mardi 29 octobre 2013

Résister. Par quels moyens ?

Le panopticon électronique : le « Réseau Échelon »

Remy Valat

Dans la « guerre hors limite », la ligne démarquant la surveillance des ennemis de l'État, potentiels ou jugés comme tels, et les citoyens lambda est ténue. Aux États-Unis, à partir de 1967, en pleine guerre du Vietnam, des pacifistes, des militants pour l'égalité des droits civiques (Martin Luther King et Malcom X) font l'objet d'écoutes systématiques (opération Minaret). Les actes de résistance au système Échelon sont isolés, désordonnés, limités à un groupe d'internautes militants et leur portée symbolique. A partir des années 1950, un mouvement de protestation pacifiste, proche du modèle français des militants ayant refusé l'installation du camp militaire du Larzac, marque son opposition à la présence de bases américaines, notamment sur le site de Menwith Hill.

Dans le contexte de la Guerre Froide et de la guerre du Vietnam, ces personnes rejettent principalement l'ingérence américaine. A partir de 1994, un groupe de militantes, dont le noyau a atteint l'âge mûr, multiplie les démonstrations non violentes (manifestations, enchaînement aux grilles du camp, etc.). La répression de ces mouvements par le gouvernement britannique est implacable, plus de 1700 interpellations , 183 condamnations, pour 27 acquittements entre 1988 et 1994 . Ces femmes, installées dans un camp de fortune appelé *Women Peace Camp*, n'hésitent pas à s'introduire dans la base pour y dérober des informations secrètes en fouillant les poubelles (des photocopies ou des impressions ratées de documents).

Ces renseignements ont mis à jour plus de 250 systèmes opérant à Menwith Hill, et plusieurs bases secrètes implantées sur le sol britannique. Ces actions, certes localisées, ont connu une forte mobilisation principalement en raison de la publication de l'article fondateur du journaliste écossais, Duncan Campbell, *Somebody's listening*, paru dans la revue *New Statesman*, le 12 août 1988. Les écrits de Campbell, seront suivis par l'ouvrage du néo-zélandais Nicky Hager (1996) et les publications d'un groupe de chercheurs de l'université George Washington qui ont extrait d'archives déclassifiées des

documents attestant les missions de surveillance électronique opérées à partir de la base de Sugar Grove en Virginie (1999).

D'autres actions revendicatives ont été initiées par des utilisateurs d'Internet. Un groupe de militants a lancé une « cyber-campagne de mobilisation » et proposé de saturer le réseau d'interception en adressant un grand nombre de courriels comportant les mots clés supposés être détectés par Ėchelon . Le 21 octobre 1999, le Jam Echelon Day est un échec qui met en évidence la solidité du système.

Des doutes subsistent sur les risques de manipulations de ces groupes, dont on ignore les sources réelles de financement. La prise de conscience sur les atteintes portées aux libertés publiques a débuté aux États-Unis sous l'influence de la National Security Archives et a impulsé le *Freedom Act* demandant l'ouverture des archives, dont on ignore les éventuels tri préliminaires qui auraient pu y être faits par le service versant. Les autorités américaines et australiennes jouent la transparence pour dissimuler au public l'existence d'un second réseau entre les membres de l'UK-USA, portant sur l'analyse et l'échange de renseignements traités. Par ailleurs, la redondance et le faible nombre des documents signifieraient que ceux-ci proviendraient d'une seule et unique source.

Confrontés à la collusion entre les entreprises de logiciel et les États, les citoyens n'auraient comme recours que la cryptographie indépendante. La cryptologie sécurise les messages en faisant perdre la valeur de l'information par la perte de temps consacrée au déchiffrement du message, car le « chiffre indéchiffrable » est une utopie. Au milieu des années 1970 (Whitfield Diffie, Martin Hellman et Ralph Merkle) ont imaginé de crypter l'information avec des fonctions mathématiques difficilement réversibles, puis l'apparition du chiffrement asymétrique (système RSA, pour Ron Rivest, Adi Shamir, Leonard Adleman, ses inventeurs) compliquait encore le décryptage.

Mais, à cette époque, ces procédés ingénieux n'inquiétaient aucunement le gouvernement américain qui jouissait du monopole d'un réseau Internet naissant. Cependant, au début des années 1990, Phil Zimmerman suggéra d'échanger des messages cryptés avec des chiffres symétriques d'un déchiffrement plus rapide et de transmettre la clé de chiffrement via le système de clés publiques.

Dans ce cas, l'émetteur crypte la clé de déchiffrement avec la clé publique du receveur et le receveur utilise sa clé privée pour décrypter la clé de déchiffrement et utilise ensuite un système de clé symétrique (IDEA) pour décrypter le message.

La superposition des deux systèmes de chiffrement offrait certainement une résistance aux moyens de décryptage de la NSA et lorsque Phil Zimmermann se mit a distribuer gratuitement son logiciel (PGP) sur Internet (1991), ses ennuis judiciaires ont commencé. Une enquête criminelle a été aussitôt

diligentée par le gouvernement pour transgression des règles d'export des logiciels de cryptographie. Les procès intentés contre lui ont conduit à l'impasse et le gouvernement fédéral a retiré sa plainte (1996).

Dans les mois et les années qui suivirent, Phil Zimmermann accumule les honneurs et créé une société pour diffuser commercialement son produit. Ce succès, et surtout l'aval donné par les autorités américaines à la dernière version de son logiciel laisse planer le doute d'une entente entre le concepteur et les agences fédérales, entente peut-être matérialisée par la présence d'une « porte dérobée ».

L' « affaire Zimmermann » témoigne de l'intérêt porté par les gouvernements sur la cryptographie, et surtout du rôle important qu'aurait à jouer la cryptographie indépendante et militante, au risque que cette innovation soit exploitée par le crime organisé, des réseaux terroristes, ou autres malfaisants !

Soulignons encore que le chiffrement à l'aide de clés publiques pose le problème de l'identification de l'émetteur, et par conséquent la mise en place d'une autorité d'authentification. Cette dernière mettrait les clés des utilisateurs sous séquestre et ne pourraient communiquer qu'aux autorités policières ou judiciaires. Les clés de chiffrement restent un dilemme.

En 2013, le réseau Ėchelon est toujours l'atout majeur du système de renseignement électronique nord-américain qui ne cesse de développer, et nous le savons grâce aux révélations de Edward J. Snowden, des moyens toujours supérieurs de collecte et de traitement d'informations fermées.

Précurseur dans ce domaine, Ėchelon a été imité par de nombreux pays développés dans le cadre de partenariats publics-privés, parfois transnationaux.

Cette prolifération est particulièrement inquiétante, parce qu'elle multiplie les acteurs du renseignement et du contrôle et, potentiellement, les risques d'atteintes à la vie privée. Mais, la définition extensible qui peut être faite de l'« ennemi de l'intérieur », du « terroriste », du « subversif », ou du « déviant » laissent en l'état de latence les velléités d'une dérive totalitaire au service de la politique impériale nord-américaine.
Restons vigilants !

Remy Valat

Le site d'information en langue française sur le réseau « Echelon On Line, Connaître le réseau Echelon » est logé à l'adresse

suivante : echelononline.free.fr

http://www.metamag.fr/metamag-1628++cs_TIR++Le-panopticon-electronique-le++cs_TIR++Res...
http://www.metamag.fr/metamag-1628--Le-panopticon-electronique-le--Reseau-%C4%96chelon-.html

http://www.legrandsoir.info/le-panopticon-electronique-le-reseau-echelon.html