USA, surveillance, renseignement, sécurité nationale et cyberespace

Daniel Ventre, CNRS (CESDIP/GERN). Titulaire de la Chaire Cybersécurité & Cyberdéfense

Avril 2015, Article III.22

Cet article de synthèse présente quelques-unes des récentes informations relatives aux stratégies américaines en matière de sécurité nationale, de surveillance et de renseignement. L'évolution des enjeux, les lectures des menaces évolutives, appellent à la redéfinition constante de cadres stratégiques, juridiques, et à une évolution des institutions elles-mêmes.

I – La stratégie de sécurité nationale américaine

La Maison Blanche a publié en février 2015 sa nouvelle stratégie de sécurité nationale (National Security Strategy. The White House. February 2015)[1].

Les Etats-Unis mettent en avant dans ce document leur puissance, celle qui sait surmonter toutes les difficultés, celle qui a par exemple stoppé la crise financière internationale la plus grave depuis la grande dépression (1929) et qui depuis 6 ans a renoué avec la croissance.

Dans ses lignes dédiées à la cybersécurité, le document rappelle que :

- La menace de cyberattaques majeures ne cesse de croître. La cybersécurité est au rang des défis les plus sérieux pour la sécurité nationale.
- La cybersécurité est l'un des enjeux pour lesquels les Etats-Unis se doivent d'exercer un leadership. La communauté internationale sera capable de traiter ces risques (cybernétiques et autres) uniquement si les grandes puissances s'impliquent. L'Amérique assume par exemple son leadership mondial en définissant des standards de cybersécurité applicables à tous (« *We are shaping global standards for cybersecurity* ») et des capacités internationales pour contrer les cybermenaces. Les Etats-Unis étant le berceau de l'internet, les Etats-Unis ont une responsabilité particulière (p.12) pour diriger, guider, orienter (« lead ») un monde en réseau. Les Etats-Unis aideront d'autres nations à créer leur cadre juridique (« *we will assist other countries to develop laws* »).
- Pour affirmer sa détermination l'Amérique poursuit la construction de sa cybersécurité, notamment en renforçant la sécurité et résilience de ses infrastructures critiques, mais aussi en poursuivant les auteurs des cyberattaques et en les sanctionnant, en leur faisant payer le prix (« *impose costs on malicious cyber actors* »), y compris (et donc pas seulement ?) en les portant devant des tribunaux (« *including through prosecution of illegal cyber activity* »). La

1 [https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf]

Chine est spécifiquement visée (p.24) par ces mesures et cette détermination à protéger les intérêts américains contre les atteintes émanant de l'étranger.

II – Le renseignement : ses stratégies, ses analyses et ses acteurs

2.1. Stratégie et lois pour le renseignement

James R. Clapper, directeur du renseignement national (Director of National Intelligence - DNI), a rendu public en septembre 2014[2] le rapport intitulé « The National Intelligence Strategy of the United States of America. 2014 »[3].

Le « cyber » y est bien sûr omniprésent :

- Le cyber-renseignement est l'une des missions centrales du renseignement (avec le contre-terrorisme, la contre-prolifération…)
- L'objectif du cyber-renseignement est de fournir du renseignement sur les cyber-menaces (p.6)
- Le cyber-renseignement est « la collecte, le traitement, l'analyse et la diffusion d'information de toutes les sources de renseignement sur les cyber programmes d'acteurs étrangers, leurs intentions, leurs capacités, leurs activités de recherche et développement, leurs tactiques, leurs activités opérationnelles et indicateurs ; leur impact ou effets potentiels sur la sécurité nationale, les systèmes d'information l'infrastructure, les données ; la caractérisation des réseaux, ou une analyse des composantes, structures, usages et vulnérabilités des systèmes d'information étrangers » (p.8)

En 2014, deux lois ont été votées aux Etats-Unis, sur le renseignement :

- L'Intelligence Authorization Act (IAA) FY 2014 (P.L. 113-126), votée en juillet 2014[4]
- L'IAA (FY2015), P.L. 113-293, votée en décembre 2014[5].

Du texte voté en juillet 2014, nous retiendrons le Titre VI, sur les donneurs d'alerte et notamment la section 601, qui prévoit d'accorder une protection aux donneurs d'alerte dans la communauté du renseignement (question déjà prise en compte dans le Whistleblower Protection Act – ICWPA[6]) de 1998)[7]. Celle-ci prévoit qu'aucune sanction, forme de représailles ne peut être prise à l'encontre d'un employé qui aura signalé, dans le respect du cadre réglementaire, une information au DNI (Director of National Intelligence), ou à l'inspecteur général de la communauté du renseignement (Inspector General of the Intelligence Community). Le texte énumère la liste des personnes autorisées à recevoir les alertes. Pour autant, ces assurances accordées aux lanceurs d'alertes empêcheront-elles que de nouveaux individus ne volent des informations classifiées ?

Du texte voté en décembre 2014 nous retiendrons la section 309, sur la conservation des données de citoyens américains, acquises dans la cadre d'enquêtes menées auprès de personnes étrangères. Le texte prévoit que les données des communications interceptées ne pourront pas être conservées plus de 5 ans, sauf dans certains cas :

- si la communication constitue un acte d'espionnage, ou si elle est nécessaire pour comprendre ou évaluer le renseignement étranger ;
- si la communication est un élément de preuve de crime ;
- si la communication est chiffrée ;
- si on peut raisonnablement penser que l'information a un sens secret ;

2 [http://www.dni.gov/index.php/newsroom/reports-and-publications/204-reports-publications-2014/1114-dni-unveils-2014-national-intelligence-strategyDNI%202014]

3 [http://www.dni.gov/files/documents/2014_NIS_Publication.pdf]

4 [https://www.congress.gov/bill/113th-congress/senate-bill/1681/text]

5 [https://www.congress.gov/113/bills/hr4681/BILLS-113hr4681enr.pdf]

6 [https://www.law.cornell.edu/topn/intelligence_community_whistleblower_protection_act_of_1998]

7 [Ce texte définit la procédure que doivent suivre les employés de la DIA, NGA, NRO et NSA pour rapporter des faits qu'ils jugent importants, au comité du renseignement du Congrès. Cette loi a été complétée par la Presidential Policy Directive 19 (PPD-19) de B. Obama en 2012.]

- s'il y a de bonnes raisons d'estimer que toutes les parties de la communication sont non-américaines ;
- si la conservation est nécessaire à la protection contre des menaces imminentes

La section 312 de cette loi traite de la coopération avec l'Ukraine en matière de cybersécurité et lutte contre la cybercriminalité. Elle prévoit d'aider l'Ukraine à développer ses capacités de lutte contre la cybercriminalité, y compris renseignement et justice, et de rapprocher les procédures et outils américains et ukrainiens, notamment pour faciliter l'extradition de cybercriminels ukrainiens vers les Etats-Unis lorsque des citoyens américains en sont victimes.

La dernière section du texte, section 331, demande la publication d'une étude afin d'envisager la formation à la cybersécurité de vétérans et retraités des agences de renseignement américaines.

Une analyse de ces deux textes de loi est proposée par Anne Daugherty Miles, dans un rapport publié par le Congrès en janvier 2015[8].

2.2. Evaluation des cybermenaces par le renseignement américain

Le 26 février 2015, la communauté du renseignement américain (US Intelligence Community) a proposé son évaluation de la menace, par le biais d'un rapport signé James R. Clapper (Director of National Intelligence): « Worldwidethreat Assessment of the US Intelligence Community »[9].

Ce document relativement court (25 pages) identifie et analyse les principales menaces à la sécurité nationale américaine. Il classe ces dernières en deux grandes catégories : les menaces globales et les menaces régionales.

La cybermenace vient en premier rang des menaces globales (devant le renseignement, le terrorisme, les armes de destruction massive, l'espace, le crime organisé transnational, les ressources économiques et naturelles, la sécurité humaine). De ces cybermenaces il est dit :

- Qu'elles pèsent sur la sécurité nationale et la sécurité économique
- Qu'elles ne cessent de croître (en fréquence, échelle, sophistication, sévérité d'impact, nombre d'acteurs impliqués, variété de méthodes d'attaques, de systèmes ciblés, en nombre de victimes)
- Les réseaux qui traitent l'information non classifiée du gouvernement, de l'armée, mais aussi de l'industrie et plus largement de la société, demeurent fragiles, vulnérables, notamment à l'espionnage et aux perturbations
- De plus en plus d'Etat attaquent le secteur industriel américain pour soutenir leurs propres objectifs économiques
- Qu'elles ne peuvent pas être éliminées, car trop nombreuses. Il faut donc apprendre à gérer le risque. Les méthodes de calcul et gestion des risques utilisés par certaines entreprises doivent être redéfinies pour prendre en compte des variables telles que la cybermenace étrangère (entendre ici provenant directement de gouvernements étrangers) ou les interdépendances systémiques entre secteurs d'infrastructures critiques.
- Les cyberattaques à des fins politiques sont un phénomène croissant.
- Parmi les Etats acteurs de la cybermenace, sont aux premiers rangs la Russie (qui crée son cyber commandement), la Chine (espionnage économique), l'Iran (pour exercer des représailles contre ses ennemis politiques), la Corée du Nord (à des fins politiques) et le terrorisme (avec des attaques menées par des sympathisants des groupes terroristes, pour attirer l'attention des médias).

Plus intéressants toutefois sont les arguments suivants :

8 [Anne Daugherty Miles, Intelligence Authorization Legislation for FY2014 and FY2015 : Provisions, Status, Intelligence Community Framework, Congressional Research Service, January 14, 2015, http://fas.org/sgp/crs/intel/R43793.pdf]

9 [http://cdn.arstechnica.net/wp-content/uploads/2015/02/Clapper_02-26-15.pdf]

- **La probabilité d'une attaque majeure** (« catastrophic attack ») **est faible**. Cette vision est assez différente des discours officiels sur la menace (gouvernement, NSA, industriels, etc.) Il réfute l'hypothèse d'un très prochain Cyber Armageddon et propose d'autres scénarios plus probables selon lui. Il envisage plutôt des séries d'attaques de niveau faible à modéré, provenant de multiples sources, qui vont finir par coûter cher (« *will impose cumulative costs* ») à l'économie américaine, sa compétitivité, et sa sécurité nationale. Car c'est cette multiplication des sources, des moyens, des cibles, qui va contraindre l'Amérique à sécuriser, défendre tous ses systèmes, et non pas quelques-uns en particulier.
- **La non attribution sera de moins en moins la règle**. Gouvernement et entreprises font des progrès importants en matière de détection et attribution, et il semblerait que ce point technique, qui accordait à l'attaquant un avantage considérable, soit en passe d'être remis en cause. Les hackers ne peuvent plus s'estimer intouchables, indétectables, non identifiables (p.2 du rapport).
- **Le cyberespace restera encore assez longtemps un espace permissif**. Jusqu'alors les victimes de cyberattaques ont répondu timidement, confortant les agresseurs dans la possibilité d'utiliser le cyberespace à des fins coercitives.
- Le cyberespionnage porte atteinte à la confidentialité ; les attaques DDoS portant atteinte à la disponibilité des données ; mais à l'avenir nous pourrions voir davantage d'actions qui modifieront, manipuleront l'information, **compromettant cette fois l'intégrité de l'information**.

2.3. La NSA et ses défis

Pour lutter contre le terrorisme, la NSA estime ne pouvoir faire autrement que d'accéder à l'ensemble des communications. De leur côté les défenseurs des libertés individuelles affirment que la sécurité nationale ne peut pas tout légitimer, et surtout pas les atteintes à la vie privée, aux données personnelles, et autoriser la surveillance de tout un chacun sans que ne soient établies des limites strictement respectées. Dialogue de sourd entre les deux camps. Les choix d'industriels (Apple, Google) désireux de proposer des outils de cryptage (pour smartphones, tablettes), supposés assurer aux utilisateurs une totale confidentialité de leurs échanges, auront suscité de multiples réactions. Parmi lesquelles celles de la NSA, qui par la voix de son patron, l'Amiral Michael Rogers, a exprimé sa position[10]: il faut que la NSA puisse accéder, lorsque cela est nécessaire, aux communications et impérativement à celles des mobiles cryptés. Sa position rejoint celle du directeur du FBI, James Comey[11].

Michael Rogers demande que les moyens pour remplir sa mission lui soient accordés. L'accès aux communications cryptées fait partie de ces moyens. Il faut pour cela que soit défini un cadre juridique précis, auquel la NSA se conformera, comme elle l'a toujours fait jusqu'alors, affirme-t-il :"*We fully comply with the law … We do that foreign intelligence mission operating within (a legal) framework*"[12].

Si le directeur de la NSA a, à de multiples reprises, exprimé publiquement son attachement au respect du cadre juridique qui contraint son action, rappelons toutefois que ce rapport à la loi ne va pas de soi. Le Président B. Obama lors d'un entretien accordé à BC's Fusion network13[4] en octobre 2013 réaffirmait la nécessité de contrôler davantage l'action de l'agence : "*We give them policy direction," Obama said. "But what we've seen over the last several years is their capacities continue to develop and expand, and that's why I'm initiating now a review to make sure that what they're able to do, doesn't necessarily mean what they should be doing."*

Au travers des multiples débats impliquant l'agence de renseignement, plusieurs questions doivent être analysées (mais il y en a d'autres…) :

- Le rapport de la NSA au droit (quel cadre, quel respect, quel contrôle de la conformité, quel respect des valeurs…)
- Le rapport de la NSA au pouvoir politique

10 [http://securityaffairs.co/wordpress/34071/intelligence/nsa-director-rogers-legal-framework.html]

11 [http://www.presstv.ir/Detail/2015/02/24/398934/NSA-defends-access-to-encrypted-devices]

12 [http://www.globalpost.com/dispatch/news/afp/150223/nsa-chief-seeks-compromise-encrypted-phone-snooping]

13 [http://www.reuters.com/article/2013/10/28/us-usa-security-idUSBRE99Q07E20131028]

- Le rapport de la NSA à l'industrie
- La résolution du dilemme qui semble opposer sécurité et droits fondamentaux. Y a-t-il un équilibre optimum ? Toute concession en faveur des droits fondamentaux se traduit-elle nécessairement par une réduction de la sécurité ?
- La perception qu'ont les citoyens (entreprises, élus, pouvoir politique, etc.) du renseignement et dont dépendent, d'une certaine manière, les capacités d'action des agences.

Donnant suite à une série de plaintes déposées par des groupes de défense des libertés et des droits de l'homme, consécutivement aux révélations Snowden, l'Investigatory Powers Tribunal britannique (créé en 2000) vient de juger[14] illégaux les échanges de données entre la NSA et le GCHQ. Il est reproché au GCHQ d'avoir obtenu des informations sur les citoyens britanniques auprès de la NSA (contournant ainsi les normes juridiques protectrices des individus), laquelle collecte les données de millions d'individus de par le monde via ses projets PRISM et Upstream. Cet usage de données de la NSA est jugé illégal car contraire à la convention européenne des droits de l'homme[15]. La démarche aurait contraint les agences de renseignement à expliquer les mesures prises en matière de sécurité et usages des données. Amnesty International se félicite[16] en tous cas de cette victoire sur les agences de renseignement, et leurs pratiques de surveillance que les enjeux de sécurité nationale ne sauraient toujours légitimer. Mais le jugement va-t-il véritablement modifier la nature des échanges entre les agences britanniques et américaines ? Va-t-il clarifier les pratiques, permettre de les encadrer ? Rend-il désormais les échanges entre agences britanniques et américaines plus légaux pour autant ? Le jugement change-t-il quelque chose, fondamentalement ?

2.4. Les restructurations au sein de la CIA

Selon un article qui vient d'être publié par le Washington Post (23 février 2015)[17] la CIA envisage d'étendre ses capacités de cyberespionnage, Le directeur de la CIA, John Brennan, envisagerait le renforcement des capacités de cyberespionnage de l'agence. Cette expansion s'intègre dans un projet plus large de restructuration et de modernisation de l'agence. Le recours au cyber est appelé à devenir plus systématique, pour s'intégrer dans chacune des catégories d'opérations de la CIA (identification, recrutement d'informateurs, confirmer les cibles pour les frappes de drones, etc.) L'un des projets les plus importants évoqués – mais non confirmé - , outre cette systématisation de l'usage du cyber, réside dans la création d'une nouvelle direction cyber, au même niveau que les branches d'analyse ou d'opérations clandestines (l'agence comprend actuellement 4 services[18] qui devraient eux-aussi faire l'objet d'une refonte de leur modèle de fonctionnement et d'organisation). Ainsi la fonction Humint qui est celle traditionnelle de la CIA, ne peut-elle s'exercer sans maîtrise du cyberespace. Il y a nécessairement dans cette stratégie une volonté de réaffirmation des positions vis-à-vis de la NSA (ne serait-ce que pour solliciter l'octroi de crédits plus importants). La dernière grande réforme structurelle de l'agence remonte à la période post-11 septembre 2001. Les tensions, résistances à cette restructuration se font sentir : le directeur des opérations clandestines a démissionné récemment.

Les capacités cyber de la CIA se trouvent au sein de :

- L'Information Operations Center (IOC)[19] (qui serait le second centre le plus important en taille, juste derrière le centre dédié au contre-terrorisme) ayant succédé au Clandestine Information Technology Office créé en 1996[20])
- L'Open Source Center – OSC (renseignement sur sources ouvertes) que l'agence supervise (unité de renseignement créée en 2005).

14 [http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf]

15 [http://www.wired.com/2015/02/uk-tribunal-declares-nsas-data-sharing-british-intel-illegal/]

16 [http://www.amnesty.org/fr/for-media/press-releases/uk-historic-surveillance-ruling-finds-intelligence-sharing-illegal-2015-02-]

17 [http://www.washingtonpost.com/world/national-security/cia-looks-to-expand-its-cyber-espionage-capabilities/2015/02/23/a028e80c-b94d-11e4-9423-f3d0a1ec335c_story.html]

18 [https://www.cia.gov/about-cia/todays-cia]

19 [https://www.cia.gov/offices-of-cia/intelligence-analysis/organization-1/ioc-ag.html]

20 [http://intellworld.blogspot.fr/2009/06/linformation-operations-center-de-la.html]

Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Téléphone: 01-45-55-43-56 - courriel: contact@chaire-cyber.fr; SIRET N° 497 802 645 000 18
La chaire remercie ses partenaires