

La France, terrain de jeu privilégié des espions chinois



La France,
terrain de
jeu
privilégié
des
espions
chinois

Au début du mois, « l'Obs » dévoilait l'existence d'un centre d'écoutes des services de renseignement chinois en banlieue parisienne. Si la Chine a démenti les affirmations de l'hebdomadaire, l'exécutif français n'a absolument pas réagi. Une passivité qui dit bien la liberté d'action dont bénéficient en France les espions chinois. Impossible de prendre le risque d'une brouille diplomatique avec Pékin pour une vague affaire d'espionnage compte tenu des enjeux commerciaux.



Lors de la visite du président chinois, Xi Jinping, à Paris en mars 2014 – Orban Thierry-POOL/SIPA

Une annexe de la « NSA chinoise » en banlieue parisienne ! Au début du mois de décembre, l'Obs dévoilait l'existence de ce que l'hebdomadaire croyait être un centre d'écoutes des services de renseignements chinois.

« C'est une totale invention !, tonne Monsieur Wu, chargé de communication de l'ambassade de Chine en France, Ces installations ne font qu'assurer le système de communication de l'ambassade. Cela permet des connexions sécurisées. Cela a été fait en totale conformité avec la législation française. Nous respectons les lois françaises. J'ai sous les yeux les papiers datés du 11 octobre 2002 qui attestent de l'autorisation donnée par l'Autorité de régulation des télécoms qui est parfaitement au courant de ces installations. Il n'y a là bas que des diplomates, aucun militaire. Tout est transparent ». Quand nous lui demandons, si la totale transparence et la bonne volonté chinoise pourraient aller jusqu'à nous laisser visiter ces installations, Monsieur Wu hésite tout de même... avant de répondre par la négative ! La transparence a des limites...

Paradoxalement, du côté français, on est encore moins prolixe. Interrogé sur l'existence supposée d'un bâtiment des renseignements chinois sur le territoire français, le quai d'Orsay répond « pas de commentaires ». En théorie, le ministère de l'Intérieur, les Affaires étrangères et les services de renseignement français sont parfaitement au courant de l'existence de cette annexe de l'ambassade de Chine et les autorités françaises auraient même validé l'installation de ces antennes.

Les « grandes oreilles » de Pékin en France... par *LeNouvelObservateur*

Si l'Obs surévalue sans doute en partie la menace représentée par les trois paraboles perchées sur ce bâtiment de Chevilly-la-Rue au point d'en faire une annexe de la « NSA chinoise » – on « souhaite » à Pékin de disposer d'autres moyens pour espionner Paris –, l'article de l'hebdomadaire, que l'on sent largement alimenté par la DGSI, dit bien toute la frustration et l'impuissance du contre-espionnage français face au pillage d'informations exercées par l'Empire du Milieu en France. Compte tenu du poids économique que représente la Chine pour la France, les espions chinois opèrent en effet relativement tranquillement sur le territoire français au grand dam du contre-espionnage français.

La France n'a tout simplement pas les moyens de se payer une brouille diplomatique avec Pékin au prétexte de trois paraboles installées en banlieue parisienne. Les milliards de contrats commerciaux signés avec les Chinois valent bien quelques sacrifices... Ce laisser-faire relève néanmoins de l'humiliation permanente pour les services français, contraints d'avaler toutes les couleuvres chinoises.

Non que Pékin ne possède pas, comme les Américains, mais aussi comme la France, de « grandes oreilles » un peu partout dans le monde, et prioritairement dans les pays et les dictatures amies du régime. En 2008, dans son ouvrage *Les services secrets chinois*, Roger Faligot estimait déjà que la Chine jouait dans la cour des grands avec les Etats-Unis et la Russie en matière de renseignement électro-magnétique. Six ans plus tard, les budgets du renseignement chinois ont explosé et les techniciens ont progressé, formés depuis les années 80 par le BND allemand et même jusque dans les années 90 par... la NSA américaine.

Selon Roger Faligot, la Chine a mis en place au fil des ans une « armée populaire des cyberguerriers » : « Ce service dépend de l'armée populaire de libération. Il est organisé en deux départements qui travaillent sur le renseignement de guerre et l'interception des communications. Ils procèdent en envoyant des virus qui permettent de pirater des informations ou de bloquer des sites gênants. Ils opèrent également en mode "testing" en piratant des systèmes pour étudier la capacité de réaction de l'ennemi. Nous sommes ici en plein volet de guerre psychologique et idéologique ».

Une guerre surtout économique désormais, comme l'avait illustré en septembre dernier une enquête de Franck Renaud et Hervé Gattegno parue dans *Vanity Fair*. Les journalistes avaient mis la main sur un rapport de la délégation interministérielle à l'intelligence économique (D2IE) sur les objectifs et méthodes chinoises pour piller les innovations technologiques françaises. Un espionnage d'une toute autre ampleur que le renseignement d'origine électro-magnétique. Cette instance signale chaque année plusieurs dizaines de vols ou tentatives de vols de données par captation ou indiscrétion. Toutes les techniques d'espionnage seraient utilisées. De la simple « oreille baladeuse » chinoise dans les trains Thalys ou Eurostar largement fréquentés par les industriels, aux « agents de charme » chargés de séduire les élites industrielles, à l'organisation de voyage de tourisme industriel, à l'infiltration d'étudiants chinois dans les universités françaises, le vol de matériels informatiques ou bien encore des méthodes de « phishing » très sophistiquées. Il faut aussi ajouter l'incroyable « pouvoir de persuasion » des Chinois pour imposer à leurs partenaires des transferts de technologies lors de la signature de contrats commerciaux ou la création de joint-ventures, de filiales communes.

« La Chine est déterminée à devenir indépendante de l'Occident en matière d'innovation technologique. Elle est donc avide de connaissances, de savoir-faire et de procédés à faire venir en Chine ou à absorber à l'étranger » précisait le rapport de la D2IE. De leur côté, « les entreprises françaises, attirées par ce marché qu'elles envisagent immense (...) et par les coûts de main-d'œuvre locaux inférieurs aux coûts européens, sont souvent prêts à transférer leur technologie et leur savoir-faire, fournissant ainsi un avantage à leurs concurrents chinois ».

Paris se rassure en estimant que Pékin n'a pas encore les capacités d'exploiter à plein les renseignements politiques, économiques ou industriels qu'ils obtiennent, la Chine se limitant pour l'instant à du rattrapage technologique et à des copies de mauvaise qualité. Mais les énormes moyens affectés à la cyberguerre servent aussi le renseignement économique notamment par le biais de piratages informatiques massifs ainsi que le vol de propriété intellectuelle.

Derrière chaque touriste chinois, un espion potentiel ?

En 2013, la société de sécurité américaine Mandiant publiait un rapport documenté (accessible librement http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf) sur l'unité 61398 du renseignement chinois. Chargée du « suivi » des pays de langue anglaise, l'unité aurait compromis jusqu'à 141 entreprises dans vingt grands secteurs industriels, en dérobant un volume considérable d'informations relevant de la propriété intellectuelle. L'infrastructure de commandement et de contrôle de cette unité compterait de 850 à 1 000 machines situées dans 13 pays. Le coût de ce pillage informatique des entreprises américaines était estimé à au moins 24 milliards de dollars en 2012. L'unité 61046, chargée notamment du suivi de l'Europe, fonctionne sans doute sur le même principe avec la même efficacité, mais est moins connue.

Elle a néanmoins permis aux espions chinois d'accéder aux ordinateurs du président de la Commission européenne, du ministère français des Finances en mars 2011 même de l'Elysée en juillet 2012, causant à l'époque une panique certaine dans les couloirs de la présidence. Chaque attaque est l'occasion pour les services occidentaux d'identifier les priorités des services chinois ainsi que les commanditaires pour mieux connaître leur organisation encore très nébuleuse.

Un an plus tard, dans une mise à jour de son rapport, la société Mandiant disait avoir constaté une « mise en sommeil » pendant quelques mois des activités de l'Unité 61398 suite à la publication de son rapport et aux protestations américaines. De même, toutes les adresses IP des cyberattaques chinoises qui ont frappé les Etats-Unis depuis ont été modifiées, suggérant un changement de stratégie des renseignements chinois.

Mais l'espionnage informatique continue. En octobre dernier, une société américaine de cybersécurité privée identifiera une nouvelle unité de espions informatiques chinois baptisée « groupe Axiome » : « Axiome est chargé de diriger les opérations de cyberespionnage très sophistiquées contre de nombreuses grandes entreprises, des journalistes, des groupes écologistes ou pro-démocratie, des sociétés de logiciels, des établissements universitaires et des organismes gouvernementaux dans le monde entier ». Cibles prioritaires : Les Etats-Unis, l'Europe et les voisins asiatiques.

Le Washington Post dévoilera quelques jours plus tard une note du FBI destinée aux industriels américains les alertant sur cette unité de cyberpirates que le FBI considérait comme directement liée aux services de renseignements chinois et jugeait plus performante que l'unité 61398.

Une forme d'espionnage aigüé qui oblige les services français à une attention de tous les instants. Très récemment la lettre spécialisée Intelligence online rapportait l'escapade à Saint-Nazaire d'une équipe du service culturel de l'ambassade de Chine, venue célébrer l'anniversaire de la construction d'un bateau de croisière chinois. La délégation se serait tellement attardée à « mitrailler » le porte-hélicoptères Mistral destiné à la Russie que cela aurait fini par éveiller les soupçons de la DGSI. De la surveillance à la paranoïa, il n'y a parfois pas loin.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : http://www.marianne.net/La-France-terrain-de-jeu-privilegie-des-espions-chinois_a243309.html
par Régis SOUBROUILLARD – Marianne

4,5 millions de données médicales dérobées aux Etats-Unis – Un vol de données de plus...

Community Health Systems, un spécialiste américain de la gestion des hôpitaux, a reconnu avoir été victime d'une attaque informatique entre avril et juin 2014. Résultats : 4,5 millions de données personnelles ont été dérobées. Un vol de données de plus...