L’affaire Snowden et la nouvelle géopolitique du cyberespionnage

written by Philippe Boulanger | 5 février 2014

L’environnement numérique devient plus complexe au point que les usagers ont peine à comprendre les récentes mutations technologiques qui touchent directement leur vie quotidienne. Lors de la révélation de l’affaire Snowden en juin 2013, l’opinion publique internationale découvre qu’un programme de cyberespionnage américain surveille, depuis 2007, les institutions de plusieurs Etats et certaines organisations internationales comme la vie privée de chacun d’entre nous. Cette affaire est révélatrice des nouveaux enjeux géopolitiques liés à l’accès aux données confidentielles sur le numérique et par la téléphonie mobile. Qu’en est-il véritablement de ce programme de cyberespionnage américain ?

La découverte du programme Prism et l’affaire Snodew en juin 2013

L’affaire Snowden est à l’origine de l’une des plus graves crises diplomatiques liées à l’espionnage depuis l’affaire Wikileaks en 2010. Edward Snowden est un agent de la CIA devenu, pendant quatre ans, administrateur système de la National Security Agency (NSA), l’une des plus puissantes agences fédérales de renseignement des Etats-Unis. A peine âgé de trente ans, il quitte précipitamment, le 20 mai 2013, son domicile à Hawaï pour se réfugier, dans un premier temps, à Hong Kong où une interview filmée et diffusée par le Guardian révèle les méthodes d’espionnage numérique menée par la NSA. Edward Snowden fait état de « *graves violations de la part du gouvernement des Etats-Unis d’Amérique de leur Constitution* ». Le journaliste du *Guardian*, Glenn Greenwald, qui est en contact avec lui, fait allusion à des informations susceptibles de provoquer « *en une minute plus de dommages qu’aucune autre personne n’a jamais pu le faire dans l’histoire des États-Unis* » (*Le Monde*, 14 juillet 2013).

En effet, par ses fonctions au cœur du système de la NSA, il aurait accédé à des données secrètes dont certaines seraient enregistrées sur une clé USB. Ces données seraient issues d’un vaste programme de surveillance et d’espionnage américain tenu secret. L’opinion publique internationale en découvre la teneur, les 6 et 7 juin 2013, par le *Guardian* et le *Washington Post* qui font allusion à une fuite de la NSA. Deux jours plus tard, Snowden est identifié comme la source de ces fuites. Il devient la nouvelle figure emblématique des défenseurs des libertés individuelles sur le numérique à l’instar du fondateur de Wikileaks Julian Assange et du sergent Bradley Manning, dont le procès a lieu au même moment et qui encourt la prison à perpétuité pour la

divulgation d'informations confidentielles. Accusé de vol et d'espionnage par la justice américaine le 22 juin, Snowden est traqué par les services américains. Il fuit Hong Kong pour Cuba en prenant, le 23 juin, un avion de l'Aeroflot qui doit d'abord faire escale à Moscou. Se sachant suivi non seulement par les autorités américaines qui demandent son extradition, mais aussi par les journalistes de la presse internationale, il se réfugie dans la zone internationale de l'aéroport de Cheremetievo. Privé de passeport, il demande alors l'asile politique à l'Equateur, qui avait déjà accueilli Julian Assange, au Venezuela, à la Bolivie, puis au Nicaragua. Il l'obtient finalement auprès de la Russie, le 1er août, après d'âpres négociations entre la NSA et le FSB (service de renseignement russe) et plus d'un mois passé dans la zone internationale de l'aéroport.

Le renseignement d'origine électromagnétique au cœur d'une crise diplomatique internationale : les nouveaux enjeux géopolitiques du cyberespionnage

L'impact de l'affaire Snowden crée une onde de choc planétaire. Celle-ci est révélatrice des nouvelles rivalités internationales dont l'un des enjeux est l'accès, la conservation et la transmission des données numériques. La connaissance par l'image satellite avait été au cœur des grandes affaires de renseignement au cours de la guerre froide. Ce sont désormais les données collectées par les médias numériques qui suscitent les convoitises des services de renseignement, notamment américains. Outre la dimension rocambolesque de la traque de Snowden jusqu'à début août, cette affaire révèle l'existence d'un programme ultra-secret de renseignement d'origine électromagnétique (ROEM en français) nommé Prism.

Le programme Prism est un moteur de recherche très puissant qui permet d'intercepter les paquets de données à travers les réseaux de câbles sous-marins. Mis en œuvre depuis 2007 par la NSA, en collaboration avec d'autres Etats comme l'Angleterre, l'Australie, et le Canada, il sélectionne les données en temps réel transitant dans le monde entier. Selon le *Washington Post*, plus de 117 000 « cibles » sont concernées, par exemple, par le programme pour la seule journée du 5 avril 2013. Prism ne constitue toutefois qu'un élément d'un ensemble de programmes de cyberespionnage. Il s'intéresse à des suspects déjà identifiés, comme des terroristes, qui pourraient mettre en cause la sécurité nationale. Un autre système d'analyse des données brutes, connu sous le nom de XKeyscore, englobe un spectre plus large. Il permet de tout connaître des internautes comme les pages internet qu'ils ont consultées et leurs centres d'intérêt. Les données sont conservées pendant quelques jours, puis stockées ou supprimées en fonction de la nature du renseignement recherché par les analystes de la NSA. Selon les Etats et les méthodes employées, un ensemble de programmes de cyberespionnage est révélé à partir d'août par *The Guardian*. Pendant des années, la NSA et le FBI ont

recueilli des informations en accédant directement au serveur d'une cible, une entreprise par exemple, et auprès des utilisateurs de l'opérateur téléphonique Vérizon, d'AOL, Apple, Facebook, Google, YouTube, Microsoft, Skype, Paltalk et Yahoo. Ceux-ci démentent catégoriquement, sans toutefois nier leur relation avec la NSA lorsque celle-ci demande des renseignements ou un accès avec un mandat. Par exemple, Facebook reconnaît avoir répondu à 10 000 requêtes des autorités américaines durant le premier semestre 2013, tout en assurant protéger les données de ses utilisateurs. Se pose, dès lors, un autre enjeu d'ordre juridique sur le droit à la liberté numérique et sur la politique de confidentialité des données appartenant aux millions d'internautes. En outre, d'autres révélations précisent que ces méthodes concernent des entreprises étrangères. Deux opérateurs indiens, Tata Communications et Reliance Communications, ont accepté, respectivement en 2005 et 2007, de transmettre aux autorités américaines des données sur leurs clients vivant sur le sol américain, non seulement pour procéder à l'espionnage de suspects, mais aussi pour protéger ces données des puissances étrangères.

Pour un certain nombre d'organisations, comme Anonymous, ce programme dépasse le cadre juridique autorisé. En juin, devant des cours fédérales, des groupes d'abonnés à Verizon portent plainte pour contester la légalité des autorisations d'écoute données aux services secrets. Ils seront suivis par les adhérents de l'association américaine de défense des libertés publiques Electronic Privacy Information Center, qui portent plainte le 8 juillet, devant la Cour suprême. Pour la première fois, un recours de ce genre est déposé devant la plus haute juridiction américaine.

Pour les autorités américaines, ces opérations de cyberespionnage se justifieraient dans le cadre de la lutte contre le terrorisme international depuis les attentats de New York de 2001. Prism serait un programme de « *collecte autorisée statutairement d'informations des renseignements étrangers* » à l'encontre d'individus vivant en dehors des Etats-Unis, par la section 702 du *Foreign Intelligence Surveillance Act*, adopté en 1978 pour encadrer l'espionnage des communications privées, mais étendu par la section 215 du *Patriot Act* du 26 octobre 2001. Mis à jour en 2007, 2008 et 2012, celui-ci permet la collecte et la surveillance des communications sans mandat ou ordonnance judiciaire, surpervisées par un tribunal spécial, des citoyens américains en lien avec des étrangers soupçonnés de terrorisme ou d'espionnage. Grâce à cette autorisation, l'ensemble des programmes de surveillance américain aurait ainsi permis de déjouer une cinquantaine de tentatives d'attentat, dont au moins dix sur le sol américain, dans une vingtaine de pays. « *Ces programmes sont extrêmement précieux pour protéger notre nation et assurer la sécurité de nos alliés* » déclare, le 18 juin, le général Keith Alexander, responsable de la NSA, devant la commission du renseignement de la Chambre des représentants. Il n'en demeure pas moins

que l'affaire Snowden se révèle comme l'un de ses pires cauchemars durant l'été 2013. Non seulement des informations secrètes peuvent être rendues publiques, mais les organisations terroristes ont désormais connaissance des méthodes employées pour les surveiller. A ces difficultés s'ajoutent encore celles qui touchent directement les relations des Etats-Unis avec certains Etats.

L'annonce publique de ce programme provoque une double crise diplomatique. Tout d'abord, la décision de la Russie de régulariser la situation de Snowden, en lui accordant l'asile temporaire (pour un an, reconductible un an) le 1er août, soulève de vives réactions des élus républicains et démocrates aux Etats-Unis. Cette décision russe, donnée sans préavis vis-à-vis de ceux-ci, mettait en danger la reprise des relations entre Obama et Poutine en amont du sommet du G20 à Saint-Pétersbourg en septembre 2013. Les sujets de tension sont ravivés, comme la question syrienne, celle du nucléaire iranien et celle du projet de bouclier antimissile américain en Europe de l'Est. Ensuite, l'annonce d'un vaste programme d'espionnage déclenche une crise diplomatique mondiale, en juin-juillet 2013, entre les Etats-Unis et plusieurs pays. La France, l'Argentine, le Brésil ou l'Italie ont ainsi appris l'espionnage par leur allié de leurs agents d'ambassade ou de leurs entreprises. Le 1er juillet, le président français François Hollande demande que « *cessent immédiatement* » les écoutes des pays européens. Son appel, qui est d'ailleurs la seule manifestation émise par les Européens, provoque de vives réactions parmi ses alliés anglo-saxons, qui critiquent à leur tour les pratiques de l'espionnage français.

Les méthodes de collecte de l'information sont au cœur de la crise internationale qui éclate à la fin juin 2013. Tout d'abord, la France, l'Italie, l'Espagne et le Portugal interdisent le survol de leur territoire à l'avion du président bolivien Evo Morales, à la fin juin, considérant que Snowden pouvait être à bord. Humilié par les Européens, celui-ci est accueilli en héros à Montevideo. Par la suite, toute une série d'annonces sur le cyberespionnage américain commence à susciter un malaise dans les relations diplomatiques internationales. Début juillet, à la suite d'informations diffusées par le journal brésilien *El Globo*, les autorités brésiliennes apprennent que des opérations d'espionnage auraient été menées à partir de Brasilia. En septembre, un document de la NSA, diffusé à la télévision brésilienne TV Globo, attesterait de l'espionnage de messages internet et téléphoniques de la présidente brésilienne Dilma Rousseff et du président mexicain Enrique Pena Nieto, à partir d'infrastructures d'écoute installées dans les ambassades américaines de ces deux pays.

Sous la présidence du Venezuela, l'organisation Mercosur adopte immédiatement une résolution sur la sécurité contre l'espionnage. Elle rappelle ses ambassadeurs (brésilien, argentin, uruguayen et vénézuélien) dans les quatre pays européens cités et fait face aux

pressions des Etats-Unis qui demandent de ne pas accorder le droit d'asile à Snowden. Par ailleurs, dans le contexte de négociation d'un accord de libre-échange entre Européens et Américains, différents quotidiens européens annoncent que les bureaux de les ambassades de France, de Grèce, l'Union européenne et 38 cibles, telles que les ambassades de France, de Grèce, d'Espagne et d'Italie à Washington, les représentants de l'Union européenne aux Nations unies et le Conseil européen à Bruxelles, sont soumis à des opérations de cyberespionnage. D'après *The Guardian*, des opérations portant des noms de code de tribus indiennes d'Amérique visaient à espionner directement la représentation française aux Nations unies (opération *Blackfoot*) ainsi que l'ambassade de France à Washington (opération *Wabash*). Selon *Der Spiegel*, des micros étaient installés dans les bureaux des institutions européennes tandis que les courriers électroniques étaient analysés. Les communications téléphoniques sont également quotidiennement interceptées par la NSA, de l'ordre de deux millions pour la France et de 15 millions pour l'Allemagne qui serait le pays plus surveillé.

L'affaire Snowden en juin 2013 devient le scandale Snowden le mois suivant. Des pratiques d'espionnage inédites sont révélées au grand jour, provoquant une crise diplomatique planétaire comme une crise de confiance de l'opinion américaine. Le président Obama annonce, dès août 2013, une réforme du *Patriot Act* pour regagner cette confiance, tandis que Keith Alexander, directeur de la NSA, échaudé par la désertion de Snowden, prévoit de supprimer 90 % des 1 000 postes d'analystes, ceux-ci étant remplacés par des programmes informatiques. Sur le plan international, ces pratiques dévoilent surtout une nouvelle géopolitique du cyberespionnage qui ne concerne pas seulement la NSA, mais bien toutes les grandes puissances mondiales.

Au moins cinq grandes puissances disposent de telles capacités d'espionnage électromagnétique dans le monde. Le programme Prism n'est qu'une partie visible des moyens déjà mis en pratique depuis la fin des années 1940.

Plus de 60 ans d'espionnage électromagnétique

Si l'opinion publique (re)découvre ainsi la possibilité d'être espionnée par la NSA, il y a tout lieu de penser que les services de renseignement de plusieurs Etats étaient déjà informés de ses pratiques. Toutes les grandes puissances mondiales et régionales (Etats-Unis, Russie, Chine, Angleterre, France, Israël) disposent vraisemblablement de systèmes d'interception des données électromagnétiques bien qu'il soit toujours difficile de confirmer ou pas telle donnée. Chacun de ces Etats connaît ou suppose l'existence de programmes de renseignement d'origine électromagnétique (ROEM ou Sigint, *Signal Intelligence*, à la NSA), développés par une autre puissance, voire participe à des échanges de renseignements. Le programme Prism apparaît être une partie d'un

ensemble de programmes menés par ces puissances depuis plus de 60 ans.

Aux Etats-Unis, le système Echelon est l'un des premiers maillons d'une grille planétaire de contrôle des communications et de l'information. Mis en place en 1947, ce système s'inscrit dans le cadre d'une alliance sous l'égide des Etats-Unis avec le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande. Le traité Ukusa (United Kingdom-United States Communication Intelligence Agreement) réunit les alliés anglo-saxons qui partagent la défense des mêmes valeurs libérales face au monde communiste. Ce réseau est complété d'accords de coopération avec le Danemark, la Norvège, la Turquie et l'Allemagne. Il consiste tout d'abord en un partage de l'information entre les différents services secrets et les agences de renseignement dont la plus importante est la National Security Agency aux Etats-Unis.

Grâce à un réseau de 120 satellites militaires et bases d'écoute réparties dans les pays membres, le système Echelon forme un système global de communications privées et publiques qui vise à intercepter les écoutes téléphoniques, les émissions radio haute fréquence, les ondes ultracourtes du trafic hertzien au sol, les câbles sous-marins en cuivre de télécommunications, les télécopies, les courriels par internet. Des millions de messages sont ainsi traités à l'échelle planétaire afin de détecter, à partir de mots clés, les informations recherchées. Le quartier général de la National Security Agency, à Fort George Meade, dans le Maryland, depuis novembre 1952, réunit les infrastructures d'analyse nécessaires à ces interceptions ainsi qu'aux cryptages, en toute clandestinité, afin d'éviter un nouveau Pearl Harbor. Ces mêmes infrastructures bénéficient d'améliorations constantes depuis leur création. Fin 2013 s'ouvre le plus grand centre d'écoute planétaire à Bluffdale dans l'Utah pour sur- veiller l'information numérisée (tickets de parking, achats sur internet, etc.) transmise dans le monde. L'ensemble s'étend sur 9 hectares de bâtiments remplis de serveurs pour analyser 1 yottabit de données simultanément (soit mille millions de milliards de livres de 500 pages).

Le réseau Echelon présente une vocation de renseignement militaire. Mais il évolue à des fins de renseignement économique et devient stratégique avec la mondialisation des échanges et la concurrence économique entre les grands groupes mondiaux. Le programme P-415, conçu en 1984, prévoit l'interception des satellites pour les communications civiles des pays en développement (Inde, Indonésie) et les communications diplomatiques du Japon, du Pakistan et de la Corée du Nord. Révélé au grand public par les médias depuis la fin des années 1980, le système Echelon n'a pas d'existence officielle et continue de servir les Etats-Unis à des fins économiques, politiques et militaires dans le monde entier.

D'autres systèmes de collecte d'informations dans le cyberespace semblent être en fonction. Le système britannique serait étroitement

associé à celui des Etats-Unis. En France, le système Frenchelon s'appuie sur un dispositif d'une vingtaine de stations d'écoute réparties en France et dans une partie importante de sa zone d'influence (Antilles, Guyane, Centrafrique, Mayotte, Réunion, Djibouti, Nouvelle-Calédonie), pour intercepter des données électromagnétiques (communications téléphoniques, sms, *e-mails*, fax). Ces données sont stockées par la Direction générale de la sécurité extérieure, et accessibles aux différentes directions de défense et de sécurité nationale.

Les pays émergents disposent également de leurs propres systèmes de cyberespionnage des individus et des institutions étrangères, bien que peu de données soient communiquées sur ce sujet. Le système chinois, qui vise ainsi à étendre l'influence chinoise dans le monde, aurait une vocation planétaire avec des infrastructures implantées en Asie du Sud-Est. Un réseau de stations d'écoute électronique est en fonction à Hainan, aux îles Paracel, au Laos et en Birmanie. Le réseau russe est considéré comme le deuxième plus grand réseau d'écoute mondial. Héritier du plus grand système de renseignement électromagnétique comportant 500 stations de captation et employant 350 000 personnes à la fin de la guerre froide, il est actuellement dirigé par le Service des communications spéciales et d'in- formation (*Spetssvyaz*). Il comprendrait des stations d'écoute à Cuba (Lourdes), Vietnam (Cam Ranh), en Inde, Afghanistan, Yémen et Nicaragua. Chaque réseau renforce les capacités de cyberespionage en appui des systèmes électroniques mis en place durant la guerre froide. Ils sont un des facteurs de puissance d'un Etat. Chacun est généralement complété d'une politique active en matière de cyberactivités étatiques. Au début des années 2010, les Etats développant une capacité informatique avancée, très offensive, sont les Etats-Unis, la Russie, la Chine, Israël, suivis de l'Iran, l'Inde, le Pakistan, la Grèce et la Corée du Nord.

En somme, l'annonce du programme Prism par Edward Snowden ne constitue en rien une révélation d'exception. Voici plus de 60 ans que les grandes puissances, principalement les Etats-Unis, la Chine, la France, l'Angleterre, Israël, ainsi que l'Allemagne et l'Inde, utilisent leur système de ROEM afin de défendre leurs intérêts militaires ou économiques. L'affaire Snowden est ainsi à replacer dans cette géopolitique de l'information et de la communication et dans les rivalités de pouvoir entre grandes puissances dans le champ électromagnétique.