

Géopolitique de l'Internet

Quel "secret d'État" dans le cyberspace ?



Par Jean-François
Fiorina

Directeur adjoint
 de Grenoble Ecole
 de Management
 Directeur de l'ESC
 Grenoble

**La Toile ne manque pas
 de cyber-activistes qui
 cherchent à faire valoir leur
 cause ou leur idéologie à
 coups de divulgations plus
 ou moins sensationnelles...**

PRISM, XKeyscore, Tempora, Bullrun... Depuis les premières révélations fracassantes d'Edward Snowden, les programmes d'écoutes de la NSA et de ses alliés n'en finissent pas de faire la une de l'actualité. Cette dernière affaire en rappelle une autre : les divulgations en 2010 des War Logs et de télex diplomatiques par WikiLeaks. À chaque fois, la même marque de fabrique : des "lanceurs d'alerte" qui portent à la connaissance d'un large public des informations classifiées, via Internet, mais avec le concours actif de grands titres de la presse écrite. *"S'interroger sur le secret à l'ère numérique revient à se demander comment les invariants - anthropologiques - du secret s'articulent avec l'innovation technologique. Et les réponses peuvent surprendre : le sans précédent coexiste avec le toujours pareil"*, écrivent François-Bernard Huyghe et Paul Soriano en introduction du remarquable numéro que la revue *Médium* consacre au sujet. Malgré les apparences en effet, il n'est pas sûr que les nouvelles technologies modifient les rapports de force entre acteurs - qu'ils prêchent la "transparence" ou la défense de la "raison d'État".

Dès ses débuts, pourtant militaires, Internet a été perçu comme un espace de liberté d'expression totale. Mieux, ce nouveau média permettait d'espérer qu'il suffirait d'une connexion "pour que la planète ait accès à des documents originaux prouvant l'espionnage, la bavure ou le déni de droit" (François-Bernard Huyghe). Si la décennie écoulée a largement fait la preuve que l'Internet libre n'était pas pour demain, l'impossibilité technologique d'empêcher la révélation d'un secret est désormais acquise. À partir des seuls réseaux sociaux, un individu peut - en théorie du moins - mobiliser des millions de gens à sa cause. Et la Toile ne manque pas de cyber-activistes qui cherchent à faire valoir leur cause ou leur idéologie à coups de divulgations sensationnelles.

David contre Goliath ?

Le lanceur d'alerte renvoie à une sous-catégorie qui réunit des acteurs agissant dans l'intérêt commun en rendant public "des éléments qu'il[s] considère[nt] comme menaçants pour l'homme, la société, l'économie ou l'environnement" (Francis Chateau-Raynaud et Didier Tornay). Il est l'adaptation de la notion anglo-saxonne de *whistle-blower*, qui fait référence au "coup de sifflet de l'arbitre". Figure hautement controversée, le lanceur d'alerte est pour les uns un héros de la vérité et de la justice, mais pour les autres un "mouchard" - voire un traître. Le phénomène apparaît aux États-Unis dès les années 1970 avec Daniel Ellsberg et l'affaire des *Pentagon Papers*.

Le réseau ne permet pas seulement de "dénoncer un secret", mais d'en apporter la preuve. Wikileaks en fera le coeur de sa stratégie, Edward Snowden son assurance-vie.

Sortis de la couche cognitive, qui n'est qu'une partie d'Internet, les briseurs de secrets n'ont pas les moyens de s'opposer aux puissances des États et de leurs industriels...

Les révélations sont le plus souvent d'abord faites par la presse écrite, mais ensuite largement relayées par les médias de masse que sont la radio et la télévision. Avec Internet, la caisse de résonance change de dimension : elle est à la fois mondiale et instantanée. Les divulgations faites par WikiLeaks ou les révélations de Snowden bénéficient également d'un "effet Streisand" - c'est-à-dire d'une augmentation importante de la diffusion d'informations ou de documents faisant l'objet d'une tentative de retrait ou de censure. Autrement dit, plus l'on veut éteindre l'incendie, plus les flammes repartent de plus belle. Le réseau permet enfin de ne plus seulement dénoncer un secret, mais d'en apporter la preuve matérielle en diffusant les documents originaux ou leurs copies. WikiLeaks en fera le coeur de sa stratégie, Edward Snowden son assurance-vie.

Le lanceur d'alerte et les réseaux sociaux alimentent l'image d'une stratégie "du faible au fort" (Christian Harbulot) autorisant de défier les puissances établies que sont l'État et ses institutions, mais aussi les multinationales et les grandes ONG. Internet favorise-t-il pour autant une nouvelle distribution des cartes de la puissance en faveur des plus faibles ? L'utilisation du réseau à des fins de divulgation a assurément une dimension asymétrique - caractérisée par le recours à la ruse (*mêtis*) plutôt qu'à la force (*arété*). Elle s'exprime à chaque fois par le contournement d'un arsenal juridique (protection du secret-défense ou de la confidentialité des affaires) et des autorisations hiérarchiques. Gamme stratégique *a priori* intéressante, mais "nous entrons ici dans le jeu des perceptions et de l'influence, [...] dont les effets sont difficilement évaluables. Au-delà d'une indignation passagère, quelle portée accorder aux actions de WikiLeaks ? Peut-on évaluer l'action des Anonymous dans les Printemps arabes ? ", interroge Olivier Hubac, chercheur associé à la Fondation pour la recherche stratégique. Dix ans après le scandale ECHELON, non seulement le gouvernement américain et la NSA n'ont pas été inquiétés, mais l'on (re)découvre avec l'affaire Snowden que ses programmes d'interception se sont sensiblement améliorés...

Beaucoup de bruit pour rien ?

Certains ont voulu voir - croire ? - qu'avec Internet nous assistions à la dissolution des rapports de pouvoir dans une sphère des échanges de savoir devenue égalitaire. Mais, loin de mettre "au placard la vieille politique et son grand échiquier" (Régis Debray), les nouvelles technologies sont en réalité autant d'instruments qui les servent. Les révélations sur les écoutes des services de renseignement ne mettent-elles pas surtout en évidence qu'il existe une différence fondamentale entre "globalité et universalité" ? Internet ne semble pas modifier les rapports de puissance : il tend même plutôt à les renforcer. Pour l'heure, le bilan concret des affaires récentes se résume en effet à "Manning jugé, Snowden pourchassé, [et] Assange assiégé" (François-Bernard Huyghe). Les acteurs qui détiennent la maîtrise du contenu et du sens sont ceux qui disposent d'une capacité d'action globale dans toutes les couches constitutives du cyberspace, dont celle "constituée de toutes les infrastructures physiques et celle - dite logique - qui comprend l'ensemble des applications et des données analogiques ou numériques qu'elles véhiculent" (cf. note CLES n°54, 9/02/2012). Sortis de la couche cognitive, les briseurs de secrets n'ont pas de moyens véritables à opposer aux puissances que sont les États alliés aux grands groupes industriels de l'Internet. Surtout, le secret d'État n'est-il pas, le plus souvent, un mal nécessaire ?

Le propre d'un service de renseignement extérieur est d'agir dans l'illégalité pour connaître les secrets des autres. C'est même sa raison d'être. Les dirigeants politiques victimes d'espionnage peuvent le déplorer, mais sûrement pas feindre de découvrir la nature du monde du renseignement. En la matière, la notion d'ennemi/ami est toute relative. Autrement dit, les Américains sont les alliés des Européens dans la lutte contre le terrorisme, davantage des compétiteurs - voire des adversaires - en matière économique. Pour cette raison, l'affaire Snowden plonge dans l'embarras les chancelleries européennes, car "il est désagréable de rappeler qu'il s'agit d'une guerre économique entre nations où tous les moyens sont bons pour terras-

ser le concurrent" (Régis Debray). Seule la presse pousse ici à la réaction. Quant à la révélation du contenu exact d'échanges diplomatiques confidentiels, c'est méconnaître les mécanismes de toute négociation, publique comme privée. Déjà, en 1926, Jules Cambon lançait cet avertissement aux tenants d'une certaine forme de "dictature de la transparence": "Le jour où il n'y aura plus de secrets dans la négociation, il n'y aura plus de négociation du tout". Ce que confirme l'ancien ministre des Affaires étrangères, Hubert Védrine: "l'idée que tout doit être connu, tout de suite, est évidemment incompatible avec une négociation internationale sérieuse, a fortiori dans la vie économique (et d'ailleurs on ne l'applique pas dans la vie des affaires). Mais c'est surtout une question de moment". Et de préciser: "L'idéologie de la transparence ne souffre aucune contradiction, aucune nuance, elle est totalitaire, se présente comme un absolu."

Cela signifie-t-il qu'il faille condamner toute action dès lors qu'elle se réclame de la transparence et de la liberté d'expression? N'est-il pas des cas où la divulgation d'un secret peut être salvatrice et donc souhaitable?

La tentation de Prométhée

Les révélations dans le cadre de l'affaire Snowden soulèvent aussi d'autres questions. Si les programmes d'espionnage d'État ont toujours existé, ceux déployés par la NSA américaine surprennent par leurs capacités. Il s'agit d'abord de systèmes d'interception de flux massifs d'information allant de la collecte de métadonnées multi-supports (c'est-à-dire de données sur les données) jusqu'aux contenus mêmes de millions de communications Internet. N'y a-t-il pas dès lors un risque de banalisation de l'espionnage domestique? Quand et comment détermine-t-on ceux qui doivent faire l'objet d'une introspection plus poussée? Le "scandale" de la NSA vient ensuite confirmer une imbrication croissante entre acteurs publics et privés, et ce à plusieurs niveaux. PRISM démontre la collaboration volontaire des principaux opérateurs d'Internet à la collecte du renseignement, tandis que l'analyse se voit confier en partie à une cascade de sous-traitants privés. Cela pose la question de la privatisation grandissante du renseignement. Est-il pertinent de partager une mission régaliennne? Quels sont les moyens de contrôle mis en œuvre? Enfin, il y a aux États-Unis une forte ambiguïté sur la légalité d'une partie des écoutes de la NSA dès lors qu'elle concerne des ressortissants américains sur le sol national. Face aux possibilités offertes par la technique, et notamment Internet, la NSA a-t-elle été tentée de s'affranchir de la loi, à moins que ce ne soit avec une caution politique? Dans tous les cas, il y a manifestement danger pour les libertés publiques quand une agence de renseignement extérieur se tourne vers l'intérieur...

Ces nombreuses questions ne concernent pas les seuls Américains, loin s'en faut. Elles renvoient au souci d'équilibre entre nécessaire action clandestine et préservation des libertés civiles - et en particulier de la vie privée. Comme nous prévient John le Carré: "L'âme d'une nation se révèle dans ses services secrets". ■

Pour aller plus loin: "Alerte en sept leçons" (François-Bernard Huyghe), "Entretien avec Hubert Védrine" et "Rien de nouveau?" (Régis Debray), in *Secrets à l'ère numérique*, revue *Médium* n° 37-38, 362 p., 30 €; "L'adversaire dans le cyberspace: diversité, capacité d'action et asymétrie", *DSI*, Hors-série n°32, octobre 2013, 10,95 €.

PRISM démontre la collaboration volontaire des principaux opérateurs d'Internet à la collecte du renseignement, tandis que l'analyse se voit confier en partie à une cascade de sous-traitants privés. Ce qui pose la question de la privatisation grandissante du renseignement.

EXTRAIT :

Sur l'ambivalence de la "transparence": "L'idéologie de la transparence dissimule la pratique de l'occultation. Le pays qui entend imposer la gouvernance globale et soutient les cyberdissidences contre les dictatures nous espionne. Ceux qui réclament la publication de tous les secrets d'État sont obligés de se conduire en conspirateurs." (François-Bernard Huyghe, "Alerte en sept leçons", op. cit.)

Retrouvez d'autres analyses géopolitiques sur www.diploweb.com et sur <http://notes-geopolitiques.com>