sur sudouest.fr
Puisseguin : la vie après
Notre dossier spécial

du point de vue des échanges commerciaux et économiques », a commenté Wu Shaohua, représentant de la troisième banque d'État chinoise. De nombreux investissements chinois sont bienvenus. Et les groupes français sont très actifs en Chine, formidable relais de la croissance mondiale. Le problème majeur est sans doute ailleurs. Aucun de ces investissements n'est le fruit de la seule initiative privée. Le Parti communiste chinois contrôle les réserves de change. Il a développé au niveau national et dans les provinces une série de fonds publics qui pilotent ces engagements. C'est la municipalité de Shanghai qui est, en fait, l'actionnaire d'Accor par exemple. « Tous ces capitalistes chinois sont soumis à un contrôle politique et nous manquons en France et en Europe de moyens de droit pour contrôler et réguler ces investissements », résume Philippe Delalande. Alors que les investissements en Chine ne peuvent se faire que via une entreprise chinoise. Il appelle les pouvoirs publics à moins de naïveté.

(1) « La Chine depuis le Congrès de 2012. Ambitions et résistances », éditions L'Harmattan.

Le tourisme et l'hôtellerie ciblés

CAPITAL Plusieurs fleurons de l'économie française sont passés sous contrôle chinois, total ou partiel

Le rachat d'Adisseo, spécialisé dans l'alimentation animale, à Rhône-Poulenc en 2006, fait de cette société le plus gros employeur chinois de France, avec 2 000 salariés. Son nouveau propriétaire est une filiale de ChemChina, conglomérat industriel dirigé par un membre du Parti communiste chinois. L'entreprise a été créée en 1939, à Commentry, dans l'Allier, par un polytechnicien, Marcel Lingot. Deux autres sociétés importantes sont passées sous le contrôle total des Chinois.

Début 2015, le chinois Fosun, plus grand conglomérat privé du pays, basé à Shanghai, devenait, à l'issue d'une longue bataille boursière, l'actionnaire majoritaire du Club Méditerranée pour un peu moins de 1 milliard d'euros. L'opération s'est faite en total accord avec le conseil d'administration de l'entreprise et son PDG, Henry Giscard d'Estaing, qui y voyait une opportunité de développement en Asie. En 2015, la société Jin Jiang, premier groupe hôtelier et de voyage chinois, prenait le contrôle de Louvre Hôtels, le groupe français qui exploite, dans 51 pays, les hôtels Première classe, Kyriad ou Campanile. Jin Jiang est aussi le premier actionnaire du groupe Accor, numéro quatre mondial de l'hôtellerie, avec 12,6 % du capital.

En 2011, c'est un des fonds souverains, China Investment Company, qui prenait 30 % du capital d'Engie Exploration et Production. Les nouvelles technologies aiguisent aussi les appétits chinois. EDevice a inventé une box qui permet, quel que soit l'opérateur, la gestion partagée de données de santé entre le patient et le centre de soins. Elle vient tout juste d'être rachetée par iHealth, propriété du groupe chinois Anton, pour 94 millions d'euros. Créée en 2000 à Mérignac, eDevice y emploie 30 salariés.

Fosun est devenu actionnaire majoritaire du Club Med avec l'accord de son PDG. PHOTO AFP

Des questions après la cyberattaque massive

INTERNET Certains sites ont été empêchés de fonctionner durant plusieurs heures, suscitant l'inquiétude des autorités américaines

Une cyberattaque menée en plusieurs vagues a sérieusement perturbé le fonctionnement d'Internet vendredi aux États-Unis, privant des millions de personnes d'accès à Twitter, Spotify, Amazon ou eBay notamment et suscitant l'inquiétude des autorités. Aucun de ces sites n'était directement visé par les pirates. Ils s'en sont en réalité pris à la société Dyn, qui redirige les flux Internet vers les hébergeurs et traduit en quelque sorte des noms de sites en adresses IP.

« Quand je vois une telle attaque, je me dis que c'est un État qui est derrière », estime Eric O'Neill, responsable de la stratégie pour la société de sécurité informatique Carbon Black et ancien chargé de la lutte contre l'espionnage au FBI (police fédérale). Pour cet expert, les conséquences pourraient être beaucoup plus graves dans les secteurs de la finance, du transport ou de l'énergie, bien moins préparés que Dyn à ce type de cyberattaques.

> « Quand je vois une telle attaque, je me dis que c'est un État qui est derrière »

« C'est une attaque très élaborée. Chaque fois que nous la neutralisons, ils s'adaptent », a expliqué Kyle Owen, un responsable de Dyn, cité sur le site spécialisé Techcrunch. La première attaque, lancée à 11 h 10 GMT, a été suivie par plusieurs offensives successives à mesure que l'impact se déplaçait de la côte est des États-Unis vers l'ouest du pays. À 22 h 17 GMT, Dyn a indiqué que l'incident était résolu.

En pleine recrudescence de la cybercriminalité, cette attaque a alerté les autorités américaines. « Le département de la Sécurité intérieure (DHS) et le FBI ont été informés et enquêtent sur toutes les causes potentielles », a indiqué une porte-parole du DHS. L'identité et l'origine géographique des auteurs demeurent encore inconnues.

WikiLeaks et les Anonymous

Le site WikiLeaks a cru déceler dans cette attaque une marque de soutien à son fondateur, Julian Assange, réfugié dans l'ambassade de l'Équateur à Londres et dont l'accès à Internet a été récemment coupé. « M. Assange est toujours en vie, et WikiLeaks continue de publier. Nous demandons à nos soutiens d'arrêter de bloquer l'Internet américain. Vous avez été entendus », a twitté le site. Le groupe de hackers Anonymous semblait, lui, appeler à poursuivre l'offensive. « Le toit, le toit, le toit est en feu. Nous n'avons pas besoin d'eau. Laissez l'enfoiré brûler », a-t-il twitté.

Quelle qu'en soit l'origine, l'attaque a mis en lumière les dangers que présente l'utilisation croissante des objets connectés, qui peuvent être utilisés à l'insu de leurs propriétaires pour bloquer l'accès à un site. La technique employée vendredi consiste à rendre un serveur indisponible en le surchargeant de requêtes. L'attaque est souvent menée à partir d'un réseau de machines zombies (« botnets »), elles-mêmes piratées.

Les Anonymous ont appelé à poursuivre l'offensive. PHOTO AFP

Sophistication et précision

« Ces attaques vont continuer à harceler nos organisations. Malheureusement, ce que nous voyons n'est que le début en termes de "botnets" à grande échelle et de dommages disproportionnés », prédit ainsi Ben Johnson, ex-hacker pour l'agence américaine de renseignement NSA et cofondateur de Carbon Black.

Des objets connectés et a priori totalement inoffensifs comme des machines à café ou des réfrigérateurs peuvent ainsi être utilisés par des pirates. « Internet continue de se reposer sur des protocoles et une infrastructure conçus avant que la cybersécurité ne soit un problème », relève M. Johnson.

> Des objets a priori inoffensifs comme des machines à café ou des réfrigérateurs peuvent être utilisés par des pirates

Selon James Scott, expert en cybercriminalité de l'Institute for Critical Infrastructure Technology, des attaques similaires ont été menées en décembre 2015 par des cyberdjihadistes à l'aide de 18 000 appareils mobiles. Cette nouvelle attaque « trahit une vulnérabilité bien connue dans la structure d'Internet », assure-t-il, ajoutant que sa « sophistication » et sa « précision » semblaient pointer du doigt un État comme la Chine ou la Russie.

Les attaques informatiques et autres actes de piratage sont en pleine recrudescence aux États-Unis et dans les autres pays industrialisés. Yahoo Mail a récemment reconnu que les données de 500 millions de ses utilisateurs avaient été compromises il y a deux ans. Plusieurs attaques ont également visé le secteur financier, conduisant les pays du G7 à adopter, mi-octobre, une série de règles de protection.