistes s'accordent toutefois à estimer que l'implantation de logiciels espions chez un concurrent est une pratique qui existe bel et bien. Elle nécessite une préparation minutieuse et d'importants moyens financiers, ce qui en ferait une arme réservée aux entreprises d'État ou aux grands groupes industriels. La fréquence de ces attaques est difficile à estimer. Et pour cause : « Une entreprise n'a aucun intérêt à divulguer qu'elle a été victime d'un hack à distance, explique Pascal Junod. Ces problèmes se règlent entre quatre yeux. »

Une chose reste certaine : « 80% des attaques informatiques reposent sur de l'ingénierie sociale », rappelle Pascal Junod. Car le point faible de tout système informatique, ce sont les êtres humains qui l'utilisent.

3 LA FAILLE HUMAINE

Les spécialistes de l'anti-espionnage le répètent à l'envi : les employés sont la partie la plus vulnérable d'une entreprise. Les cibler représente l'une des façons les plus efficaces de récolter de l'intelligence économique. Les tactiques d'approche sont diverses : réserver un billet d'avion à côté de la personne que l'on veut faire parler, fréquenter les mêmes congrès ou l'inviter à donner une conférence. « Il existe de nombreuses techniques pour mettre quelqu'un à l'aise et le convaincre de s'exprimer, note Alain Mermoud, chercheur en intelligence économique et fondateur de la plateforme Swiss-intelligence.info. Comme demander à son interlocuteur comment il va, lui faire un compliment ou adopter une gestuelle rassurante. » Idéalement, la cible ne doit même pas se rendre compte qu'elle s'apprête à trahir son entreprise.

« Certains employés n'ont pas conscience de la valeur de l'information qu'ils détiennent, fait remarquer Nicolas Moinet, un professeur à l'École de management de Poitiers qui vient de publier un ouvrage sur la question. Un travailleur en charge des aspects techniques ne va pas se rendre compte qu'il ne doit pas divulguer de données financières sur l'entreprise, et vice-versa. »

On peut en outre jouer sur les frustrations de sa cible. « Un employé mécontent va avoir tendance à trop parler », glisse Alain Mermoud. Gillette en a fait l'amère expérience en 1998, lorsqu'un ingénieur de Wrigh Industries, une firme chargée de développer sa nouvelle génération de rasoirs, est parti en claquant la porte après s'être fâché avec son patron. Pour se venger, il a envoyé des dessins du nouvel accessoire aux concurrents de Gillette : Warner-Lambert, Bic et American Safety Razor.

L'argent a lui aussi tendance à délier les langues. Entre 2010 et 2012, Yong Pang, un ingénieur travaillant pour Dyson, a reçu plus de 11'500 livres de la part de son concurrent Bosch en échange d'informations sur les moteurs ultra-puissants qui équipent les sèche-cheveux et les aspirateurs du fabricant d'électroménager britannique. Parfois l'information peut valoir bien plus encore. Entre 1989 et 1997, un employé de la firme américaine Avery Dennison, spécialisée dans les produits adhésifs, avait reçu plus de 150'000 dollars de la part du conglomérat taïwanais Four Pillars en échange de quelques secrets de fabrication.

Il arrive que l'on joue simultanément sur plusieurs plans. Walter Liew, un entrepreneur chinois, a entretenu une relation de près de quinze ans avec Tim Spitler, un ancien ingénieur de Dupont, pour lui soutirer le secret de fabrication du dioxyde de titane, utilisé notamment pour produire le blanc de titane. Il a payé pour l'enterrement de sa fille et lui a offert 15'000 dollars. Chaque Noël, il lui envoyait en outre un panier garni. Il a aussi exploité l'amertume de cet homme qui ne s'était jamais remis des licenciements effectués par son ex-employeur dans les années 90.

« L'UTILISATION DU SEXE POUR OBTENIR DES INFORMATIONS EST UNE TECHNIQUE CLASSIQUE. »

4 LE VICE ET LE CHANTAGE

Lorsque la méthode douce ne fonctionne pas, on peut passer à la méthode forte. « On repère un employé qui détient l'information dont on a besoin, puis on fouille dans son passé ou dans sa vie privée pour trouver des failles à exploiter, détaille Edward M. Roche. On va ensuite le menacer de divulguer ces secrets à son employeur ou à ses proches s'il ne coopère pas. »

Parfois, on le pousse carrément au vice. Dans un rapport des services de renseignement français daté de 2010, on apprend qu'un chercheur d'une grande entreprise pharmaceutique s'est fait inviter à dîner, puis séduire par une jeune femme chinoise. Le lendemain, lorsqu'elle lui a montré l'enregistrement vidéo de leurs ébats, réalisé à son insu, il s'est dépêché de lui livrer toutes les informations qu'elle voulait. « L'utilisation du sexe pour obtenir des informations est une technique classique », explique un spécialiste suisse du renseignement.

Ce chantage atteint parfois des sommets de perversité. Edward M. Roche cite le cas d'un ingénieur chinois travaillant aux États-Unis qui s'est fait contacter par les services de renseignement de son pays d'origine pour obtenir des données confidentielles sur son travail. Il a refusé de les livrer. Quelques mois plus tard, il apprenait que son frère, souffrant de retard mental et vivant en Chine à des centaines de kilomètres de sa mère, avait été déplacé tout près du domicile de cette dernière. Lorsque les espions chinois sont revenus le voir, il leur a tout donné. « Le message était limpide : s'il n'obtempérait pas, son frère serait à nouveau envoyé à l'autre bout du pays, et il n'a pas eu le cœur d'infliger cela à sa mère », relate l'expert.

5 FAUX APPELS D'OFFRES ET EMBAUCHES FACTICES

La guerre économique est fondée sur une multitude de petits et de gros mensonges. « Les faux appels d'offres sont l'une des tactiques les mieux éprouvées pour obtenir de l'information sur l'offre et les prix pratiqués par ses concurrents, livre Éric Denécé, le directeur du Centre français de recherche sur le renseignement. On lance un appel, on étudie les propositions reçues, on demande plus de détails et au final on ne passe pas commande. » Cette méthode a en outre pour avantage de neutraliser ses compétiteurs. « Lorsqu'ils sont occupés à répondre à un appel d'offres, ils ne font pas autre chose », glisse le spécialiste.

En 2008, la société française ECA Robotics se fait contacter par la firme chinoise Shenzhen Zhong Zhen Tong. Celle-ci lui fait miroiter un contrat d'achat d'une centaine de pièces de son robot Inbot. Chaque machine vaut 20'000 euros. Mais elle veut d'abord en acquérir une, pour la tester, dit-elle. Cette première commande est honorée puis, plus rien. Deux ans plus tard, la firme basée à Shenzhen sort son propre robot, étrangement identique à celui d'ECA Robotics.

Ce procédé n'a pas été inventé par les industriels chinois. Au début des années 60, le groupe américain Douglas Aircraft avait lancé un appel d'offres pour produire un avion moyen-courrier. L'un des postulants, le français Sud Aviation, venait de développer la Caravelle, le premier appareil moyen-courrier au monde. Après réflexion, Douglas Aircraft décide de produire son avion à l'interne. « Peu de temps après, raconte Nicolas Moinet, le DC-9 débarquait sur le marché, présentant de méchantes similarités avec la Caravelle… »

Les faux recrutements sont une autre façon d'obtenir de l'information sur les pratiques de ses compétiteurs. « On place une annonce pour un poste à pourvoir et on voit une trentaine de candidats, explique Éric Denécé. Durant l'entrevue, on leur demande de détailler les principaux projets qu'ils ont menés à bien auprès de la concurrence et au bout du compte, on n'engage personne. » Pris dans la logique de l'entretien, ils vont se lâcher, tenter de convaincre ce futur employeur en lui livrant une multitude d'informations sur leurs accomplissements.

En Suisse, les milieux financiers utilisent parfois cette méthode. « Cela permet de se renseigner sur le nombre de personnes travaillant sur les desks des autres banques ou de savoir combien d'actifs ces derniers ont sous gestion », indique Alain Mermoud. Et si dans le cadre de ces faux entretiens, on tombe sur la perle rare, rien n'empêche de l'engager.

Dans les années 2000, deux anciens cadres de Starwood ont été débauchés par Hilton. Ils ont amené avec eux plus de 100'000 pages de données confidentielles détaillant un nouveau concept d'hôtels appelé W, développé par leur ex-employeur. Hilton a ensuite lancé en 2009 sa propre marque d'établissements lifestyle, Denizen. Mais Starwood ne s'est pas laissé faire et a déposé plainte contre Hilton, qui a dû stopper son projet et payer 75 millions de dollars à Starwood, en plus de lui attribuer pour 75 millions de contrats de gestion.

6 CONNAÎTRE SON ENNEMI

La guerre économique passe aussi par une surveillance et une analyse des nombreuses sources figurant dans le domaine public. On appelle cela l'information blanche, car elle est légale et libre d'accès. Lorsque ces sources sont payantes, on parle d'intelligence grise.

« Admettons que nous travaillons pour un groupe pharmaceutique, détaille Albert Pélissier, qui dirige le cabinet d'intelligence économique romand Pélissier & Partners. Nous allons examiner les brevets émis dans son domaine, répertorier les normes légales adoptées, garder un œil sur ce qui se dit dans les colloques et les salons, consulter les publications scientifiques et recenser l'offre et les prix pratiqués par ses compétiteurs. » Cela va lui permettre de mieux lutter contre la concurrence, d'identifier – en toute discrétion – des firmes à acquérir et de découvrir de nouveaux débouchés pour ses produits.

« ON PEUT AUSSI SONDER LE WEB INVISIBLE, SOIT LES DONNÉES QUI NE SONT PAS INDEXÉES PAR DES MOTEURS DE RECHERCHE TRADITIONNELS. »

Les méthodes utilisées reposent aussi sur le big data. « Il existe de nombreuses bases de données spécialisées en ligne, comme LexisNexis qui regroupe des informations légales ou Factiva qui agrège les contenus publiés par les médias du monde entier », note Alain Mermoud. De même, la plupart des pays ont un registre du commerce qui recense les sociétés incorporées sur leur sol. Et l'Organisation mondiale de la santé tient un portail qui détaille tous les essais cliniques menés dans le domaine médical.

« On peut aussi sonder le web invisible, soit les données qui ne sont pas indexées par des moteurs de recherche traditionnels comme Google, en utilisant des fonctionnalités de recherche avancées ou des serveurs d'information professionnels qui permettent d'effectuer des recherches très poussées via des logiciels de data mining », relève Anne-Marie Libmann, directrice opérationnelle du cabinet d'intelligence français FLA Consultants. Les archives de journaux, les flux RSS et les réseaux sociaux sont d'autres façons de récolter de l'information utile.

7 LA CELLULE DORMANTE

Prendre le dessus sur un compétiteur est un travail de longue haleine. En 2004, Chi Mak, un ressortissant chinois naturalisé américain, travaillait depuis plus de vingt ans pour Power Paragon, une entreprise d'armement. « Il faisait partie des meubles, relate Edward M. Roche. Il était ami avec le CEO de la firme. Ils faisaient des pique-niques en famille. » Or durant toutes ces années, il œuvrait pour le compte des services de renseignement chinois, en tant que taupe infiltrée qui pouvait à tout moment être activée. Il s'est fait prendre en 2004, lorsqu'il a cherché à exfiltrer vers la Chine trois CD-Roms contenant des informations sur un nouveau système de propulsion silencieuse pour sous-marins.

Ce n'est pas un cas isolé. En 2015, le Département américain de la justice a inculpé six citoyens chinois qui avaient cherché à voler des données brevetées aux fabricants de puces informatiques Avago Technologies et Skyworks Solutions pour les utiliser en Chine. Or, deux de ces hommes étaient des employés de longue date des deux entreprises visées.

Huang Yusheng était l'un des employés les plus respectés de Serenex, une petite société pharmaceutique basée en Caroline du Nord. Sa spécialité : les traitements anti-cancer. Quelle n'a donc pas été la surprise des dirigeants de l'entreprise de découvrir en 2007 qu'une demande de patente avait été faite auprès de l'Organisation mondiale de la santé et en Chine pour une molécule quasiment identique à celle sur laquelle Huang Yusheng travaillait. Elle avait été déposée par Zhang Tongxiang, l'un de ses amis.

EN TOUTE LÉGALITÉ

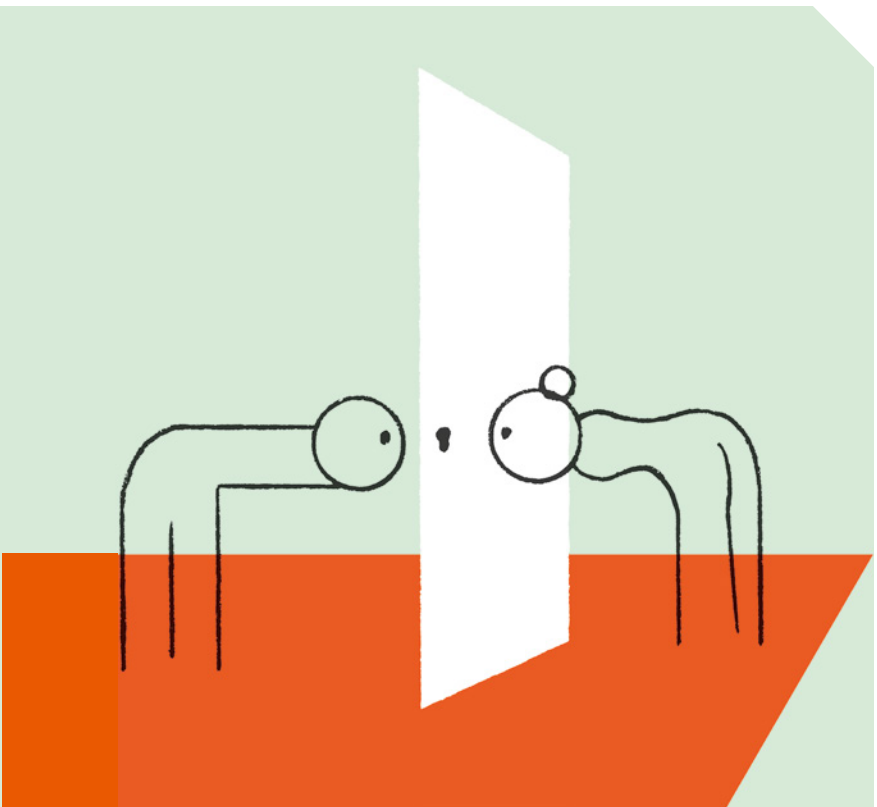
LA LÉGISLATION D'UN PAYS PEUT SERVIR D'ARME OFFENSIVE

La guerre économique n'est pas toujours une affaire de secrets et de dessous de table. Certaines batailles se mènent de front. « La loi chinoise oblige les entreprises qui souhaitent investir dans le pays à opérer des transferts de technologie, explique Edward M. Roche. Elles doivent former des ingénieurs locaux, fournir des procédés et créer des usines sur place. » Kawasaki, l'inventeur du Shinkansen, en a fait les frais. La technologie que le groupe japonais a fournie à son homologue chinois CSR Sifang dans le cadre d'un accord conclu en 2004, a permis à l'Empire du Milieu de développer son propre train à grande vitesse. Il s'agit d'une copie quasi conforme du Shinkansen.

De même, l'inauguration en 2008 par Airbus d'une ligne d'assemblage pour l'A320 à Tianjin sera suivie quelques années plus tard par l'annonce d'un nouvel avion 100% chinois, le Comac C919, dont le premier vol a eu lieu en 2016. Il ressemble beaucoup à l'A320. Mais là non plus, la méthode n'est pas exclusivement chinoise. « Dans les années 80, le Brésil a mené une politique similaire, obligeant les entreprises qui souhaitaient profiter de son immense marché à produire sur place, avec du personnel et des composants locaux », précise Edward M. Roche. Cela lui a permis de développer une industrie informatique, largement inspirée par la R&D des groupes américains opérant sur son territoire.

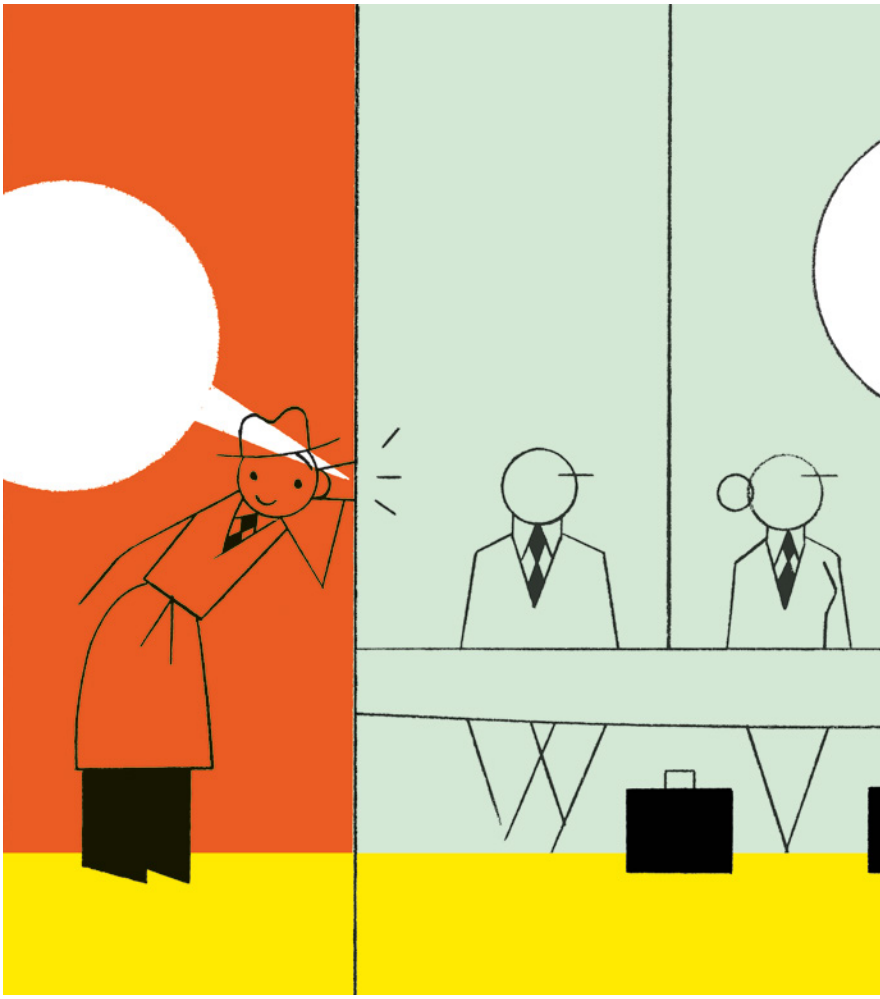
La législation d'un pays peut aussi servir d'arme offensive. « Les Américains utilisent leur loi anti-corruption pour cibler les industries françaises qui sont en concurrence avec les leurs, comme le pétrole, l'armement et la finance », dit Éric Denécé. Pour lui, la décision d'imposer une amende de 8,9 milliards de dollars à la banque française BNP Paribas pour avoir fait des affaires en Iran ou de s'en prendre avec autant de virulence aux banques helvétiques accusées d'évasion fiscale relève de cette logique.

De même, l'acharnement de la justice américaine contre Alstom, qui s'est vu infliger en 2014 une amende de 772 millions de dollars pour des affaires de corruption en Indonésie, en Arabie saoudite ou en Égypte aurait eu pour principal but d'affaiblir le groupe d'ingénierie français. « Cela a ouvert la voie à son rachat par General Electric en 2015 », estime Éric Denécé. Le montant de la transaction, qui s'est élevé à 10 milliards de dollars, serait bien en deça à de la valeur réelle de ce fleuron de l'économie française, de l'avis de plusieurs spécialistes.



LES GRANDES OREILLES

La technique de l'écoute est un grand classique. Pose de micros dans les salles de réunion d'une entreprise, « écoute » du réseau wifi des aéroports, fréquentation des lounges VIP. « C'est fou ce que l'on peut récolter comme informations utiles en faisant régulièrement le trajet Paris-Londres en première classe », raconte un professionnel du renseignement. Toutefois, ces méthodes sont chronophages et sans garantie de résultat, ce qui les disqualifie souvent aux yeux des spécialistes.



« Ces techniques existent, mais elles sont dépassées, estime Alain Mermoud. Pour acquérir de l'information aujourd'hui, le plus simple est de le faire avec des sources ouvertes, sur Internet et les réseaux sociaux. » Reste qu'en matière d'écoutes, certains dispositifs d'État, autrement plus puissants, sont parfois mis au service des grandes entreprises nationales. Des méthodes qui n'auront pas attendu les plus récentes révélations d'Edward Snowden pour être connues. Bien avant d'apprendre que la NSA interceptait systématiquement les communications dans les avions d'Air France, il y a eu l'affaire « Échelon ».

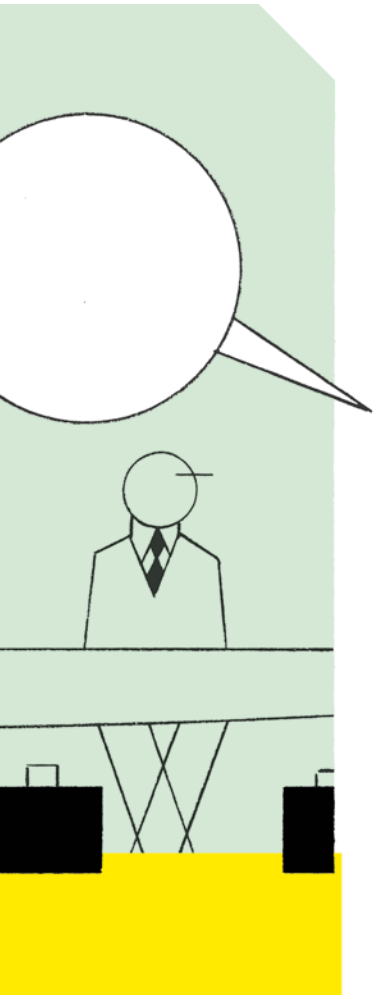
En 2000, l'Union européenne s'émouvait d'apprendre l'existence de ce vaste réseau d'écoute électronique né en 1947 pour espionner les cibles militaires soviétiques. Avec le temps, il s'est reconverti pour obtenir des informations privées, commerciales et non militaires. Aucune preuve solide n'a jamais démontré qu'Échelon a été utilisé à des fins d'espionnage industriel.

Toutefois, dans une interview donnée au *Figaro* dans le cadre de ce scandale, James Woolsey, un ancien directeur de la CIA, estimait que les États-Unis étaient pour ainsi dire obligés de recourir à cette forme d'espionnage industriel, puisque les Européens, eux, n'hésitaient pas à distribuer des pots-de-vin pour obtenir des marchés. À la guerre économique comme à la guerre.

Et l'homme d'admettre à demi-mots que l'avionneur européen Airbus, par exemple, avait perdu un contrat en Arabie saoudite au profit de l'américain McDonnell-Douglas grâce à des informations recueillies par Échelon.

Le scandale récent des moteurs truqués de Volkswagen aux États-Unis pourrait avoir son origine dans ces mêmes méthodes, suggère Alain Mermoud. « Lorsque l'on étudie les mécanismes qui ont permis d'organiser le scandale, on note tout un faisceau d'éléments démontrant que les attaques contre VW ont été conçues par les États-Unis pour favoriser son industrie automobile. »

10 LA MAUVAISE RÉPUTATION



Les batailles se gagnent aussi en affaiblissant son adversaire. « On fait circuler des rumeurs ou des informations négatives au sujet d'un concurrent pour l'écarter d'un appel d'offres ou d'un marché en le décrédibilisant », détaille Éric Denécé.

CES TACTIQUES DE DÉSTABILISATION PEUVENT AVOIR POUR BUT DE FAIRE PERDRE DE L'ARGENT

En août 2016, le groupe français DCNS, une industrie nationale dont Thales est aussi actionnaire, a subi une fuite importante : 22'000 pages de détails confidentiels sur des sous-marins qu'il construisait pour l'Inde ont été livrés à la presse australienne. En faisant douter de sa capacité à assurer la sécurité de ses installations, cet incident a affaibli la position de l'entreprise française alors qu'elle était en train de négocier avec l'Australie un contrat de 50 milliards de dollars portant sur 12 sous-marins de dernière génération.

Ces tactiques de déstabilisation peuvent aussi avoir pour but de faire perdre de l'argent à un concurrent. Éric Denécé pense que la publication en 1990 d'informations sur la découverte de traces de benzène dans les bouteilles d'eau de Perrier ne doit rien au hasard : « Ces révélations ont obligé Perrier à retirer de la vente des millions de bouteilles et permis son rachat par Nestlé deux ans plus tard à un prix très avantageux. »

De même, le groupe de construction français Vinci a été victime de la publication en novembre d'un faux communiqué de presse annonçant le licenciement de son directeur financier suite à la découverte de graves erreurs comptables. « Cela a fait chuter son action de plus de 18% », relève Nicolas Moinet.

Mais comment faire circuler une rumeur sans se faire repérer ? « Le plus souvent on passe par un intermédiaire, relève Alain Mermoud. Cela peut être un journaliste à qui on glisse l'information ou une organisation de défense des consommateurs qu'on alerte ou encore une ONG que l'on rend attentive à un scandale. » Ces acteurs vont jouer le rôle de caisse de résonance.

À l'extrême, on peut même financer une étude qui a pour but de décrédibiliser les produits d'un concurrent. Ou créer de toutes pièces une ONG qui dénoncerait ses pratiques. ◢