print

Préparatifs des États-Unis pour une guerre informatique contre la Chine

De Peter Sysmonds

Global Research, février 27, 2013

Url de l'article:
http://www.mondialisation.ca/preparatifs-des-etats-unis-pour-une-guerre-informatique-contre-la-chine/5324562

Le gouvernement Obama, travaillant main dans la main avec les médias américains, a ouvert un nouveau front dans sa campagne agressive contre la Chine. Une série d'articles, notamment dans le *New York Times*, est apparue au cours de la semaine passée pour soi-disant révéler l'implication de l'armée chinoise dans le piratage d'entreprises américaines et donner des indications sur la menace de guerre informatique qui existerait sur des infrastructures américaines vitales comme le réseau électrique.

L'article du *Times* de jeudi s'appuyait sur les affirmations non-prouvées et très biaisées en faveur des États-Unis d'un rapport préparé par la compagnie de sécurité informatique Mandiant qui prétend qu'une unité de l'armée chinoise installée à Shangaï serait responsable d'attaques informatiques sophistiquées aux États-Unis. Le reste des médias aux Etats-Unis et ailleurs a suivi, avec des articles fourmillants de commentaires d'analystes, de groupes de réflexion et de responsables publics qu'ils soient à la retraite ou toujours en fonction, au sujet de la « cyber-menace chinoise », en ignorant totalement les dénégations appuyées des ministères de la Défense et des Affaires étrangères chinois.

Cela a créé les conditions voulues pour la publication mercredi de la « Stratégie de l'administration sur l'atténuation des vols de secrets commerciaux américains » d'Obama, laquelle, sans nommer formellement la Chine, cite de nombreux exemples d'espionnage informatique pouvant lui être attribués. En des termes très généraux, ce document présente la réaction américaine, y compris la « pression diplomatique soutenue et coordonnée » contre les pays en infraction ainsi que la menace implicite de représailles économiques au moyen d'« outils de politique commerciale. »

Le procureur général américain Eric Holder a mis en garde contre « une menace significative et en croissance régulière contre l'économie américaine et les intérêts de la sécurité nationale. » Le vice-ministre de l'Intérieur Robert Hormats a déclaré que les États-Unis « s'inquiètent de plus en plus du vol de secrets commerciaux par tous les moyens au plus haut niveau de la part de responsables chinois haut placés. »

La diabolisation de la Chine comme menace informatique mondiale suit un mode opératoire bien établi : elle vise à créer un climat de peur et d'hystérie dans le public en préparation d'un nouvel acte d'agression – cette fois dans le domaine de la guerre informatique. Depuis sa prise de pouvoir en 2009, Obama a lancé une large offensive économique et stratégique visant à affaiblir et isoler la Chine et à renforcer la domination mondiale des États-Unis, en particulier en Asie.

Ces accusations de piratage informatique chinois viennent compléter la poussée économique du gouvernement Obama en Asie menée par l'intermédiaire de son Partenariat trans-pacifique (PTP), un nouvel accord commercial multilatéral visant à développer le commerce américain au détriment de la Chine. La protection des « droits de propriété intellectuelle » est un élément central du PTP, du fait que les

profits des grands groupes américains viennent pour beaucoup de leur monopole sur des marchés obtenus par les marques commerciales et la technologie. Les allégations d'espionnage informatique vont devenir le prétexte à de nouvelles mesures de guerre commerciale contre la Chine.

Cependant, l'aspect le plus sinistre de la propagande anti-chinoise est la préparation d'une guerre contre la Chine. Sous la bannière de son « pivot vers l'Asie », le gouvernement Obama a mis en marche une offensive diplomatique et stratégique de grande ampleur visant à renforcer les alliances militaires existantes avec le Japon, la Corée du Sud, l'Australie, les Philippines et la Thaïlande, à forger des partenariats stratégiques et des liens plus étroits, en particulier avec l'inde et le Vietnam, ainsi qu'à saper les bonnes relations existantes entre la Chine et des pays comme la Birmanie ou le Sri Lanka.

Ce « pivot vers l'Asie » d'Obama a déjà entraîné une escalade dangereuse des conflits maritimes en Mer de Chine du Sud, et en Mer de Chine orientale. Encouragés par les États-Unis, le Japon, les Philippines et le Vietnam ont ravivé leurs différends frontaliers avec la Chine. La concentration sur ces eaux stratégiques n'est pas accidentelle, c'est par elles que passent les lignes de navigation dont dépend la Chine pour importer des matières premières et de l'énergie du Moyen-Orient et d'Afrique. Les États-Unis sont en train d'établir de nouveaux accords pour des bases militaires en Australie, en Asie du Sud-Est, et ailleurs dans la région pour s'assurer qu'ils ont la capacité d'étrangler les lignes de ravitaillement vitales de la Chine en cas de confrontation ou de guerre.

Le Pentagone considère la guerre informatique comme un élément essentiel de l'énorme machine de guerre américaine et a consacré des ressources considérables à son développement, en particulier sous le gouvernement d'Obama. En mai 2010, le Pentagone a installé son nouveau centre de commandement informatique dirigé par le Général Keith Alexander, directeur de la NSA (*National Security Agency* – les services renseignements militaires), qui s'appuie sur les ressources informatiques déjà massives dont disposent la NSA et l'armée américaine.

Les accusations américaines d'espionnage informatique chinois sont complètement hypocrites. La NSA, entre autres agences, est engagée dans l'espionnage et le piratage informatiques des systèmes informatiques et des réseaux étrangers à une vaste échelle. Sans aucun doute, la Chine est déjà en haut de la liste de ses cibles. Le ministère des affaires étrangères chinois a affirmé cette semaine qu'au moins 14 millions d'ordinateurs en Chine ont été piratés par 73 000 utilisateurs basés à l'étranger cette année, dont de nombreuses attaques informatiques contre le ministère de la Défense chinois.

Les États-Unis ont déjà procédé à des actes agressifs illégaux de sabotage informatique contre les installations nucléaires iraniennes et leurs infrastructures. Avec Israël, ils ont infecté les contrôleurs électroniques des centrifugeuses à gaz utilisées dans l'usine d'enrichissement iranienne de Natanz avec le vers *Stuxnet*, en poussant des centaines d'entre elles à tourner trop vite et à s'autodétruire. Cette activité illégale a été utilisée aux côtés de formes plus traditionnelles d'attaques, tels l'assassinat de physiciens nucléaires iraniens et d'autres actes de sabotage de la part d'Israël.

Il est inconcevable que les capacités informatiques du Pentagone ne soient déployées qu'à des fins purement défensives face à la « menace chinoise ». En fait, quand il a pris ses fonctions de chef de la guerre informatique en 2010, le général Alexander a présenté son point de vue au sous-comité aux Forces armées de la Chambre des représentants. Après avoir déclaré que la Chine est considérée

comme responsable d'« un grand nombre d'attaques contre les infrastructures occidentales, » il a ajouté que si les États-Unis étaient soumis à une attaque organisée, « Je voudrais aller abattre la source de ces attaques. »

En août dernier, l'armée de l'air des États-Unis a publié ce que le *New York Times* a décrit comme « Un appel d'offre très clair à des articles la conseillant sur les "capacités d'attaque dans la guerre du cyberespace", comprenant des armes pour "détruire, refuser l'usage, tromper, corrompre ou usurper un réseau d'ordinateurs ennemis et d'autres cibles de haute technologie. Le même article faisait référence à la branche recherche du Pentagone, la DARPA (*Defence Advanced Research Projects Agency*), qui abrite un ensemble de contractants privés qui veulent participer au « Plan X », c'est-à-dire au développement de « technologies révolutionnaires pour comprendre, planifier et gérer la guerre informatique. »

La propagande de cette semaine sur la « cyber-menace chinoise » donne le prétexte pour développer les préparatifs déjà bien avancés des États-Unis et visant à mener des attaques informatiques contre des cibles militaires et civiles en Chine. Dans le contexte de tensions de plus en plus grandes entre les États-Unis et la Chine, provoquées par le « pivot en Asie » d'Obama, des actions américaines sans merci dans le domaine de la guerre informatique ne peuvent qu'accentuer le risque d'une confrontation militaire ouverte entre les deux puissances.

Peter Sysmonds

Article original, WSWS, paru le 23 février 2013