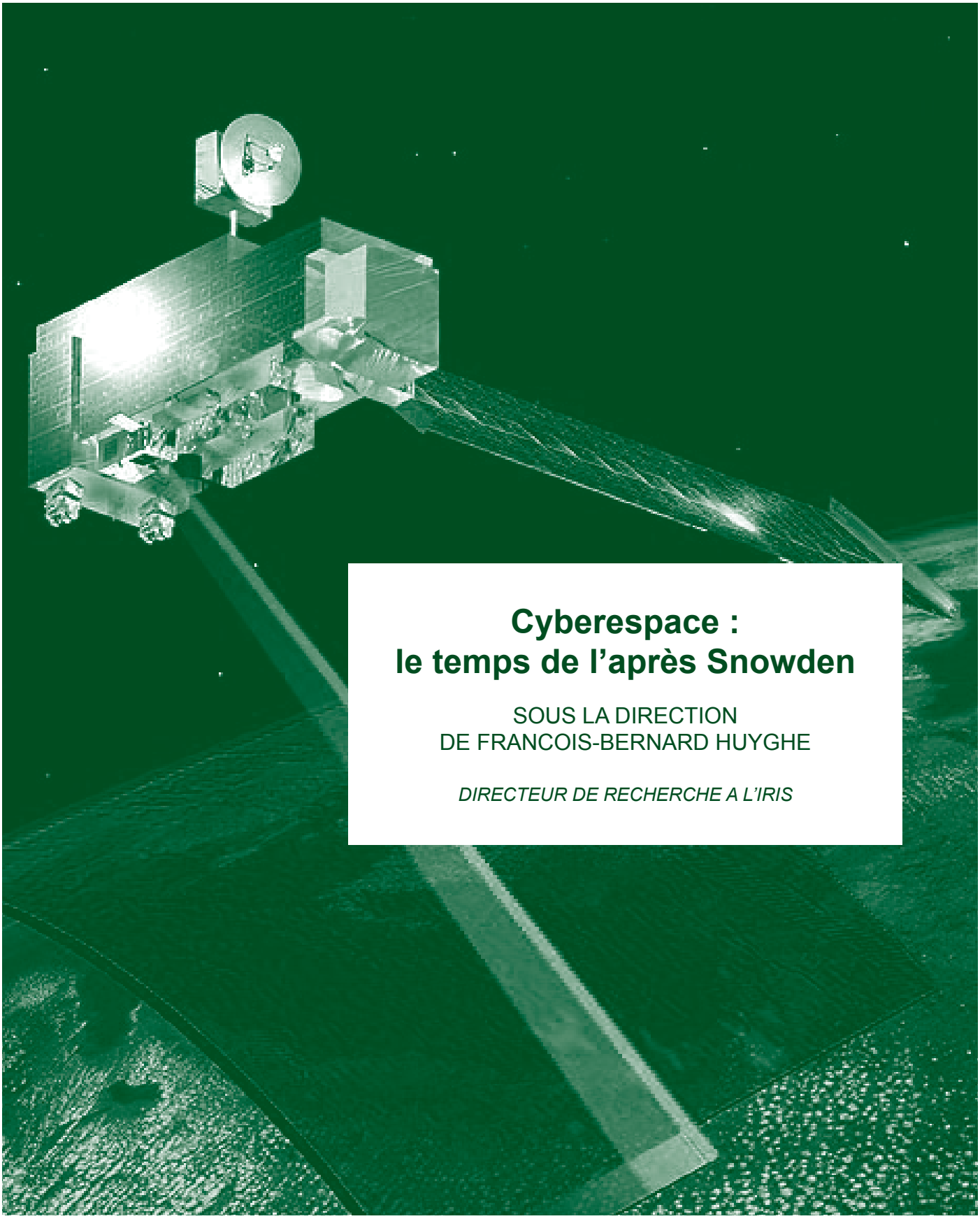
IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

OBSERVATOIRE GEOSTRATEGIQUE
DE L'INFORMATION

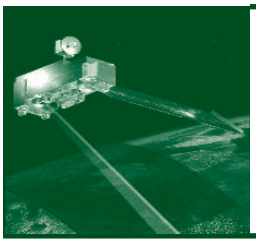
Mars 2014



Cyberespace : le temps de l'après Snowden

SOUS LA DIRECTION
DE FRANCOIS-BERNARD HUYGHE

DIRECTEUR DE RECHERCHE A L'IRIS



OBSERVATOIRE GEOSTRATEGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATEGIQUES

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

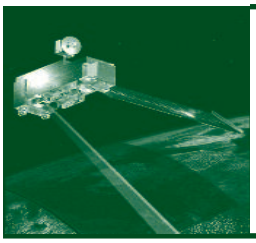
Et maintenant que nous savons

Depuis qu'Edward Snowden a révélé l'importance des interceptions mises en place par la NSA, les signes se multiplient quotidiennement des conséquences de ces révélations. Un jour on apprend qu'un « câble va relier le Brésil et l'Europe pour contourner l'espionnage américain », le lendemain, on commente les prédictions du gourou de la cybersécurité Bruce Schneier : les relations entre NSA et opérateurs privés « partent en quenouille ». Dans le même temps, un sondage montre que 57 % des Français estiment justifiée une surveillance des échanges sur la toile, tandis que certains gouvernements espionnés ne font pas de reproches trop agressifs à l'administration Obama. Alors ? Plus rien ne sera comme avant ? Ou : on savait bien et rien de nouveau ?

Pour sortir des simplifications, nous avons demandé à des experts de traiter chacun un aspect de l'affaire Snowden dont on voit bien qu'elle comporte des dimensions techniques, économiques, géopolitiques, idéologiques, etc. Florence Hartmann s'est penchée sur le phénomène, pas si récent, du « Whistelblowing », Robert Damien pointe l'idéologie fondatrice américaine qui explique le comportement de Snowden. Olivier Kempf montre ensuite que cette affaire est révélatrice des positions stratégiques des États. Nicolas Mazzucchi s'intéresse à la dimension « espionnage économique ». Loïc Damilavile revient sur les changements possibles dans la gouvernance d'Internet, Nicolas Arpagian sur la réaction de l'Europe, tandis que Jérémie ZImmermann explique ce que pourraient faire les citoyens pour échapper à la surveillance.

Nous nous efforcerons de conclure sur les nouveaux rapports entre secret, hostilité et confiance. Enfin, comme la force et la vulnérabilité à la fois du système NSA résident dans son hallucinante complexité, nous indiquerons au lecteur les rares sources qui permettent de s'orienter dans le labyrinthe de la surveillance sans limite. ■

François-Bernard Huyghe



OBSERVATOIRE GEOSTRATEGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATEGIQUES

Lanceurs d'alerte : un mal nécessaire ?

Entretien avec Florence Hartmann
Ancien Grand reporter du Monde
***Auteur de* Lanceurs d'alerte, les mauvaises consciences de nos démocraties,**
Ed. Don Quichotte, 2014

IRIS : Dans votre livre, vous revenez sur le phénomène du whistleblowing, ou plus précisément, des lanceurs d'alerte. Ce phénomène semble très en vogue ces dernières années, mais est-il pour autant un concept récent ?

Florence Hartmann : Le concept est peut-être récent mais la démarche, elle, existe depuis fort longtemps. Les sociologues comme Francis Chateauraynaud et Didier Torny ont eu le besoin de nommer dans les années 1990 autrement un phénomène ancien : celui d'informateur public ponctuel. Au regard de l'Histoire, il y a toujours eu des « lanceurs d'alerte ». On ne les appelait simplement pas ainsi. Certains évoquent Martin Luther (1483-1546) qui a dénoncé les abus économiques de l'Eglise au XVI^{e} siècle. Je pense aussi à Jan Krasky (1914-2000), résistant polonais qui avait alerté les Alliés de l'extermination des Juifs en Pologne par les Nazis en leur remettant dès 1943 des microfilms. Ils étaient à leur manière des lanceurs d'alerte. A leur époque, on préférait cependant parler d'« informateur ». Or, ce terme générique peut recouvrir plusieurs significations. La création de la notion de « lanceur d'alerte » vise surtout à clarifier une situation jusque-là ambigüe. Les sociologues ont voulu séparer les termes d'informateur, de dénonciateur et de délateur. Chacune renvoyant vers une démarche dont la finalité est sensiblement différente. Le lanceur d'alerte, lui, s'inscrit dans une démarche éthique, souvent de contre-pouvoir. Il souhaite informer ses concitoyens d'une transgression de la légalité de la part d'une autorité ou d'une entreprise.

IRIS : En se désolidarisant du groupe, les lanceurs d'alerte ne se mettent-ils pas automatiquement en opposition avec ce groupe ?

Florence Hartmann : Les lanceurs d'alerte ne sont pas forcement dans une dimension d'opposition au groupe. Ils ne sont pas « antisystème », mais « antidérive d'un système ». Un lanceur d'alerte ne se positionne pas comme un révolutionnaire ou un dissident, mais comme un citoyen qui a fait partie d'une structure et qui estime que cette structure a, à un moment donné, outrepassé ses prérogatives. Ils ne veulent pas que le système s'effondre mais que ce dernier soit plus en accord avec lui-même. Pour reprendre le cas de Snowden, il ne remet pas en cause le fait que la NSA fasse du renseignement, mais que les interceptions faites par la NSA soient généralisées et donc illégales et que le secret serve à occulter cette illégalité. Le lanceur d'alerte fait parti intégrante du système.

Le lanceur d'alerte, avant de se désolidariser du groupe, était le plus souvent d'une très grande loyauté envers son employeur. Et c'est parce qu'il y a dérive qu'il se désolidarise mais seulement des contrevenants pour se solidariser avec la société qui, directement ou indirectement, subie les préjudices des dérives mises au jour. Pour illustrer ces propos, nous pouvons citer l'histoire de Daniel Ellsberg ou encore celle de Mordechai Vanunu, qui tous deux travaillaient sur des projets sensibles dans le domaine de la défense – américaine pour le premier, israélienne pour le second. Ils n'ont jamais mis sur la place publique des informations confiden-

■■■ tielles jusqu'au jour où ils ont constaté une grave dérive du système qui avait besoin du secret pour se perpétuer et que seule la lumière pouvait interrompre. En cela, les lanceurs d'alerte font office de contre-pouvoirs, mais uniquement lorsque tous les autres recours ont échoué. C'est une méprise courante de croire que les lanceurs d'alerte sont des dictateurs de la transparence. La plupart du temps, ils alertent d'abord en interne, ils saisissent leur hiérarchie, ou comme Ellsberg, le Congrès américain, mais face à l'inertie ou au refus de rétablir la légalité, ils prennent à témoin l'opinion publique dans l'espoir de faire cesser le danger dénoncé.

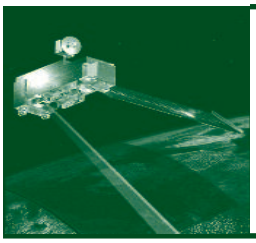
IRIS : Si la transparence est la règle en démocratie, comment justifier la notion de confidentialité dans ce système politique ?

Florence Hartmann : Démocratie et confidentialité ne s'excluent nullement. Ce sont les fondements mêmes de la démocratie : la transparence est la règle pour assurer le contrôle démocratique des trois pouvoirs notamment et garantir l'État de droit. Le secret est, en revanche, l'exception parce qu'il y a d'autres libertés à protéger concomitamment ; celle d'avoir une vie privée par exemple et celle de notre sécurité. S'agissant d'une exception, le secret ou la confidentialité est défini par la loi. C'est l'une des spécificités intrinsèques des démocraties. Si le secret sort du cadre de ce qui est prévu par les lois, alors on s'éloigne d'un système démocratique et donc de l'État de droit. Les domaines où le secret/la confidentialité est, dans une certaine mesure, autorisé par la loi est la défense, la diplomatie, l'innovation industrielle, l'instruction judicaire. Le seul domaine où le secret est très peu limité est la vie privée. Dans les autres domaines, il n'y a pas de place à l'arbitraire. Ne peuvent être classifiées que les informations qui rentrent dans le cadre des lois existantes et restrictives. Hélas, on l'oublie trop souvent. Pourtant, c'est le seul moyen démocratique de pouvoir empêcher que la confidentialité serve d'instrument pour cacher des abus, des pratiques illégales, voire des crimes. Les lanceurs d'alerte ne prônent pas la fin de toute confidentialité. Il dénonce simplement les abus du système.

IRIS : Verra-t-on dans un futur proche des lanceurs d'alerte partout ? Par exemple dans les entreprises ou en politique ?

Florence Hartmann : La réponse est non ! Lancer une alerte n'est pas un phénomène de mode mais une réponse concrète à une dérive ponctuelle. Si l'on veut qu'il y en ait moins, il est nécessaire de régler les problèmes existants. Cela ne sert à rien de lancer une chasse aux sorcières. Pour en revenir à l'affaire Snowden, il est nécessaire que nos démocraties respectent leur législation, leur constitution et les normes de droit international, notamment dans le domaine du renseignement. Il ne s'agit pas d'empêcher l'action, de brider le politique, seulement de garder à l'esprit les sages conseils de Montesquieu. ■

*
* * *
*



OBSERVATOIRE GEOSTRATEGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATEGIQUES

Edward Snowden, un pur produit américain ?

Entretien avec Robert Damien
Professeur émérite de philosophie politique et d'éthique de l'Université de Paris-Ouest
Auteur d'*Éloge de l'autorité : généalogie d'une (dé)raison politique*, Ed. Armand Colin, 2013

IRIS : Il n'y a pas si longtemps, Internet signifiait pour la plupart un espace sans contrôle. Pourtant, été 2013, l'affaire Snowden éclate. Nous aurait-on caché des informations ?

Robert Damien : Cette affaire, aussi surprenante et malsaine soit-elle, nous fait revenir aux origines de l'Internet. La version actuelle du Web est un dérivé d'un programme de communication militaire américain conçu par des agents plutôt libertaires aux heures sombres de la Guerre froide. Dans son essence même, il y a ainsi la notion d'Etat et de contrôle. Dans le même temps existe une certaine revendication de liberté créatrice et d'autonomie disponible. L'ouverture vers le monde civil et la multiplication du nombre d'internautes ces dernières années nous ont un instant laissé croire que cet espace serait à tous et pour tous, direct et immédiat sans institution ni frontière, sans interdit ni surveillance. L'affaire Snowden nous fait redécouvrir une évidence : Internet reste l'instrument d'une puissance étatique dont les Etats-Unis sont à la fois les créateurs et pour le moment, le leader. En tant que tel, Internet devient l'instrument de l'hégémonie d'une souveraineté politique.

IRIS : Dans votre dernier livre, vous faites l'éloge de l'autorité – du moins, lorsque celle-ci est démocratique –, mais que devient cette autorité lorsqu'elle outrepasse ses prérogatives ?

Robert Damien : Cette autorité est tout simplement remise en cause. La confiance jusque-là accordée s'est effritée. Elle n'est plus là. Il est donc nécessaire que le système soit revu, et corrigé, afin de s'adapter aux nouvelles contraintes. L'autorité démocratique possède en son essence une légitimité : celle de prendre des décisions au nom du groupe représenté. L'électeur délègue, autorise un autre à décider pour lui. Ce pouvoir transmis à l'élu n'est pas illimité. Ce dernier doit à un moment ou un autre rendre des comptes. En démocratie, il n'y a pas de chef sans mandant. Ce système pyramidal – des électeurs, des élus – trouve cependant ses limites lorsque cette autorité se retrouve confrontée à un impératif de survie. Dans ce cas, l'autorité peut être amenée à prendre des décisions déontologiquement discutables et à outrepasser temporairement ses prérogatives au nom de la survie de la communauté. Pour un Etat, nous parlerons de « raison d'Etat ». Dans ce schéma, seul le groupe a de l'importance. Il prime sur l'individu. Toute la problématique est de définir correctement les menaces qui viennent mettre en péril la communauté. Avec l'affaire Snowden, nous sommes passés d'une surveillance antiterroriste à une surveillance économique, politique et militaire. Les décisions du chef jusque là respectées, sinon tolérées, sont remises en cause.

IRIS : Justement, quelles sont les qualités qui font d'un chef, « un bon chef » ?

Robert Damien : Pour qu'un chef soit un « bon chef », trois éléments sont nécessaires. Tout d'abord, un chef est celui qui sait en raison d'une intelligence instruite des données éclairantes. Il les sélectionne et les ordonne sans dogmatisme mais avec une compé- ■■■

■■■ -tence avérée de gestionnaire. Il est ensuite celui qui possède un discernement judicieux dans l'anxiété d'une situation contingente et aléatoire. Il a cette capacité à trancher correctement dans l'incertitude de l'action et en affrontant les dissonances d'une situation toujours chargée d'impondérables. Enfin, il est celui qui assume les conséquences de ses actes ou décisions en les menant à bon port malgré les effets pervers imprévus.

Le chef commence en prenant la tête puis continue et poursuit mais surtout il achève. Il va au bout de son choix et mène à bonne fin en gouvernant selon un cap. Quand tous ces points sont réunis, et c'est rare et difficile car beaucoup sont souvent incompétents, sans jugement ou inconséquents, le chef est suivi. Il donne alors le sentiment individuel et collectif de nous emmener plus loin, plus haut et mieux que nous l'espérions. Il augmente notre puissance de devenir et de faire plus. Il est alors une autorité pour qui on se donne à plein.

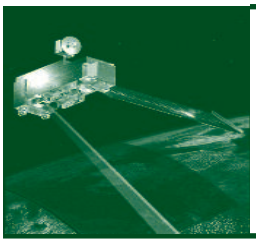
Dans le cas présent, Edward Snowden s'attaque uniquement au deuxième point : le jugement judicieux. Il ne dénigre pas l'idée qu'un service de renseignement fasse du renseignement. Il remet cependant en question l'idée qu'un Etat, en l'occurrence, le sien, l'Etat américain qui se veut le fer de lance d'un monde plus démocratique, outrepasse ses prérogatives par des interceptions dont la finalité réelle reste discutable car elle aboutit à des conséquences insoutenables pour la liberté. S'il est qualifié de traitre par certains, Edward Snowden est en réalité un pur produit du libéralisme américain. Il met en avant la primauté de la conscience morale sur l'ordre du groupe. On retrouve dans sa démarche l'idéologie fondatrice américaine.

IRIS : Qu'entendez-vous par « idéologie fondatrice américaine » ?

Robert Damien : En dénonçant un système jugé abusif, Edward Snowden revient au mythe fondateur protestant des Etats-Unis. Il défend l'idée qu'un individu a le droit de trahir les siens car au-dessus du groupe, ici l'Etat, se trouve l'individu libre, moral et autonome tel que défini par la pensée libérale américaine. Dans cette pensée, il existe un droit, et même un devoir, de faire ce qui est juste moralement. Sans être ce cow-boy solitaire au grand cœur défendu par Hollywood dans ces films, Snowden s'est volontairement détaché du groupe, il s'est mis « hors-la-loi », en dehors de la loi en espérant la faire évoluer et revenir dans le cadre légal. Snowden est ainsi un héros typiquement américain. Ce côté hors-la-loi mais juste se retrouve dès la création des Etats-Unis lorsque les treize colonies s'unissent contre la puissance coloniale britannique. Le petit, le faible, a le droit de se rebeller contre le grand, le puissant, le fort si sa cause est moralement juste. Remettre en cause le système n'est pas considéré aux Etats-Unis comme un acte nécessairement antipatriotique. L'exemple le plus flagrant vient du sommet même de l'Etat lorsque le troisième président des USA, Thomas Jefferson (1743-1826) justifiant l'action de ses troupes durant la guerre d'indépendance affirmait que « L'arbre de la liberté [devait] être revivifié de temps en temps par le sang des patriotes et des tyrans. ».

Avec Snowden, pas de morts, pas de blessés, nous sommes dans le cyberespace, mais cette citation montre qu'il est possible dans cette tradition de renverser un système politique si celui-ci devient amoral, autoritaire ou encore tyrannique, s'il abuse de son autorité et outrepasse les limites de l'autonomie individuelle.■

*
* * *
*



Conséquences stratégiques

par Olivier Kempf,
Docteur en Sciences politiques, Chercheur associé à l'IRIS,
Auteur de* Introduction à la cyberstratégie*, Ed. Economica, 2012

L'affaire Snowden constitue un tournant stratégique majeur dans la conflictualité du cyberespace. En effet, de crises en crises, des « événements » montrent la dimension croissante de cette conflictualité généralisée qui touche de multiples acteurs mais, d'abord, les États. Ainsi, même si l'on décrivait à l'époque (en 1999 !) la guerre du Kosovo comme une « Web war one » à cause des agressions de militants serbes contre le site de l'Otan (sans que cela ait eu une quelconque influence sur la conduite des opérations), le premier véritable tournant a été l'attaque contre les serveurs informatiques de l'Estonie en 2007. La communauté internationale prit alors conscience que le cyberespace pouvait être instrumentalisé à des fins politiques. L'État pouvant apparaitre alors comme une victime.

L'affaire Stuxnet, en 2010, apporta une autre prise de conscience : un État pouvait mener une opération ciblée contre un autre État. Autrement dit, l'État n'était pas simplement victime, il pouvait également devenir l'agresseur. Toutefois, cela se produisait dans le cadre d'une situation d'une conflictualité ouverte puisqu'elle opposait l'Iran avec son programme de recherche nucléaire à l'Occident (États-Unis en collaboration avec Israël) qui voulait empêcher la prolifération. Nous étions dans des systèmes classiques de conflictualité où les États sont au centre du jeu. Le cyber n'apparaissait en fait que comme un autre milieu où pouvait s'exprimer cette conflictualité.

L'affaire Snowden apporte une nouvelle dimension et constitue à ce titre une surprise stratégique. Jusqu'à présent, le cyberespace était considéré comme un milieu par lequel une agression de grande ampleur pourrait être menée, selon le syndrome américain de Pearl Harbor ou du 11-Septembre, or, la réalité a démontré autre chose qui a « surpris ». Certes, nous avions entendu parler d'Echelon en 1999 et 2000. Mais alors qu'on allait justement commencer à tirer les conséquences de cet espionnage généralisé, l'anéantissement des tours jumelles de New-York a radicalement modifié le débat stratégique. Nous parlons depuis de terrorisme et de guerre asymétrique. Avec Stuxnet, nous voici revenus à Echelon. Mais la vrai surprise réside dans la manifestation de la nouvelle nature post-hobbesienne du monde. Le système international n'est ni multipolaire ni unipolaire ni néobipolaire ou toute autre configuration schématique qui obnubile les internationalistes. Il est apolaire, c'est-à-dire qu'il signifie une lutte de tous contre tous. Autrement dit, nous n'avons plus d'ennemis et donc, nous n'avons plus d'amis.

Les Etats-Unis... et le « reste du monde » !

Les États-Unis sont les premiers à adopter cette attitude « globale » au sens français (« générale ») et américain (« universelle »). Les États-Unis ont inventé très tôt la notion de « Reste du monde ». Avec PRISM et son espionnage généralisé, ils révèlent ce qu'ils ont toujours inconsciemment senti : l'altérité constitue l'adversité. Chacun sait, même les plus atlantistes, qu'il peut désormais être tenu pour un adversaire par les États-Unis. Et qu'il l'est de facto. En fait, PRISM « révèle » (dévoile) la fin de la vieille grammaire stratégique d'antan, celle ■■■

■■■ des alliances établies. Le monde est dorénavant déstructuré et le cyberespace renforce cette déstructuration. Voici qui nous mène logiquement à des postures stratégiques où l'intérêt souverain revient au premier plan. Alors que nous sortons définitivement du monde westphalien, voici resurgir la souveraineté : quel paradoxe !

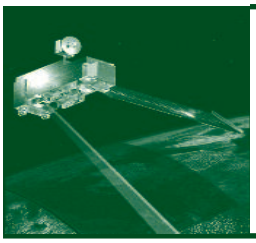
Comme on pouvait s'y attendre, les réactions sont logiquement diverses ! Certains ont pris tout de suite conscience des enjeux. Est-ce un hasard s'il s'agit en premier lieu des pays émergents ? En effet, revenus au rang des nations grâce à leur développement économique récent, ils supportent très difficilement toutes les tentatives de domination. Ainsi voit-on le Brésil développer une stratégie d'autonomie après qu'on eût révélé que sa présidente avait été écoutée par la NSA, au point que ce pays s'est rapproché de l'Argentine malgré les différends séculaires pour bâtir des outils communs de protection. De même, l'Indonésie a très vivement réagi à la révélation de l'espionnage de ses autorités par l'Australie. Djakarta a ainsi suspendu sa coopération militaire et dans le domaine du renseignement avec Canberra en novembre 2013.

Les réactions de l'Europe

En Europe, les réactions ont été variées. Le Royaume-Uni a montré une solidarité de fait avec le cousin américain. La France a été remarquablement discrète hormis quelques condamnations verbales lors des révélations. C'est en Allemagne que le scandale a eu le plus d'effet, au point que la chancelière Merkel apparaît en pointe pour proposer des solutions nationales ou européennes. Constatons pour l'heure une certaine incertitude et une apparente résignation gnérale. Toutefois, la réalité finit par s'imposer et il est probable que chacun prenne des mesures pour augmenter sa propre protection. Ainsi, à l'occasion de la présentation du nouveau « Pacte de défense cyber » par le ministre de la défense français (février 2014), il n'est pas anodin de constater que la première action du premier axe s'intitule « Accentuer le développement et l'usage des moyens techniques contribuant à l'autonomie de nos actions souveraines ». Nous soulignons que le mot « souverain » est utilisé sept fois dans le pacte.

L'affaire Snowden a-t-elle agi comme un révélateur stratégique ? Elle va inéluctablement favoriser les mesures nationales de protection et donc une certaine fragmentation du cyberespace, ce que d'aucuns appellent la balkanisation. Celle-ci n'est pas conduite par des motifs techniques ou économiques, mais d'abord par des motifs politiques. Chacun sait désormais qu'il n'y pas que les Russes ou les Chinois qui peuvent conduire des opérations hostiles dans le cyberespace et qu'il faut se méfier de tout le monde, y compris de ceux qu'on croyait ses amis les plus fiables. PRISM a affaibli des mécanismes de solidarité qui étaient déjà fragilisés par ailleurs. PRISM ne pose pas simplement la question des libertés publiques, mais aussi celle de la souveraineté des nations.■

*
* * *
*



Les contradictions des géants du Net

Entretien avec Nicolas Mazzuchi,
Chercheur associé à l'IRIS,
Directeur de Polemos consulting

IRIS : Le système mis en place par la NSA est censé protéger les Américains du terrorisme, de la prolifération des ADM et des cyberattaques. Mais peut-on penser qu'il sert aussi à des fins d'espionnage économique ?

Nicolas Mazzucchi : Il faut d'abord comprendre le fonctionnement du système global de renseignement américain dans lequel la NSA n'est qu'un élément. Il existe en tout et pour tout 16 agences de renseignement aux Etats-Unis qui forment ce que l'on appelle la communauté du renseignement. Parmi ces dernières, se trouvent des agences purement dédiées à la lutte contre le terrorisme, contre la prolifération des menaces NRBC ou au renseignement d'intérêt militaire, mais aussi d'autres dont les attributions sont plus floues. Il est donc logique de penser que des agences comme la CIA ou l'OICI du Department of Energy ne sont pas actives uniquement dans des domaines souverains. La NSA leur sert avant tout de fournisseur d'informations suite aux interceptions qu'elle réalise. Or, la CIA est un acteur actif dans les domaines économiques, notamment via des sociétés qu'elle possède ou non comme Texas Pacific Group ou InQTel qui rachètent des entreprises étrangères disposant de technologies – notamment IT - considérées comme cruciales pour le gouvernement américain. Enfin, l'implication des services de renseignement dans l'appui aux appels d'offres internationaux où candidatent des entreprises américaines est bien connu. Ce n'est pas une exception puisque le MI6 britannique fait de même en lien avec l'équivalent national de la NSA, le GCHQ, et donne des renseignements issus de ses interceptions aux entreprises du pays. L'un des buts officiels du MI6, affiché sur son site Internet est d'exploiter les opportunités de promouvoir les intérêts britanniques y compris dans le domaine économique. Comme dans le cas américain, la notion d'intérêt peut être particulièrement large…

IRIS : Les grandes sociétés du Net (Apple, Google, Microsoft, etc.) ont une attitude ambiguë à l'égard de la NSA. Apparemment, elles lui laissent un certain accès à leurs données, mais en même temps elles en subissent les intrusions... Comment peuvent évoluer les rapports entre la Silicon Valley et la Maison blanche ?

Nicolas Mazzucchi : Les grandes sociétés américaines de l'Internet ont tout intérêt à jouer la surprise vis-à-vis de la NSA qu'elles aient ou non collaboré au système. Elles se sont pour la plupart construites sur une image jeune, anticonformiste et détendue ; découvrir aujourd'hui qu'elles travaillent avec l'incarnation même du secret et de la machine bureaucratique – qui n'a d'ailleurs pas très bonne presse auprès des Américains – est une catastrophe en termes d'image. Que les dirigeants de Google et Microsoft poussent maintenant des cris d'orfraie apparait surtout comme une stratégie de communication. Ils sont quoi qu'on en dise très dépendants du gouvernement américain. Internet étant une création de l'Etat américain puisqu'il est le successeur du réseau militaire ARPANET et que les Etats-Unis, via l'ICANN et ses dépendances comme Verisign contrôlant physiquement le réseau, les grandes entreprises ont eu tout intérêt à collaborer. Il est quand même étonnant de voir que personne ne se ■■■

■■■ soit douté que si la NSA et la CIA utilisaient Twitter et Facebook en appui aux mouvements du « Printemps arabe », elles pouvaient faire de même dans l'autre sens. En revanche, il est possible, eu égard aux possibilités techniques de PRISM et autres solutions d'interception de la NSA, que la « collaboration » des entreprises du Net soit allée plus loin qu'elle ne l'auraient souhaité ; de la même manière que la coopération allemande dans le domaine du renseignement n'a pas empêché la mise sur écoute du téléphone d'Angela Merkel. Les rapports entre la Maison Blanche et les entreprises peuvent-ils évoluer ? Quelle est en effet la marge de manœuvre de ces entreprises qui ont absolument besoin de l'appui du gouvernement, notamment via l'ICANN, pour prospérer ? Elle semble assez faible. Qu'une certaine défiance naisse entre les deux parties semble inévitable ; néanmoins la coopération continuera d'une manière ou d'une autre.

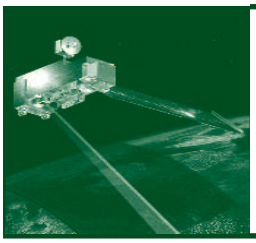
IRIS : Complices ou victimes, ces grandes compagnies ont perdu une certaine confiance de la part de leurs consommateurs. Or tout repose sur la confiance dans un monde où de multiples services sont gratuits. À terme, les révélations de Snowden peuvent-elles représenter une catastrophe économique pour les grands du Net ?

Nicolas Mazzucchi : En effet la force de Facebook, Twitter ou Google, c'est la gratuité de leur service de base qui sert ensuite à proposer des contenus payants aux clients ou aux annonceurs. Mais malgré cette apparente gratuité, ce sont des empires financiers, reposant plus sur le « goodwill » que sur des actifs tangibles et qui sont aux prises dans une compétition impitoyable. Il est amusant de constater que ces entreprises profitent quelque part de cette affaire en se dénonçant l'une l'autre. En témoigne la ligne de produits Microsoft (t-shirts, mugs) anti-Google portant des slogans comme « I'm watching you » ou « Keep calm while we steal your data » avec le logo du navigateur Chrome de Google. De même, Google avait, lors de son affrontement avec Yahoo au milieu des années 2000, mis en avant la coopération de son concurrent avec les autorités chinoises, notamment via son client email.

A partir de là, de plus en plus d'études prédisent la mort ou la déchéance de tel ou tel en se fondant sur des cycles de vie industrielle – presqu'à la manière de Kondratiev – avec les exemples de Myspace ou de Yahoo. Tout le succès d'une entreprise comme Apple a été de dépasser ces effets de mode en vendant non pas des produits mais un mode de vie.

A cet égard on peut dire que le principal apport de Steve Jobs n'a pas été technique mais marketing puisqu'il avait compris l'extrême volatilité de ce marché. La survie de ces géants passera avant tout par ce biais puisque la solution technologique elle-même finit toujours par être dépassée. Cette affaire, si elle ne remet pas en cause par elle-même l'utilisation de ces sites/outils – après tout Facebook vous propose d'indiquer vos orientations religieuses, politiques ou sexuelles, il ne vous y force pas – elle pourrait accélérer le déclin de certains déjà perçus comme plus ou moins obsolètes. ■

*
* * *
*



La gouvernance de l'Internet aux lendemains des révélations

Entretien avec Loïc Damilaville
Adjoint au Directeur général de l'AFNIC en charge de la stratégie

IRIS : Avions-nous les moyens de savoir que les Etats-Unis avaient mis en place un vaste système d'écoute ?

Loïc Damilaville : La réponse est oui ! De tels programmes étaient déjà actifs aux Etats-Unis au lendemain du 11-Septembre. On peut par exemple citer le projet « Total Information Awareness » opportunément rebaptisé « Terrorism Information Awareness – TIA ». Lorsque les membres du Congrès s'inquiétèrent de son coût et de sa portée en 2003, 53 millions de dollars avaient déjà été investis. Les défenseurs des libertés individuelles eurent finalement gain de cause et le Sénat repoussa un temps le programme de financement. Mais pouvait-on vraiment supprimer d'un simple trait d'écriture un dispositif considéré comme stratégique ? Dès la mort de TIA, ses composantes se réorganisèrent rapidement. En mettant peut-être un peu moins l'accent sur la surveillance interne des Etats-Unis – chose qui avait choqué le Sénat – et en conservant l'aspect « contre-espionnage à l'étranger ».

Un rapport publié à cette époque est assez clair : « l'accord n'interdit pas au National Foreign Intelligence Program l'utilisation d'outils de traitement et d'analyse dans le cadre de l'espionnage à l'étranger contre le terrorisme ». Parmi les programmes de cette période qui héritèrent sans doute de TIA, on peut mentionner NIMD (« Novel Intelligence from Massive Data ») dépendant de la discrète « Intelligence Community Advanced Research and Development Activity ». Un autre rapport, parmi tant d'autres, aurait pu susciter l'attention : celui de la DARPA (Defense Advanced Research Projects Agency) qui présentait un certain nombre des projets de cette agence. La question n'est donc pas vraiment de « savoir qui savait », car toutes les agences de renseignement de la planète étaient en mesure de connaître ce que l'internaute Lambda peut encore découvrir en quelques clics.

IRIS : Dans ce cas, pourquoi l'affaire Snowden a-t-elle eu un tel retentissement ?

Loïc Damilaville : Ce qui est en effet le plus étonnant, c'est cette vague d'indignation qui a agi comme un tsunami sur les Etats-Unis. J'y vois deux raisons principales : d'une part, les Etats-Unis ont été pris en flagrant délit de pratiques peu compatibles avec leur statut de « chefs du monde libre ». L'espionnage est peut-être un « métier de seigneurs », mais ce n'est certainement pas une activité de gentlemen ; ces « révélations » ont terni l'image de Washington. L'argument si souvent avancé « plutôt Washington que Moscou ou Pékin » a perdu de sa force.

La seconde raison est sans doute que ces pratiques étaient « tolérables » par les Etats qui n'avaient aucun moyen de s'y opposer, faisaient la même chose à leur échelle et se considéraient comme des alliés de Washington. Dans l'affaire Snowden, il y a eu beaucoup de réactions qui peuvent être associées à du cynisme (tous les Etats ont des services de renseignement et leur indignation sonne faux) mais aussi à des sentiments de déception, de trahison, d'effroi à l'idée que tout est traçable sur l'Internet. Une sorte de « perte d'innocence », d'officialisation d'un « changement de règles » dans les relations entre Etats dans le cyberespace. ■■■

La seule certitude est que ces pratiques vont continuer, et seront plus efficaces que jamais. Aux Etats-Unis bien sûr, mais aussi dans les autres pays engagés dans la course cyber-stratégique et pour qui les informations recueillies grâce à cet incident constituent un « benchmark » particulièrement précieux. A court terme, Snowden a rendu un grand service aux partisans des libertés sur Internet en démontrant la capacité d'espionnage d'une superpuissance. A long terme, ce seront les industriels de ces technologies d'écoute et d'intrusion qui seront les grands gagnants, plus que les Internautes, sauf si ceux-ci apprennent à s'en protéger. La principale portée de l'acte de Snowden a été d'empêcher quiconque de continuer à fermer les yeux. Cette prise de conscience a déjà eu des conséquences tangibles, par exemple dans la manière d'appréhender la gestion des données personnelles. Le choc a ébranlé un système, mais sans doute pas au point de le remettre fondamentalement en question. Il faut en revanche chercher à en tirer des enseignements.

IRIS : Quelles ont été les conséquences directes de l'affaire Snowden pour la gouvernance de l'Internet ?

Loïc Damilaville : La principale a été un affaiblissement marqué de l'autorité morale des Etats-Unis, affaiblissement qui a permis de « soulever le couvercle » mis en place en 2005 à l'issue de la seconde session du Sommet mondial sur la société de l'information. Cet affaiblissement a aussi fragilisé l'ICANN, au moins dans un premier temps. Cet organisme de droit américain gérant la « racine » de l'Internet avait jusqu'à présent réussi à s'imposer grâce au soutien inconditionnel de Wahington. Handicapés par l'Affaire Snowden, les USA ont dû renoncer – au moins provisoirement – à leur intransigeance sur certaines questions liées à la Gouvernance de l'Internet et notamment à leur contrôle unilatéral sur le système « racine ». Ces évolutions restent timides et plus le temps passe, plus la situation perd de sa « ductilité ». Dans ce contexte, se dessine la stratégie de l'ICANN en direction d'un modèle de gouvernance plus ouvert, fondé sur le principe du « multi-stakeholderism » associant de manière équilibrée TOUTES les parties – les stakeholders –. Or, le timing est serré. L'ICANN doit aujourd'hui prouver qu'elle peut exister en dehors de la tutelle protectrice des Etats-Unis. Cette politique conduite par Fadi Chehadé, président et CEO de l'ICANN, a été initiée avant l'affaire Snowden avec l'ouverture de bureaux notamment en Turquie et à Singapour. Les événements de 2013 n'ont fait que l'accélérer. Le système n'est peut-être pas remis en question au plan global, mais en ce qui concerne la gouvernance de l'Internet, il y a une réelle opportunité à saisir.

La réunion qui s'est tenue en octobre 2013 à Montevideo en Uruguay a été un jalon important dans le processus de réflexion autour d'un nouveau modèle de gouvernance. On a constaté que non seulement le moment était venu d'en rediscuter, mais aussi que cette discussion était portée par les principaux acteurs techniques – les organisations en charge du « fonctionnement » de l'Internet. La galaxie IETF/IAB/ISOC, le W3C ainsi que les Registres internet régionaux – RIRs (AFRINIC, ARIN, APNIC, LACNIC, RIPE NCC) ont répondu présents à l'appel de l'ICANN.

IRIS : En quoi cette Déclaration de Montevideo est-elle importante ?

Loïc Damilaville : Elle répond directement à l'affaire Snowden, même si celle-ci n'y est pas explicitement mentionnée. Les signataires préfèrent simplement évoquer leurs préoccupations quant aux conséquences de « récentes révélations sur des pratiques de monitoring et de surveillance ». Il s'agit d'une déclaration de principe qui conteste dans un premier temps le rôle prépondérant des Etats-Unis dans les mécanismes de contrôle de l'Internet. Elle rappelle l'importance d'une gestion globale et cohérente, qui ne doit pas être fragmentée au niveau national. Les signataires affirment leur opposition à une balkanisation de l'Internet encouragée par des problémati-

■■■ -ques de « cyberdéfense » au sens large, dont « l'espionnage » n'est qu'une composante. La déclaration de Montevideo appelle à une accélération du processus de mondialisation de l'ICANN et des fonctions de l'IANA tout en souhaitant que les parties prenantes interviennent sur un pied d'égalité. Un site web a été mis en ligne pour promouvoir cette démarche et permettre le partage autour des discussions en cours. Il s'agit de « 1net ».

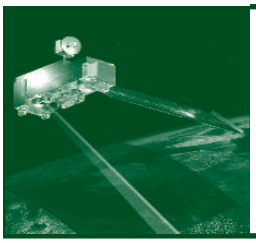
IRIS : La Déclaration de Montevideo n'est-elle pas une nouvelle « rustine » ?

Loïc Damilaville : La Déclaration en soi reste au niveau des grands principes. Elle appelle à une discussion pour réformer un système de plus en plus inadapté au point de vue géopolitique. Même en faisant abstraction des problématiques de cyberguerre, comment se projeter dans un avenir où une ressource dont dépendront tous les peuples continuerait à être techniquement, sinon politiquement, verrouillée par un seul pays. L'affaire Snowden s'est présentée comme une opportunité de « faire bouger » le système et la Déclaration de Montevideo a montré que le défi était relevé. Ensuite, nous pourrons voir si le modèle dont ces efforts accoucheront sera une véritable évolution ou une « rustine ».

IRIS : Quels sont les prochains épisodes probables dans la construction internationale de la gouvernance d'Internet ?

Loïc Damilaville : Le prochain épisode va se jouer à Sao Paulo au Brésil les 23 et 24 avril prochain. L'un des enjeux sera de savoir s'il est possible de construire une gouvernance moins américano-centrée, tout en maintenant un contrôle effectif sur les activités de l'ICANN. Le deuxième challenge est sans doute dans l'articulation difficile entre des gouvernements dotés de pouvoirs régaliens et des parties prenantes représentant d'autres intérêts, parfois ceux-là mêmes que les gouvernements prétendent légitimement représenter. Nous sommes arrivés à un point où réformer est une nécessité perçue par tous – et peut-être même par les Etats-Unis. Mais si le diagnostic est partagé, il n'y a pas encore consensus sur les remèdes. Une solution pourrait être de rechercher un schéma où cette « racine » de l'Internet, objet de tant d'enjeux soit politiquement « neutralisée », c'est-à-dire qu'aucun Etat ne puisse l'exploiter à des fins politiques contre un autre Etat. Cette hypothèse pourrait cependant impliquer un traité international ou quelque chose qui y ressemblerait fort, et un scénario est encore loin de faire l'unanimité parmi les parties prenantes. ■

*
* * *
*



OBSERVATOIRE GEOSTRATEGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATEGIQUES

L'Europe après la vague Snowden

Entretien avec Nicolas Arpagian,
Directeur scientifique du cycle « Sécurité numérique » à l' INHESJ
Auteur de* La Cybersécurité*, collection Que Sais-Je ?, PUF

IRIS : Que veulent et que peuvent faire les instances européennes pour assurer la confidentialité des données de leurs concitoyens, et la sécurité des données stratégiques ?

Nicolas Arpagian : On peut se réjouir que les Européens aient commencé à se faire à l'idée que leurs données ont de la valeur. Qu'il s'agisse de leurs correspondances dont il convient de protéger la confidentialité. Ou de leurs données personnelles carburant vital aux activités de datamining et de marketing dont vivent les géants de l'Internet : Google, Facebook… L'Europe est en train, notamment à l'initiative de ses parlementaires, de prendre conscience que son patrimoine est aujourd'hui largement informationnel. Innovation, Recherche & Développement, données de consommation… ce sont bien ces informations compilées et raffinées qui assurent à l'Europe sa prospérité économique. Si elle renonce à leur protection, l'économie européenne verrait peu à peu s'évaporer ce qui fait sa richesse actuelle, et donc future. Cela suppose de rompre avec une perception béate de l'Internet qui verrait dans le réseau qu'un seul canal de communication entre des correspondants bienveillants. Il s'agit bien de vecteurs d'informations qui peuvent faire l'objet d'interceptions, de blocages et de prises de contrôle à distance par des tiers. Les élus répugnent à se saisir des sujets de cybersécurité et de gouvernance d'Internet car ils sont rarement interpellés sur ces dossiers lors de leurs permanences dans leur circonscription. Moralité le débat se limite à quelques lobbys commerciaux affrontant des militants associatifs sous l'œil des services de l'Etat.

Quelle place pour la vie privée dans une économie de la gratuité où l'enregistrement de notre navigation et de nos réactions fait office de moyen de paiement ? Comment s'exerce la souveraineté quand nous sommes limités au statut d'utilisateurs de technologies, sans moyen de savoir comment elles sont élaborées ? Pour se faire respecter des firmes et des Etats tiers, l'Union européenne doit apprendre à parler d'une seule voix. C'est tout le paradoxe de cette Europe où nous mettons en commun des dispositifs juridiques mais où les économies, et les élections, se jouent nationalement. Snowden a permis de faire comprendre aux plus sceptiques que les Etats mettaient à l'occasion leurs équipements de surveillance numérique au service de leur tissu économique. Chaque gouvernement se préoccupe des performances de ses champions nationaux. Les emplois, la fiscalité et les scores électoraux sont des enjeux à l'échelle nationale. Comment voudrait-on que ces mêmes Etats se mettent d'accord pour réguler et encadrer les arsenaux numériques qui leur permettent dans une relative impunité de piller leur voisin, allié politique mais compétiteur économique ? Au nom de quoi renonce-t-il à cette formidable possibilité qu'offre l'arme numérique de surveiller ses rivaux et de découvrir la force de ses concurrents ? On ne voit pas comment une véritable stratégie de cybersécurité européenne pourra voir le jour, sans un bénéficiaire commun. C'est à dire une économie et un corps électoral uniques : ceux de l'Europe fédérale. Sinon, la situation persistera : des reculades économiques des discours théoriques sur l'évidente ■■■

■■■ nécessité de collaborer en matière de cybersécurité, et le maintien de stratégies et de moyens nationaux juxtaposés tentant chacun de préserver son pré carré. L'Europe deviendra un acteur crédible de cette économie numérique quand elle sera à même de susciter ses propres acteurs, et cessera de se réserver le rôle de meilleur client de produits et solutions dont la composition et la tutelle lui échappent. Sachant que des solutions alternatives sont possibles, nous sommes en mesure de résister à ceux qui exploitent les systèmes de navigation de notre téléphone et de notre ordinateur, nos recherches sur la Toile, nos photos, nos vidéos sans oublier nos déplacements et bientôt nos données médicales.

IRIS : La réforme de la NSA promise par Barack Obama dans son discours du 17 janvier 2014 est-elle de nature à rassurer les décideurs et les citoyens européens ? Rassure-t-elle d'ailleurs les internautes étatsuniens ?

Nicolas Arpagian : Barack Obama est conscient que son pays ne peut que perdre d'une redistribution des cartes, avec redéfinition du fonctionnement de l'ICANN, par exemple. Il peut d'une certaine manière se satisfaire de l'échec du sommet de Dubaï organisé par l'Union International des Télécommunications (UIT) en décembre 2012. A cette occasion les affrontements ont éclaté au grand jour entre les camps russe et chinois qui réclament une tutelle renforcée sur le réseau, les Européens peu à même d'imposer une véritable vision commune et les Etats-Unis guère enthousiastes à l'idée de perdre leur privilège sur le Net. On a l'impression que Barack Obama a multiplié les comités pour créer des situations d'enlisement. Sous prétexte de débats et de concertation, il paralyse toute réforme par l'ouverture de fronts multiples de négociation. Ses interlocuteurs s'épuisent, se divisent et ensablent peu à peu toute refonte du système. Du bel ouvrage. A contrario, notons la proposition innovante d'Angela Merkel lors du 19ème Conseil des ministres franco-allemand mi-février 2014 où elle suggère de « créer un réseau de communication à l'intérieur même de l'Europe (…) afin de conserver un niveau élevé de protection des données ». Cette initiative allemande a le double mérite de mettre le sujet sur la table au plus haut niveau politique et de constituer un chantier technologique ambitieux pour le couple franco-allemand dans un premier temps, et pour le clan européen ensuite.

IRIS : La réaction de nos dirigeants aux révélations de Snowden vous paraît-elle à la mesure de l'événement ?

Nicolas Arpagian : Il aura fallu apporter des preuves nombreuses, récentes et précises pour que le sujet de l'espionnage soit enfin sur le devant de la scène. Malgré cela, on ne peut que constater le caractère mesuré de la réponse de Barack Obama, qui a conclu : « on ne va pas s'excuser juste parce que nos services sont peut-être plus efficaces ». Il a ajouté qu'il s'expliquerait individuellement avec chacune des chancelleries européennes. Là encore l'Europe n'apparaît pas comme une entité cohérente. Avec toute la gamme des relations d'allégeance à la puissance étatsunienne, chaque Etat sait qu'il procède de même – ou aimerait pouvoir le faire – avec ses moyens d'interception. A ce jeu, Washington a été pris la main dans le sac car Snowden a trahis son engagement de confidentialité. Quelle chancellerie peut affirmer être à l'abri d'une telle défection ?

Les Etats sont confrontés à un dilemme : soit ils passent pour des naïfs démunis et inexpérimentés s'ils n'ont pas des capacités de surveillance conséquentes, soit ils font figure de grands inquisiteurs. Les deux options sont guère confortables pour des régimes démocratiques. Ce qui explique la relative modération des gouvernements ciblés, à l'exception de la Présidente Dilma Rousseff et de la Chancelière Angela Merkel, qui ont toutes deux donné de la voix. Ce qui reste très impressionnant est l'ampleur, l'ancienneté et la profondeur des moyens de surveillance. Cela pose la ■■■

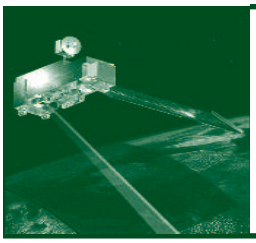
■■■ question du traitement et de l'analyse des données collectées. Afin de les identifier, les exploiter et les transmettre. Sans cette continuité du cycle de l'information, cette collecte tous azimuts reste stérile. Nos dirigeants ne sont venus que tardivement aux questions de cybersécurité qui sont depuis bien longtemps une priorité à la Maison Blanche. Ils doivent aborder les sujets technologiques pour en faire un vrai champ d'action politique, économique et technique. Cela permettra à l'opinion publique de s'en saisir. Et de ne pas se cantonne pas à être des utilisateurs passifs d'équipements dont le fonctionnement, le pilotage et le suivi leur échappent.

En Europe, rares ont été les entreprises à renoncer à tel prestataire ou tel équipementier car le capital de celui-ci était majoritairement détenu par des capitaux étatsuniens et le soumettait à l'application du programme PRISM. Les contrats limitant les conditions de sortie, des solutions techniques, un coût lié à l'identification puis au transfert à un autre fournisseur, le risque de perte de données ou d'interruption de services lors dudit transfert, la perte de compétences en interne suite à des externalisations successives… autant de « bonnes » raisons de ne rien changer. Et donc de neutraliser l'impact des révélations de Snowden. Seuls les pays émergents, qui étaient dans une situation de dépendance moindre, ont pu reconsidérer leurs investissements et faire jouer la concurrence avec des fournisseurs hors des Etats-Unis.

IRIS : L'idée même de gouvernance a-t-elle encore un sens face à l'ampleur du contrôle technique (Code is law) et face à la position de force américaine ?

Nicolas Arpagian : La souveraineté numérique passe par la maîtrise de la connaissance technique. Si vous comprenez le code que vous utilisez, vous mesurez les conséquences de son emploi. Dans une chronique publiée dans le quotidien Les Echos en août 2013 j'appelais les entreprises à se mettre au « hacking ». C'est à dire à se mettre en position de décortiquer la technique pour s'approprier son fonctionnement, et donc permettre ainsi de l'améliorer. Par cette combinaison du savoir-faire technique, de la maîtrise juridique et d'un arbitrage politique, la gouvernance peut porter ses fruits. Si les Etats, les citoyens et les acteurs économiques s'impliquent dans chacune de ces composantes. Si un de ces aspects venait à dominer ou à manquer, la gouvernance serait inopérante pour les citoyens, électeurs, consommateurs et internautes que nous sommes. ■

*
* * *
*



OBSERVATOIRE GEOSTRATEGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATEGIQUES

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

De la nécessité de se réapproprier le cyberespace

Entretien avec Jérémie Zimmermann
Co-fondateur de la Quadrature du Net

IRIS : Avez-vous été surpris par les révélations d'Edward Snowden ?

Jérémie Zimmermann : Nous avons tous été à juste titre outrés, choqués par cette affaire, notamment par l'échelle globale de la surveillance de masse, et par la collaboration active des géants tecchnologiques. Les services de renseignement dans le monde utilisent massivement l'outil internet pour surveiller, sinon contrôler, les faits et gestes des internautes, et donc des citoyens. Il existe des structures étatiques – et non étatiques – chargées d'analyser les flux de donnés échangées. Il n'y a pas si longtemps, on qualifiait, un peu rapidement, les Geeks et les hackers de paranoïaques… Mais ce que certains appelaient paranoïa autrefois était en réalité de la prudence.

IRIS : La NSA n'est qu'un des nombreux services de renseignement dans le monde, est-il encore possible, lorsqu'on est un simple citoyen, d'échapper à cette surveillance ?

Jérémie Zimmermann : Il faut tout d'abord distinguer deux niveaux dans cette surveillance : la surveillance ciblée et la surveillance généralisée. Pour la première, il est très difficile d'y échapper si un Etat – ou un service de renseignement – décide de vous cibler personnellement. Pour la seconde, il existe des solutions. La surveillance généralisée peut être mise en échec… Et de façon assez simple ! Il est nécessaire dans un premier temps d'arrêter d'utiliser des produits que l'on sait surveillés. Je pense à Yahoo, Google, Facebook, Apple, Microsoft… ou encore Skype. Il est illusoire de croire qu'un simple cadenas dans la barre d'adresse de votre navigateur empêche les services de renseignement de rentrer dans vos boites mails ou fils d'actualité. Au-delà de l'aspect technologique, rappelons qu'il existe des accords entre les grandes entreprises américaines du Net et certains gouvernements. Il s'agit ni plus, ni moins que de collaboration active. Il n'est, dans ce cas, même plus nécessaire de briser un mot de passe pour accéder à certaines données. L'opérateur, votre opérateur, donne, offre, ces informations à un service, à un Etat.

IRIS : Yahoo, Google, Facebook… Il semble pourtant difficile d'y échapper. Les géants du web sont partout. Quelles alternatives existe-t-il ?

Jérémie Zimmermann : Ces géants ne sont pas incontournables, bien au contraire ! Nous pouvons citer trois exemples très concrets. Premièrement, les logiciels libres. Les utilisateurs de tels outils confèrent à l'ensemble de l'humanité les mêmes droits et libertés dont ils jouissent sur leur œuvre, comme notamment la possibilité de modifier le programme. Nous pouvons citer Mozilla Firefox, GNU/Linux, Bittorrent, Vlc ou encore TOR. Avec de tels logiciels, il est plus difficile d'y insérer des fonctions malveillantes et beaucoup plus facile de les trouver s'il y en a. Deuxièmement, les services décentralisés. Chacun reste ainsi maître de ses données. Enfin troisièmement, le chiffrement de bout en bout. Chacun gère ses clefs et les échanges avec ses correspondants. Néanmoins, pour ces trois types de technologie, il est nécessaire que l'utilisateur ait une démarche active. Il est nécessaire de s'approprier la technologie pour qu'elle puisse nous rendre plus libres. ■■■

IRIS : A-t-on besoin d'être un geek pour maitriser cette autre forme d'internet ?

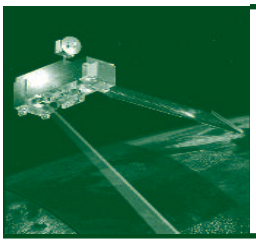
Jérémie Zimmermann : Pas du tout, d'expériences, des étudiants littéraires n'avaient besoin que de deux heures pour apprendre à chiffrer et envoyer des mails chiffres. Il est donc envisageable qu'un simple citoyen puisse dans un temps raisonnable maitriser cette technologie. Quant aux logiciels libres, ils sont d'un accès facile. Je pense notamment à des systemes GNU/linux comme Ubuntu ou Mint, à TOR ou Firefox. Les blocages que l'on voit sur cette appropriation sont d'ordre psychologique. L'utilisateur se sent impressionné. Il a peur de cette nouvelle forme de technologie. Cette technophobie n'est cependant pas justifiée. Elle est simplement renforcée par les discours marketing d'Apple ou de Microsoft qui affirment garantir la sécurité de l'internaute. Sécurité en réalité illusoire.

IRIS : Vous évoquez le système TOR qui permet à l'utilisateur de brouiller son identité, or ce système n'est pas infaillible. Il est possible sous certaines conditions de désanonymiser l'internaute ?

Jérémie Zimmermann : Si dans le monde réel, il n'y a pas de système infaillible… c'est tout aussi vrai sur Internet. TOR n'échappe pas à la règle. Il est possible dans un environnement contraint de prendre le contrôle de certains nœuds. Cependant cette démarche d'intrusion ne se fait pas naturellement, il est nécessaire de s'y attarder avec difficulté pour ne pénétrer in fine qu'une partie du reseau TOR. Pour rendre cette intrusion encore plus difficile, il est nécessaire d'augmenter le nombre d'utilisateurs car plus il y aura d'utilisateur, plus il y aura de nœuds. La NSA, selon certaines revelations de Snowden, aurait du mal à casser la cryptographie de TOR.

IRIS : Le système mis en place par la NSA est-il susceptible d'être vaincu ou contrarié ?

Jérémie Zimmermann : Pour ce qui est de la surveillance de masse, oui, c'est probablement possible ! Pour y arriver, il est nécessaire dans un premier temps que l'ensemble de la société se mobilise. Du simple citoyen aux acteurs économiques sans oublier le monde politique : tous, ont un devoir moral de reprendre le contrôle des institutions de renseignement. Ils ont une obligation d'agir et d'imposer à leurs gouvernements la mise en place de mesures de rétrocontrôles étatiques effectives. Il faut aussi des politiques publiques pour encourager et promouvoir ces technologies qui rendent plus libre (logiciels libres, architectures décentralisées et chiffrement de bout en bout), par rapport aux technologies du contrôle. C'est un processus long et douloureux car il s'agit de revoir le système en place. Par ailleurs, il est nécessaire d'informer le public. Si ces techniques d'interception sont connues du grand public, le comportement des utilisateurs évoluera de lui-même. Egalement, il serait judicieux de former les utilisateurs aux techniques de chiffrement de bout en bout. Cela n'empêchera pas forcement des interceptions mais cela compliquera lourdement la tâche des services de renseignement. Dernier point que j'aimerais évoquer. J'espère que l'on va arriver dans un futur proche à collectivement reconnaitre la valeur des lanceurs d'alerte. Il ne s'agit pas de les glorifier, mais de les protéger publiquement et juridiquement afin de permettre à plus d'individus d'avoir le courage d'avertir le citoyen des crimes et mensonges dont ils sont témoins.



OBSERVATOIRE GEOSTRATEGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATEGIQUES

Au delà de l'effet Snowden

par François-Bernard Huyghe,
Directeur de recherche à l'IRIS

Ce qu'il est convenu d'appeler « affaire Snowden » recouvre la révélation par un individu, simple rouage de la machine, ayant accès à des documents internes qui semblent authentiques, de la monstrueuse complexité du système de la NSA : ce dernier vise à collecter des milliards de données et métadonnées par toutes les méthodes connues, du prélèvement sur des câbles sous-marins à l'espionnage hyper-ciblé des téléphones de chefs d'État. C'est une entreprise sans aucune mesure avec l'alibi officiel qui est d'empêcher des attentats ou de sauver des vies.

Pour décrire un phénomène de cette ampleur, beaucoup ont évoqué la figure de Big Brother. Mais dans le roman d'Orwell, le dictateur, qui n'est peut-être qu'une image ou un fantasme, tient à ce que vous sachiez qu'il vous surveille tandis que la police de la pensée peut vraiment vous réprimer pour ce que vous avez dit ou pour la rébellion, que vous avez seulement envisagée.

Surveiller les masses, anticiper les tendances

Or, la logique du projet NSA est moins de surveiller pour punir que de collecter pour prédire. Sans doute inspirée par l'idée que celui qui sait tout ne craint rien, cette mystique de la « Total Information Awareness » traduit à la fois une confiance irraisonnée dans le calcul (en corrélant un nombre suffisant d'indices et de déterminants avec des algorithmes assez puissants, on en saurait plus sur vous que vous-même) et la crainte que quoi que ce soit échappe à la capacité d'anticiper ou de contrôler de la bureaucratie US. Plus, il faut bien le dire, le désir de conserver une supériorité ou une avance par ce qui ressemble furieusement à de l'espionnage industriel.

Un tel système peut-il être productif ? Hors son intérêt économique, nous n'en sommes pas persuadés. Vu les performances de l'administration Obama dans la lutte contre le Djihad ou dans des affaires comme le conflit syrien, on peut douter que ce soit l'arme absolue en géopolitique. Et à quoi sert de connaître les secrets de tous les autres, s'il suffit d'un employé saisi d'un scrupule pour que vos propres secrets soient mis sur la place publique ?

Se pourrait-il au contraire que ces milliards de dollars dépensés et ces milliers de cerveaux mobilisés aient produit un dommage en termes de perte de confiance ou de légitimité que ne compensera jamais aucun gain stratégique ? Les conséquences pourraient varier suivant les domaines.

Les gouvernements – certains participant au système d'échange du renseignement, d'autres espionnés par lui, plusieurs les deux à la fois – ont eu des réactions qui vont de la tension diplomatique comme le Brésil aux vagues remarques, vite enfouies sous les protestations d'amitié. Une fois passé ce stade des silences gênés, les conséquences technologiques qu'en tireront lesdits États seront cruciales : voir le projet évoqué par Angela Merkel d'un réseau européen pour le transit des données personnelles. L'affaire Snowden vient aussi de fournir un redoutable argument aux pays réputés « ennemis » d'Internet, comme la Russie et la Chine : dans les organisations internationales, où ils défendent la souveraineté numérique versus la gouvernance à l'occidentale, il leur sera trop facile de rappeler la poutre qui est dans l'œil des défenseurs supposés de la liberté. Le même schéma vaut probablement pour les grandes compagnies du Net ; elles sont décrédibilisées auprès de leurs clients pour leur complaisance envers la NSA, mais se trouvent aussi

victimes d'opérations menées par la même NSA et qui relèvent plutôt du hacking. À quel niveau de pertes financières la fuite des consommateurs et de leurs données personnelles deviendra-t-elle insupportable ? Et à quel moment la création de solutions alternatives garantissant la confidentialité des données deviendra-t-elle une vraie tentation ? Il faut se souvenir qu'il est plus facile est moins coûteux d'abandonner un réseau social ou une application que sa voiture et que tout le système repose sur deux ressources que nous répartissons relativement librement : notre attention et notre confiance.

Le choix à notre portée

Au final, ce sont les réactions des citoyens qui seront déterminantes, donc le choix qu'ils feront ou de conserver des facilités souvent gratuites (mais qui se paient du fait que nos données sont une marchandise économique et une source de pouvoir politique) ou, au contraire, d'accepter les efforts, temps et apprentissage, qu'implique la conversion à un web sécurisé.

Difficile, pourtant, de ne pas être frappé par l'incroyable passivité des opinions publiques devant ces révélations. Nous est-il vraiment indifférent que quelqu'un dans le Mayland sache où nous étions hier, quels services médicaux nous consultons et quelles sont nos orientations sexuelles ? Nous y sommes nous résignés parce qu'après tout Facebook en sait presque autant sur nous et que la police ne va pas nous interpeller à l'heure du laitier ?

Comment convaincre chacun qu'il ne s'agit pas d'un « simple » viol de son intimité, mais de l'avènement d'une société de contrôle et de prévision d'un type inédit ? De la réponse à cette question dépendra l'avenir du système de surveillance planétaire. Attendre qu'il disparaisse, miné par son absurdité et sa démesure comme une machine de Tinguely dont la fonction est de s'auto-détruire, ne nous semble pas une perspective rassurante. Et s'il faut espérer quelque chose, c'est bien que le citoyen se préoccupe d'un pouvoir invisible dont il est à la fois la victime et la source.

Pour aller plus loin...

Deux livres très récents en français ainsi que quelques hyperliens vous aideront à comprendre le système :

- *L'affaire Snowden*, par Antoine Lefébure, Edition La Découverte, 2014
- *Lanceurs d'alerte, les mauvaises consciences de nos démocraties*, par Florence Hartmann, Edition Don Quichotte, 2014
- L'animation interactive du Monde « Plongée dans la pieuvre de la NSA »:
- Le dossier « Synthèse du programme de surveillance américain »
- Une représentation du système sous forme de carte mentale
- Un graphique interactif du Spiegel sur les outils d'espionnage :
- L'observatoire de la NSA par la Quadrature du Net

L'Observatoire Géostratégique de l'Information

Sous la direction de François-Bernard Huyghe, cet observatoire a pour but d'analyser l'impact de l'information mondialisée sur les relations internationales. Comprendre le développement des médias et de l'importance stratégique de la maîtrise de l'information. Il analyse, par exemple les rapports de force entre puissances politiques et économiques et les firmes qui contrôlent le flux des informations dans le Monde.

IRIS - Institut de Relations Internationales et Stratégiques
2 bis, rue Mercoeur
75011 Paris - France
contact@iris-france.org

www.iris-france.org
www.affaires-strategiques.info

Entretiens réalisés par Pierre-Yves Castagnac