infoveilles

CENTRE DE DOCUMENTATION DE L'ÉCOLE MILITAIRE
1 place Joffre - 75700 PARIS SP07
01 76 64 85 98 /// www.cdem.defense.gouv.fr

Que révèle vraiment l'affaire Edward Snowden (*Prism*) ?

#26 /// 28 septembre 2013

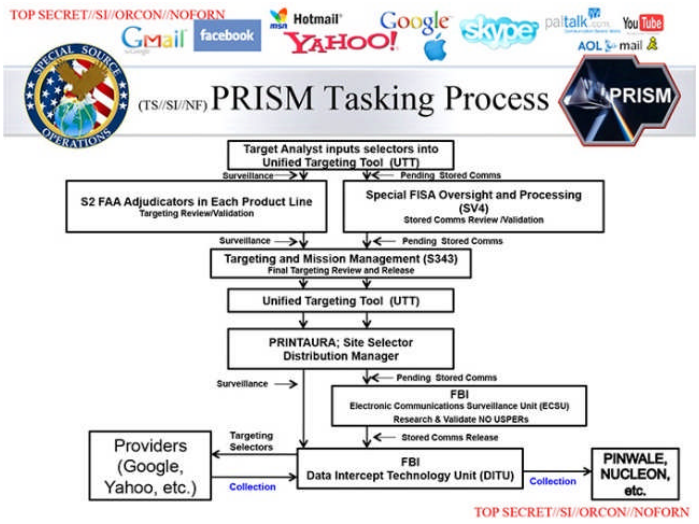
A l'attention du lecteur • Ce bulletin de veille a pour objet d'éclairer un événement marquant de l'actualité récente, d'en qualifier l'importance et d'en apprécier les conséquences éventuelles, à partir des analyses et des arguments d'experts internationaux. Les sources mentionnées ne sont en aucun cas exhaustives.

Le 31 juillet 2013, deux mois après ses révélations, l'ancien agent de la *Central Intelligence Agency* (CIA) et consultant de la *National Security Agency* (NSA) Edward Snowden obtient l'asile en Russie pour une durée d'un an. Si cet épilogue met un terme à la cavale du « lanceur d'alerte », les retentissements réels de cette affaire ne sont pas encore tous connus. Toutefois, celle-ci pose une nouvelle fois la question de la coexistence des mesures sécuritaires et des libertés individuelles dans les démocraties occidentales, et permet de mesurer l'impact considérable des NTIC sur les relations internationales, et tout particulièrement transatlantiques.

1. LES FAITS

Des « révélations ». Consultant pour le cabinet Booz, Allen & Hamilton, rattaché à la NSA et basé à Hawaï, Edward Snowden révèle le 5 juin 2013, par le biais d'une vidéo enregistrée à Hong-Kong, l'existence d'un vaste réseau d'espionnage mis en place par les Etats-Unis en 2007, et prorogé par Barack Obama jusqu'en 2015. Peu après cette révélation, plusieurs documents officiels sont diffusés dans la presse et sur Internet par Snowden lui-même, via les quotidiens anglo-saxons *The Guardian* et *The Washington Post*.

La communauté internationale apprend alors qu'un vaste programme développé par la NSA sous le nom de code *Prism* permet de surveiller des données personnelles stockées sur les serveurs des fournisseurs d'accès et des messageries Microsoft, Yahoo, Google, AOL, Skype, Youtube et Verizon, Apple, etc. Grâce à de puissants algorithmes, *Prism* est capable d'accéder simultanément au contenu des conversations téléphoniques fixes et mobiles, mails, chats, forums et aux échanges sur des réseaux sociaux tels que Twitter ou Facebook. Les requêtes sont lancées en temps réel, mais aussi de manière rétroactive car les données sont généralement conservées durant plusieurs années[1].



L'enregistrement des données par Prism.
Source image : Washington Post.

Ainsi, la NSA est en mesure de surveiller sans aucun filtre toutes les informations échangées sur le territoire étasunien, ainsi que l'ensemble des flux dirigés vers l'extérieur. Cette collecte tous azimuts tendrait d'ailleurs à considérer chaque citoyen comme un terroriste potentiel. Mais *Prism* ne constitue en réalité qu'un seul volet du programme de surveillance électronique et électromagnétique des services de sécurité américains. La police américaine dispose également de véhicules capables de scanner un certain nombre de données sur leur passage (plaques d'immatriculation, emplacements des véhicules, etc.), les drones sont de plus en plus utilisés à des fins de surveillance intérieure et les données personnelles des citoyens (fichiers bancaires, de santé, de

[1] DENECE, Eric. La dangereuse dérive de la démocratie américaine. *CF2R*, 1er août 2013. Consulté le 08/08/2013. Disponible sur : http://www.cf2r.org/fr/editorial-eric-denece-lst/la-dangereuse-derive-de-la-democratie-americaine.php

sécurité sociale, les données universitaires, fiscales et judiciaires, etc.) sont généralement peu protégées, donc facilement accessibles pour les services[2].

Des opérations de surveillance menées sur les alliés européens, notamment sur les institutions européennes, sont également dévoilées durant cette affaire. Elles auraient bénéficié du concours du centre NSA/GCHQ[3] implanté à Benhall au Royaume-Uni, et de la mise en place du projet *Tempora*[4], dont l'un des intérêts est de permettre le branchement direct sur les câbles transatlantiques de fibre optique, et ainsi de pouvoir récolter des informations en très grande quantité. Enfin, des documents sur le projet *Five Eyes*, mettant en évidence les liens étroits entre les services de renseignement américains, britanniques, australiens, néo-zélandais et canadiens, sont également divulgués dans la presse[5].

Un exil en mesure de créer une crise diplomatique. Après avoir fui Hong-Kong accompagné de la journaliste Sarah Harrison[6], Snowden se pose à Moscou le 23 juin 2013 et se réfugie dans la zone internationale de l'aéroport de Cheremetièvo. Afin d'échapper au risque de condamnation à mort pesant sur lui aux Etats-Unis, il sollicite dès le lendemain l'asile politique auprès du gouvernement équatorien, mais sa demande est rejetée. Dans le même temps, le ministre américain de la Justice, Eric Holder, assure qu'en cas d'extradition son pays n'aurait recours contre lui ni à la peine capitale, ni à la torture. Le gouvernement américain fait tout de même révoquer le passeport de l'ancien analyste, l'entravant ainsi dans ses déplacements à l'étranger[7]. Dans les semaines qui suivent, une vingtaine de demandes d'asile politique sont déposées par Snowden, dont une est adressée à la France. Seuls la Bolivie, le Venezuela et le Nicaragua y répondent favorablement. Toutefois, se retrouvant sans passeport, Snowden ne peut plus se rendre en Amérique latine. Le gouvernement russe lui accorde finalement le statut de réfugié le 31 juillet 2013, pour une durée d'un an. Moscou n'ayant passé aucun accord d'extradition avec Washington, l'analyste américain se retrouve ainsi provisoirement en sécurité, au risque de raviver les tensions diplomatiques entre Kremlin et Maison blanche[8].

2. LE CONTEXTE

La divulgation d'informations sur un réseau d'espionnage organisé par les Etats-Unis rappelle le scandale du Watergate[9], bien que le contexte actuel soit différent. Contrairement aux années 1970, ce type de révélations ne semble pas, aujourd'hui, déstabiliser le gouvernement américain, ces actes pouvant être considérés comme légitimes[10].

***Prism* : une conséquence des attentats de 2001.** Après le 11 septembre 2001, les Etats-Unis ont accru leur arsenal sécuritaire, notamment sur le plan juridique. Au cours de ces événements, les défaillances des services de renseignements ont en effet été largement soulignées par les politiques et les médias, en particulier leur incapacité à anticiper une opération d'une telle ampleur. Afin de combler ces failles, Washington s'est alors doté de la loi baptisée *USA Patriot Act*[11], votée au Congrès le 26 octobre 2001 et signée par Georges W. Bush. *Prism* découle directement de cette loi : les sections 215 et 702 de ce texte autorisent la surveillance des réseaux de télécommunications sans mandat ou ordonnance judiciaire, ainsi que la collecte d'informations portant sur des ressortissants américains et émanant des services de renseignement étrangers. Ce nouveau cadre juridique a donc ouvert la voie à une surveillance plus intense des citoyens et à une extension des écoutes vers les réseaux numériques internationaux.

Si les moyens mis à la disposition de la NSA ne sont pas connus de manière précise, il est de notoriété publique qu'ils sont colossaux, les estimations évoquant des dizaines de milliers d'employés et un budget annuel

---

[2] DENECE, Eric, *op.cit.*

[3] Un accord secret passé avec la Grande-Bretagne permet à la NSA d'accéder à toutes les informations recueillies dans le cadre du programme *Tempora*. GCHQ : *Government Communications Headquarters*.

[4] L'opération *Tempora* est principalement menée depuis 2012 par le GCHQ. Le système mis en place permet la collecte à grande échelle des données téléphoniques et provenant d'Internet. Cf. L'Expansion.com, 22 juin 2012.

[5] Snowden : The NSA and Israel wrote Stuxnet together. *Cyberwarzone*, 7 juillet 2013. Consulté le 02/08/2013. Disponible sur : http://www.cyberwarzone.com/snowden-nsa-and-israel-wrote-stuxnet-together

[6] Journaliste spécialiste du droit, employée du site internet Wikileaks.

[7] Les Etats-Unis ne requerront pas la peine de mort contre Snowden. *Le Monde.fr*, 26 juillet 2013. Consulté le 08/08/2013. Disponible sur : http://www.lemonde.fr/technologies/article/2013/07/26/les-etats-unis-ne-requerront-pas-la-peine-de-mort-contre-snowden_3454335_651865.html

[8] Prism : Edward Snowden, un mois de demandes d'asile. *Le Monde.fr*, 23 juillet 2013. Consulté le 23/07/2013. Disponible sur : http://www.lemonde.fr/technologies/article/2013/07/23/prism-edward-snowden-un-mois-de-demandes-d-asile_3451083_651865.html

[9] Affaire d'espionnage politique qui aboutit en 1974 à la démission de Richard Nixon, alors président des Etats-Unis. Les investigations par des journalistes et une longue enquête du Sénat américain ont fini par révéler l'ampleur des écoutes illégales mises en place par l'administration présidentielle.

[10] SHEVTSOVA, Lilia. Tinker, Tailor, Snowden, spy ? *Project Syndicate*, 18 juillet 2013. Consulté le 06/08/2013. Disponible sur : http://www.project-syndicate.org/commentary/what-the-snowden-scandal-revealed-about-the-state-of-western-liberal-democracies-by-lilia-shevtsova

[11] Conséquence directe des attentats du 11 septembre 2001, cette loi renforce considérablement les pouvoirs des différentes agences gouvernementales (FBI, CIA, NSA) et de l'armée américaine. Elle fut considérée comme une loi d'exception, dont certaines dispositions (seize au total) n'étaient valables que pour quatre années. Sont modifiées, entre autres, les lois sur l'immigration, les lois sur les opérations bancaires, la loi de surveillance d'intelligence étrangère (FISA). *Le Patriot Act* crée une nouvelle catégorie de crime du « terrorisme intérieur » (section 802).

d'environ 10 milliards de dollars. C'est dans ce contexte que, le 18 juin 2013, le directeur de la NSA Keith Alexander se défend des accusations portées contre le programme de son agence et contre ses moyens, en rappelant l'efficacité passée de cette dernière dans le cadre de la lutte contre le terrorisme. Ces arguments ont été rapidement repris par le général Dempsey, chef d'état-major des armées américaines, qui insiste à son tour sur la menace terroriste réelle pesant sur les Etats-Unis, notamment dans le cyberespace[12].

Cependant, si la communauté internationale et l'opinion publique semblent troublées par les informations divulguées sur la NSA, il ne s'agit pas à proprement parler de révélations. En effet, le renseignement numérique est connu de tous depuis l'affaire Echelon, révélée dans les années 1990. En revanche, l'affaire Snowden officialise l'existence des structures dédiées au renseignement électronique et permet d'en mesurer l'ampleur de manière plus précise. Les observateurs internationaux, les journalistes ou même l'opinion publique stigmatisent davantage le double discours tenu par les Américains que l'espionnage en tant que tel, qu'ils soupçonnaient déjà. Alors que Washington rappelle régulièrement à l'ordre les Chinois ou les Russes sur leur manque de respect des libertés individuelles, notamment dans l'espace numérique, les Etats-Unis se révèlent dotés d'outils de surveillance tentaculaires, où le respect de la vie privée semble là aussi ignoré[13].

Une amplification du mouvement militant des « lanceurs d'alertes ». Le principe visant à alerter l'opinion publique sur le manque de transparence du gouvernement n'est pas nouveau[14], mais il s'appuie aujourd'hui sur le respect des libertés numériques et, à ce titre, utilise la toile afin de divulguer aux millions d'internautes connectés des informations jugées sensibles[15]. Dans une vidéo diffusée sur le site du *Guardian*, Snowden affirme vouloir informer les Américains de « *ce qui est fait en leur nom et ce qui est fait contre eux* », et défendre « *les libertés essentielles et les libertés numériques* »[16], menacées selon lui par *Prism*. Avant lui, Bradley Manning[17], Aaron Schwartz[18] ou encore Julian Assange[19] ont utilisé le même procédé pour dénoncer des pratiques douteuses ou divulguer des informations classifiées ne leur semblant pas conformes aux grands principes de la démocratie, et plus particulièrement aux premier, quatrième et cinquième amendements de la Constitution américaine, censés garantir la liberté d'expression, la protection de la vie privée et le droit à un procès équitable.

Si ces militants aspirent aux mêmes idéaux (défendre un Internet libre et le droit de savoir), il semble que leurs méthodes et les enjeux visés soient à chaque fois différents. Wikileaks a diffusé des documents susceptibles de mettre en danger la sécurité du pays, puisqu'ils contiennent potentiellement des informations stratégiques majeures. Dans le cas de Snowden, les informations dénoncent une organisation étatique qui peut porter atteinte à la vie privée au nom de la sécurité. Selon Daniel Ellsberg, de la Freedom of the Press Foundation, « *Edward Snowden se trouvait dans une contradiction telle qu'il s'est senti obligé de parler* », et d'ajouter que « *le secret corrompt autant que le pouvoir* »[20].

3. LES ENJEUX

Etats-Unis : une démocratie en sursis ? Selon certains experts, les Etats-Unis semblent avoir pris peu à peu quelques distances et libertés avec ce qui constitue leur fondement, la démocratie. A ce titre, ils n'hésitent pas à parler d'Etat policier ayant une tendance au repli et à l'unilatéralisme. En évoquant le programme *Prism*, Daniel Ellberg évoque d'ailleurs une « *super Stasi internationale* »[21]. Les revendications en apparence légitimes des « lanceurs d'alertes » pointent justement les paradoxes liés à la notion même de démocratie. Lequel, de

[12] BERNARD, Philippe. Au cœur de l'Utah, les Etats-Unis déploient leurs « grandes oreilles ». *Le Monde.fr*, 12 juin 2013. Consulté le 08/08/2013. Disponible sur : http://www.lemonde.fr/ameriques/article/2013/06/12/au-c-ur-de-l-utah-les-etats-unis-deploient-leurs-grandes-oreilles_3428568_3222.html

[13] S. D. Wikileaks ou le paradoxe de la transparence : de Manning à Snowden. *Egeablog.fr*, 3 août 2013. Consulté le 3/09/2013. Disponible sur : http://alliancegeostrategique.org/2013/08/03/wikileaks-ou-le-paradoxe-de-la-transparence-de-manning-a-snowden/

[14] Daniel Ellsberg avait dans les années 1970 diffusé des « papiers du Pentagone » révélant les mensonges et l'implication militaire et politique des Etats-Unis au Vietnam. Il avait été poursuivi en justice en 1971, en vertu de l'*Espionnage Act*, pour complot, vol et diffusion illégale de documents confidentiels.

[15] ELLSBERG, Daniel. E. Snowden a bien fait de fuir. *Courrier international*, 8 juillet 2013. Consulté le 28/07/2013. Disponible sur : http://www.courrierinternational.com/article/2013/07/08/edward-snowden-a-bien-fait-de-fuir

[16] LELOUP, Damien ; SZADKOWSLI, Michaël. Prism, Snowden, surveillance : 7 questions pour tout comprendre. *Le Monde.fr*, 13 juillet 2013. Consulté le 30/07/2013. Disponible sur : http://www.lemonde.fr/technologies/article/2013/07/02/prism-snowden-surveillance-de-la-nsa-tout-comprendre-en-6-etapes_3437984_651865.html

[17] Analyste de l'armée américaine spécialisé dans le renseignement, Bradley Edward Manning transmet des documents classifiés à Wikileaks en 2010. Sous le coup de huit chefs d'inculpation criminels et de quatre violations du règlement militaire, il est condamné le 23 août 2013 à 35 ans de prison.

[18] Informaticien et militant de l'Internet, intéressé aussi par la sociologie, l'éducation civique et l'activisme, connu entre autres comme cofondateur de *DemandProgress.org* et du Progressive Change Campaign Committee, et du langage Markdown (un balisage html allégé). Le 19 juillet 2011, il est accusé d'avoir téléchargé et mis en ligne 4,8 millions d'articles scientifiques disponibles dans la base de données JSTOR6 (soit la quasi totalité du catalogue).

[19] Informaticien et cybermilitant australien connu comme fondateur, rédacteur en chef et porte-parole du site WikiLeaks. Faisant actuellement l'objet d'une demande d'extradition par la Suède, il s'est réfugié à l'ambassade d'Équateur à Londres, où il vit depuis juin 2012.

[20] ELLSBERG, Daniel, *op. cit.*

[21] SHEVTSOVA, Lilia, *op. cit.*

la transparence ou du secret, est le meilleur garant de la démocratie ? La transparence revendiquée ne risque-t-elle pas au contraire de renforcer le secret lui-même, au lieu de consolider la démocratie ? Face à la recrudescence de ce type d'affaires, les Etats sont souvent tentés de consolider les mesures de protection du secret qu'ils jugent indispensables à la démocratie[22].

Des technologies et des médias sociaux mal maîtrisés et pouvant devenir dangereux. Les nouvelles technologies de l'information et de la communication, et par extension les médias sociaux, sont devenus des armes à part entière, nécessitant une adaptation constante et, surtout, une prise de conscience globale de leur impact sur les relations internationales.

En effet, ces nouveaux médias augmentent considérablement la vitesse de propagation des informations, même les plus dangereuses. Ils offrent également des capacités de mobilisation et de coordination à l'impact immédiat (cas des manifestations iraniennes en 2009, ou lors des révoltes arabes en 2011). Par ailleurs, ils sont susceptibles de favoriser les attaques informatiques destinées à dérober de l'information ou saboter des systèmes informatiques contrôlant par exemple des systèmes d'armement. Ils peuvent aussi déstabiliser des adversaires en véhiculant de fausses informations. Cela implique que les services de sécurité cherchent à mieux contrôler la montée en puissance de ces médias sociaux encore mal maîtrisés, et bien souvent sous estimés[23]. Les gouvernements se sont d'ores et déjà fixé pour objectif de veiller, détecter et interpréter la nature des mouvements collectifs à travers le contenu des échanges et, éventuellement, anticiper les comportements, afin de contrer au mieux leur dangerosité tout en affirmant respecter les droits individuels. Cet équilibre est d'autant plus difficile à trouver que le cyberespace est aujourd'hui utilisé à des fins d'attaques asymétriques, de propagande ou de contre propagande, aussi bien par les Etats que par des groupes d'individus. Le principal obstacle étant de parvenir à faire la distinction, au sein de la masse d'information récoltée, entre les internautes *lambda* et ceux qui sont mal intentionnés.

Les pays européens où l'industrie de l'armement a une place importante, au premier rang desquels la France, craignent pour la sécurité de leurs systèmes d'armes modernes, devenus vulnérables aux cyber-attaques. Souvent développés par des entreprises nationales, ces armements sont néanmoins régulièrement modernisés par des groupes américains, ce qui les rend plus vulnérables encore à l'espionnage et aux entraves. Consciente de l'enjeu, la France entend bien résorber son retard en matière de cyberdéfense, notamment depuis les révélations sur le programme *Prism*.

Une Europe de plus en plus compétitive et menaçante ? L'affaire Snowden permet également de confirmer la complexité du monde de l'après Guerre froide, les alliés stratégiques d'autrefois étant devenus rivaux sur le plan économique. La surveillance mise au jour par l'affaire Snowden se rapproche des pratiques de l'intelligence économique agressive, et devient le révélateur d'une compétition bien réelle entre l'Europe et les Etats-Unis. Or, les débats autour de *Prism* portent avant tout sur la protection des données privées, et encore peu sur les risques et les opportunités d'espionnage industriel qui, pourtant, intéressent en priorité les services de renseignement américains dans de nombreux domaines (énergie, défense, aéronautique, télécommunications, etc.). A travers cette affaire, la puissance américaine dévoile ainsi ses craintes face à des entreprises européennes considérées désormais comme de plus en plus menaçantes[24].

Cependant, depuis cette annonce, aucune mesure de rétorsion n'a été prise de manière concrète contre les Etats-Unis ; ses relations avec les pays européens ne semblent même pas en pâtir. Sans aller jusqu'à la rupture de l'alliance transatlantique, l'Europe s'est retrouvée ces derniers mois en position de force et aurait pu tirer profit de ces révélations pour peser davantage, par exemple, dans le cadre des négociations entamées en juillet 2013 sur la création d'une zone de libre-échange, mais elle n'en a rien fait. Les désaccords récurrents existant entre Etats membres expliquent sans doute que certains d'entre eux affichent un soutien sans faille à Washington, tandis que d'autres semblent au contraire vouloir prendre des distances avec leur allié traditionnel. A ce titre, le refus du survol de l'avion bolivien en France, alors que des rumeurs évoquaient la présence de l'ancien cadre de la NSA à son bord, a été très mal perçu en Amérique latine. Selon certains observateurs, la France semble avoir manqué une occasion de marquer son indépendance et d'afficher sa détermination vis-à-vis des Etats-Unis[25].

Ainsi, l'affaire Snowden fait figure de révélateur des bouleversements atteignant aujourd'hui les équilibres internationaux. A l'avenir, l'enjeu sera donc de parvenir à réajuster l'approche de la sécurité nationale sans chercher à trouver les moyens de mieux dissimuler les méthodes employées, au risque sinon d'attiser les tensions entre Etats et d'encourager une surenchère sécuritaire à l'échelle mondiale.

---

[22] S. D. Wikileaks ou le paradoxe de la transparence : de Manning à Snowden, *op. cit.*

[23] Cf. Cyberespace & cyberdéfense. *CDEM*, Fiche de synthèse n° 1, juillet 2012. Consulté le 24/09/2013. Disponible sur : http://www.cdem.defense.gouv.fr/IMG/pdf/cyberespace_cyberdefense.pdf

[24] MAZZUCCHI, Nicolas. Prism, Golem des Etats-Unis. *Polemos.fr*, le 3 juillet 2013. Consulté le 25/07/2013. Disponible sur : http://www.polemos.fr/2013/07/prism-golem-des-etats-unis/

[25] BONIFACE, Pascal**.** Affaire Snowden / Espionnage : quel impact sur les relations transatlantiques ? *Affaires-strategiques.info*, 9 juillet 2013. Consulté le 27/09/2013. Disponible sur : http://www.affairesstrategiques.info/spip.php?article8438