Extrait du El Correo

<http://elcorreo.eu.org/Comment-la-cryptographie-est-une-arme-essentielle-dans-la-lutte-contre-les-Etats-imperiaux>

Comment la cryptographie est une arme essentielle dans la lutte contre les Etats impériaux

- Empire et Résistance - Bataille pour l'information -

Date de mise en ligne : samedi 13 juillet 2013

Copyright © El Correo - Tous droits réservés

Le codage des messages, ou cryptographie, doit permettre aux petits Etats de se défendre contre les plus grands, assure le fondateur de WikiLeaks dans une tribune exceptionnelle. Car, de Pékin à Washington, le contrôle des communications est aujourd'hui une arme de guerre.

La plupart des premiers « cypherpunks » [groupes de personnes intéressées par la cryptographie, l'ensemble des techniques de codage et de décodage de messages] étaient des militants libertariens de Californie. Je n'étais pas issu de la même tradition, mais nous étions tous unis par notre volonté de protéger les libertés individuelles contre la tyrannie de l'Etat. La cryptographie était notre arme secrète.

Les gens ont oublié à quel point cet outil était subversif. A l'époque, la cryptographie était la propriété exclusive des Etats, qui s'en servaient pour conduire leurs guerres. En concevant notre propre logiciel et en le diffusant au maximum, nous avons libéré la cryptographie. Nous l'avons démocratisée et disséminée à travers les frontières du nouvel Internet.

La réaction des autorités et leurs diverses mesures contre ce « trafic d'armes » n'ont pas réussi à enrayer le mouvement. La cryptographie est devenue un standard des navigateurs Internet et d'autres logiciels que les gens utilisent aujourd'hui quotidiennement. La cryptographie est un instrument crucial de la lutte contre l'oppression de l'Etat. C'est le message de mon livre *Menaces sur nos libertés* (éd. Robert Laffont, mars 2013). La démocratisation de solides protocoles cryptographiques ne doit toutefois pas se limiter à cela. Notre avenir ne repose pas sur la seule liberté des individus.

Surveillance de masse

Le travail de WikiLeaks permet d'accéder à un niveau élevé de compréhension des relations entre l'ordre mondial et la logique des empires. Avec le développement de WikiLeaks, nous avons vu les preuves de la domination et du harcèlement exercés par de grandes puissances sur de petites nations, qui étaient infiltrées par des entreprises étrangères et forcées d'agir contre leurs intérêts. Nous avons vu la volonté populaire privée d'expression, les élections achetées et les richesses de pays comme le Kenya volées et vendues aux enchères aux ploutocrates de Londres et de New York.

Le combat pour l'autodétermination des pays latinoaméricains concerne bien plus que les seuls habitants de cette région, car il montre au reste du monde que la bataille n'est pas perdue. L'indépendance des démocraties d'Amérique Latine reste toutefois fragile. Les tentatives de déstabilisation se poursuivent, comme récemment au Honduras, en Haïti, en Equateur et au Venezuela.

C'est pour cette raison qu'il est tellement important de faire entendre le message des cypherpunks en Amérique Latine. La surveillance de masse n'est pas seulement un problème pour la démocratie et la bonne gouvernance des pays, c'est aussi une question de géopolitique. La surveillance de toute une population par une puissance étrangère constitue de fait une menace pour la souveraineté de ce pays. L'interventionnisme incessant dans les affaires des démocraties d'Amérique Latine nous a appris à être réalistes. Nous savons que les vieilles puissances n'arrêteront pas d'exploiter le moindre avantage pour retarder ou limiter l'indépendance de l'Amérique Latine.

Il suffit de regarder la situation du point de vue géographique. Tout le monde sait que les ressources pétrolières sont

Comment la cryptographie est une arme essentielle dans la lutte contre les Etats impériaux

le moteur de la géopolitique mondiale. Ce sont les flux de pétrole qui déterminent qui est en position dominante, qui doit être envahi et qui doit être mis au ban de la communauté internationale. Le contrôle physique d'un oléoduc, ne serait-ce que d'une portion, confère une vaste influence au plan géopolitique. Les gouvernements qui jouissent d'une telle position peuvent obtenir d'énormes concessions. D'un seul coup, le Kremlin peut condamner l'Allemagne et l'Europe de l'Est à passer l'hiver sans chauffage. La seule perspective de voir Téhéran maître d'un oléoduc le reliant à l'Inde et à la Chine sert aujourd'hui de prétexte à la logique belliqueuse de Washington.

Le codage des données, nerf de la guerre moderne

Mais la véritable guerre n'est pas celle pour les oléoducs ou les gazoducs ; la véritable guerre aujourd'hui est celle de l'information, c'est-à-dire celle pour le contrôle des câbles de fibre optique qui parcourent les terres et les océans. Pour mettre la main sur le nouveau magot mondial aujourd'hui, il faut contrôler les vastes flux de données qui transitent entre les continents et les civilisations et relie des milliards de gens et d'organisations. Tout le monde sait que, sur Internet ou par voie téléphonique, toutes les communications depuis ou à destination de l'Amérique Latine passent par les Etats-Unis.

Le réseau Internet gère 99 % du trafic vers ou en provenance de l'Amérique du Sud à l'aide de fibres optiques qui passent physiquement par les frontières des Etats-Unis. Le gouvernement US n'a pas eu le moindre scrupule à violer ses propres lois pour mettre ces lignes sur écoute et espionner ses propres citoyens. Or aucune loi n'interdit d'espionner d'autres pays. Chaque jour, des centaines de millions de messages en provenance d'Amérique Latine atterrissent entre les mains des services de renseignements US, qui les stockent *ad vitam aeternam* dans des entrepôts de la taille de véritables villes. La réalité géographique des infrastructures du réseau Internet a donc des conséquences pour l'indépendance et la souveraineté de l'Amérique Latine.

Le problème dépasse toutefois la question géographique. Bon nombre d'armées et de gouvernements latinoaméricains protègent leurs secrets à l'aide d'outils cryptographiques, autrement dit des logiciels et des boîtiers qui codent et décodent les messages au niveau de l'émetteur et du récepteur. Les gouvernements achètent ces outils - souvent chèrement payés par leurs peuples - pour garantir la confidentialité de leurs secrets car ils redoutent, à juste titre, l'interception de leurs communications.

Le problème est que les sociétés qui leur vendent ces coûteux équipements sont étroitement liées au milieu du renseignement US. Leurs PDG et leurs hauts responsables sont généralement des ingénieurs ou des mathématiciens issus de la NSA [Agence nationale de la sécurité, un organisme gouvernemental du ministère de la Défense des Etats-Unis], qui exploitent des inventions créées par leurs soins pour l'Etat-surveillant. Leurs produits comportent des failles délibérées servant un objectif précis. Quels que soient leurs utilisateurs ou la manière dont ils sont utilisés, les agents US sont toujours capables de décoder le signal et de lire les messages. Ces équipements sont vendus aux pays d'Amérique latine et à d'autres régions comme un moyen de protéger leurs secrets alors qu'ils sont en réalité un moyen de les leur voler.

Les Etats-Unis ne sont pas les seuls fautifs

Dans le même temps, les Etats-Unis ont lancé une course aux armements d'un nouveau genre. La découverte des virus « Stuxnet », puis « Duqu » et « Flame » annonce l'arrivée de logiciels ultrasophistiqués utilisés à des fins militaires par les grandes puissances contre des Etats plus faibles. De ce point de vue, l'agression US de l'Iran a pour but de saboter les efforts de Téhéran pour maintenir sa souveraineté nationale, une perspective qui va à l'encontre des intérêts israéliens et US dans la région.

Il fut un temps où l'utilisation de virus informatiques comme armes offensives relevait de la science-fiction. Il s'agit

Comment la cryptographie est une arme essentielle dans la lutte contre les Etats impériaux

aujourd'hui d'une réalité internationale qu'encouragent les provocations de l'administration Obama en violation du droit international. D'autres pays vont désormais suivre l'exemple américain et augmenter leurs capacités offensives pour combler leur retard.

Les Etats-Unis ne sont pas les seuls fautifs. Ces dernières années, la Chine a directement investi dans l'amélioration des infrastructures Internet de pays comme l'Ouganda. En Afrique, Pékin propose de généreux prêts en échange de contrats pour la construction d'infrastructures de base servant à relier les écoles, les ministères et diverses communautés au réseau mondial de fibre optique.

L'Afrique arrive sur le réseau, mais avec du matériel fourni par une superpuissance étrangère en devenir. Internet sera-t-il le nouveau joug de ce continent au XXIe siècle ? L'Afrique sera-t-elle de nouveau le théâtre de confrontations entre puissances mondiales ?

La liste est encore longue des raisons pour lesquelles le message des cypherpunks va bien au-delà de la lutte pour les libertés individuelles. Outre les droits et les libertés civiles des individus, la cryptographie peut également protéger l'indépendance et la souveraineté de nations entières, les liens de solidarité entre groupes unis par une cause commune et l'idée d'émancipation mondiale. Elle peut servir à combattre non seulement la tyrannie de l'Etat sur les individus, mais aussi la tyrannie des empires sur les nations plus faibles.

Les cypherpunks n'ont pas encore terminé leur grand oeuvre. Rejoignez-nous.

Julian Assange para *The Guardian*

Originale : « [How cryptography is a key weapon in the fight against empire states](#) »

[The Guardian](#). Londres, le 9 juillet 2013