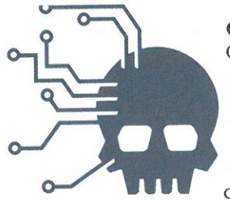
GUERRE ÉCONOMIQUE : LES PATRONS DÉGAINENT L'ARME NUMÉRIQUE

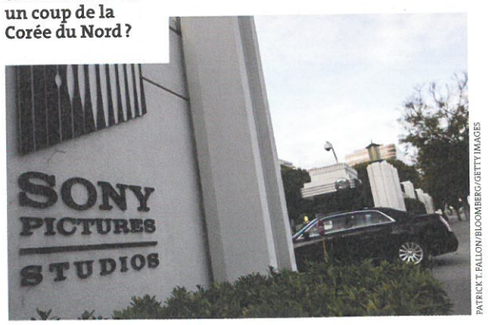
Les entreprises intègrent de plus en plus les cyberattaques illégales dans leur stratégie, pour maintenir leur avance... ou combler leur retard. Et ce, bien souvent, avec l'aval – et le soutien logistique – de leur gouvernement.

PAR **NICOLAS ARPAGIAN** DIRECTEUR SCIENTIFIQUE DU CYCLE SÉCURITÉ NUMÉRIQUE À L'INHESJ



Cent millions de dollars! C'est le montant évalué en août 2015 par la Securities and Exchange Commission (SEC), le gendarme américain de la Bourse, des gains frauduleux obtenus par des courtiers, notamment en France et aux États-Unis. Ils ont spéculé sur des titres phares comme Boeing, Caterpillar, Delta Air Lines, Ford, HP, Netflix... Avec des informations obtenues avant qu'elles soient connues du marché. Annonces de résultats, projets de fusion, découvertes de nouveaux produits... Ces financiers véreux étaient au courant avant tout le monde car ils passaient commande à deux jeunes pirates ukrainiens qui s'infiltraient dans les principales bases mondiales de publication de communiqués financiers (Business Wire, PR Newswire...) et leur transféraient en avant-première les informations prévues pour être publiées ultérieurement. En connaissant avant tout autre investisseur les grands événements qui affectent les sociétés cotées, les financiers positionnaient leurs ordres d'achat et de vente en conséquence. Leur manège a duré de février 2010 au printemps 2015. Cette affaire réunit toutes les composantes des opérations offensives envers les entreprises dans le cyberespace. Avec Internet, on peut coaliser des attaquants isolés répartis sur des territoires géographiques épars, les actifs visés (argent ou informations stratégiques) sont désormais convertis en données informatiques captables à distance, les outils informatiques ou les prestataires spécialistes ès piratage sont accessibles après quelques petites heures de recherche sur la Toile et, enfin, la faible coopération judiciaire internationale en matière de cybercriminalité favorise encore nettement les agresseurs.

Fin 2014, Sony Pictures Entertainment est victime d'un piratage massif de ses serveurs. Une attaque revendiquée par un mystérieux groupe de hackers, les Guardians of Peace... Est-ce un coup de la Corée du Nord ?



PATRICK T. FALLON/BLOOMBERG/GETTY IMAGES

QUAND L'ÉLECTRICIEN SURVEILLE LE MILITANT ÉCOLOGISTE

L'arme numérique n'est pas l'apanage des organisations criminelles. Elle trouve de plus en plus sa place dans l'arsenal des entreprises commerciales réputées et dans certains ministères. Quand il s'agit de défendre leurs champions nationaux, nombre de gouvernements n'hésitent guère à mettre leurs agents de renseignement au service d'intérêts économiques. Rien de bien surprenant après tout, notamment dans le camp occidental où une élection se gagne – ou une majorité politique se maintient – grâce à un taux de chômage bas ou à une bonne conjoncture économique. « *À la base des stratégies de sécurité nationale, y compris dans le domaine technologique, industriel et commercial, il y a une vigoureuse politique publique de renseignement*, constate Éric Delbecque, auteur de *L'Intelligence économique pour les Nuls* (First, 2015). *Plus que jamais, il importe de savoir pour agir efficacement, adroitement et rapidement.* »

Les comités de direction misent sur les technologies pour dissiper ce que le stratège prussien Carl von Clausewitz appelait le « *brouillard de la guerre* ». Et sont prêts à tout pour accéder à l'information concernant les ressources, les objectifs et les contraintes de leurs adversaires et être en mesure de les vaincre. La Fair Trade Commission, l'autorité taïwanaises chargée de la concurrence, a ainsi condamné le célèbre fabricant d'électronique Samsung qui rémunérait des internautes pour critiquer abondamment sur le Net les produits de son concurrent HTC. En France, l'entreprise EDF a été condamnée en première instance en 2006 et relaxée en appel en 2013 pour espionnage informatique à l'encontre de l'association écologiste Greenpeace. Seuls des anciens cadres de l'électricien ont finalement été sanctionnés.

GUNTHER MENN/FOCUS/COSMOS

Pour se protéger des cyberattaques, les entreprises font appel à d'anciens agents des services de renseignement spécialistes des nouvelles armes de surveillance.

En 2011, c'est le géant français du nucléaire Areva qui doit admettre que son informatique a été pillée durant presque deux ans par des pirates encore non identifiés à ce jour. Au regard de la discrétion et de la durée particulièrement longue de l'attaque, cela exonère *a priori* les activistes antinucléaires qui revendiquent habituellement à coups de communiqués et de conférences de presse leurs intrusions dans les sites industriels. C'est donc la piste de l'espionnage étatique ou économique qui est clairement privilégiée. Évidemment, la détection de ces piratages est encore plus délicate lorsque l'appareillage d'État s'en mêle. Alors, seules des fuites involontaires permettent de pointer ces pratiques. Comme au printemps 2015, quand le magazine *Der Spiegel* révèle que le BND, les services allemands de renseignement, a prêté main-forte à l'agence d'écoute des États-Unis, la NSA, pour surveiller des entreprises européennes comme Eurocopter ou EADS. À l'instar des opérations d'écoute du téléphone mobile personnel de la chancelière Angela Merkel par cette même NSA, ces agissements ne peuvent être justifiés par l'argument de la lutte antiterroriste. C'est bien l'espionnage économique et la concurrence commerciale qui expliquent de telles pratiques entre alliés diplomatiques. « *La France a certainement perdu des contrats après les cyberattaques visant ses entreprises* », reconnaît Guillaume Poupard, le directeur général de l'Agence nationale de la sécurité des systèmes d'Information (ANSSI), dont la mission est de protéger notamment les opérateurs d'importance vitale (OIV). Cette appellation désigne les quelque 250 entités publiques et privées dont le dysfonctionnement perturberait de manière critique la collectivité France dans son ensemble.

L'attaque dont a été victime Sony Pictures en décembre 2014 témoigne de l'ampleur des informations qui peuvent être dérobées et rendues publiques. Lors de cette opération très médiatisée, ce furent des téraoctets de documents sensibles qui ont été exfiltrés : les données concernant les salaires de 6000 collaborateurs, des mails internes, des copies de films inédits... Soit tout ce qui constitue le cœur même de l'activité de cette société. Aucun recoin ne semble avoir échappé aux assaillants. Cette mise à sac aurait pu se dérouler sans que les dirigeants de la firme en soient informés. Comme lors de la plupart des campagnes de cyberespionnage.

> ***EN 2011, AREVA, LE GÉANT DU NUCLÉAIRE, ADMET QUE SON INFORMATIQUE A ÉTÉ PILLÉE DURANT PRESQUE DEUX ANS.***

L'ARMÉE CHINOISE PRISE LA MAIN DANS LE SAC

Malgré cette exposition accrue au risque numérique, le vol d'informations peine encore à trouver sa place dans les législations. Ainsi, ce n'est que depuis décembre 2015 que le parlement de Strasbourg a conclu un accord avec le Conseil européen pour préciser la notion de secret des affaires. Un dispositif qui devra être repris dans un projet de directive annoncé pour le mois d'avril 2016.

Pas de quoi forcément ralentir le phénomène du cyberpiratage. « *Il y a deux sortes de grandes entreprises aux États-Unis*, expliquait James Comey, directeur du FBI, en 2014 à la chaîne CBS. *Celles qui savent qu'elles ont été piratées par les Chinois et celles qui ne savent pas qu'elles ont été piratées par les Chinois.* » Une étape supplémentaire a été franchie en mai 2014 dans la prise en compte du phénomène : le département de la Justice américain inculpe officiellement cinq officiers de l'unité 61398 de l'armée chinoise soupçonnés d'avoir pénétré entre 2006 et 2014 dans les réseaux informatiques de sociétés américaines et d'avoir fait bénéficier les concurrents chinois de ces entreprises d'informations secrètes. Le communiqué de presse de Washington précise les nom, fonction et photographie de chacun des inculpés et désigne même les sociétés ciblées (Westinghouse Electric, U.S. Steel, Alcoa, Allegheny Technologies, SolarWorld...) et les peines encourues. Bien sûr, Pékin a protesté vigoureusement et n'envisage pas une seconde de demander à ses cinq officiers de coopérer avec la justice américaine. Plus que jamais, la politique reste la continuation de la guerre économique par d'autres moyens.