Wikileaks: causes et conséquences

cahier de la pensée mili-Terre

le Lieutenant-colonel LEGRAND

publié le 02/08/2018

Histoire & stratégie

Le 25 avril dernier, le New York Times **a publié un article analysant des documents classés «secret» par le DoD[1]. Ces documents, appelés DAB[2], sont des rapports établis sur les différents détenus de la prison de Guantanamo, entre 2002 et début 2009. Le Pentagone a condamné aussitôt la révélation de ces informations, en mettant notamment en avant les impératifs de sécurité nationale. La source de ces fuites est une fois de plus le site Internet « wikileaks », qui avait déjà stupéfait le monde fin juillet 2010 en mettant en libre circulation 75.000 pages de documents classifiés, relatifs à l'activité des forces américaines en Afghanistan.**

[1] Department of Defense

[2] Detainee's Assessment briefs

Les documents, dérobés par quelqu'un qui avait le niveau d'habilitation requis, dévoilaient alors des rapports quotidiens de plusieurs unités, donnant ainsi une idée claire des opérations américaines de 2004 à 2009. On y trouvait également des rapports dévoilant la frustration américaine à propos de l'aide secrète apportée par le Pakistan aux insurgés. Les documents révélaient les dates, les heures, les noms des unités, la localisation géographique ainsi que parfois les noms des Afghans ayant travaillé avec les Américains. Alors que le Pentagone avait sommé le site de retirer ces documents et de ne pas en divulguer 15.000 autres classifiés qui mettraient en danger non seulement des Américains mais également de nombreux Afghans, WikiLeaks réitéra en octobre 2010 en divulguant ainsi près de 400.000 pages de documents classifiés sur la guerre d'Irak. Enfin, en décembre 2010, le site dévoila de nombreux câbles diplomatiques, échangés entre le Département d'État et ses missions diplomatiques à travers le monde.

Ce n'est finalement que grâce à une dénonciation que l'on apprend que les fuites seraient l'œuvre d'un Militaire du rang (Private First Class), Bradley Manning, un ancien analyste renseignement de l'Army déjà soupçonné d'avoir livré au site une vidéo qui montrait un

hélicoptère Apache tuant deux employés de l'Agence Reuters.

Dans quelles conditions un simple Militaire du rang a-t-il pu avoir accès et dérobé autant de documents classifiés?

Après une analyse des causes[1], le présent article développera les principales conséquences de cet «événement».

Causes de l'affaire Wikileaks

- Contexte
    - Manning, 23 ans, un coupable improbable?

Simple militaire du rang, Bradley E. Manning a reçu une formation d'analyste renseignement et était habilité Top secret: si cela peut déjà sembler surprenant pour un Français, il convient de préciser que pour l'Army, engagée en Irak et en Afghanistan, c'est un cas assez courant, compte tenu du besoin énorme en analystes.

Déployé en Irak en 2009 avec la 2ème BCT de la 10th Mountain Division, Manning n'est donc pas un espion mais bien un simple Private First Class qui a opéré depuis un petit camp avancé en Irak. De nombreuses voix se sont élevées aux États-Unis pour dénoncer dans un premier temps le fait qu'un soldat si jeune puisse, depuis le milieu du désert et à l'aide de seulement quelques ordinateurs, avoir accès et ensuite télécharger autant de documents classifiés. Ensuite, comment a-t-il pu rester actif aussi longtemps sans être soupçonné? En effet, son arrestation n'a pu intervenir que grâce au témoignage d'un ex-pirate informatique[2], auprès duquel Manning s'était confié.

Mais dans le monde militaire moderne d'aujourd'hui, où l'information joue un rôle capital, il semble plus facile qu'on ne le pense, selon les témoignages de nombreux officiels du renseignement, d'avoir accès et de diffuser des documents classifiés.

- Un emploi facilitateur

Le travail de Manning consistait à s'assurer que les autres analystes renseignement dans son groupe aient accès à toute l'information nécessaire, y compris les flux de renseignements entrants, provenant du monde entier. Il s'agit concrètement de l'accès au réseau JWICS[3], le réseau du DoD véhiculant l'information classifiée Top Secret. Manning avait aussi accès à un autre réseau d'information appelé SIPRNet[4], réseau classifié secret créé en 1995, destiné à l'origine au Pentagone mais ouvert aux différents départements et agences depuis les attentats du 11 Septembre 2001. C'était en effet un des progrès majeurs réalisés dans le domaine du partage du renseignement sous l'impulsion de la Commission du 11 Septembre qui avait tiré les enseignements des attentats terroristes notamment dans le domaine de l'accès au renseignement inter-agences.

En faisant des requêtes à l'aide de mots clés et en ayant une connaissance suffisante de la nomenclature usuelle, tout analyste renseignement peut ainsi avoir accès, de n'importe où, à toute information de son niveau d'habilitation. Les informations ou renseignements de niveau Top Secret ne peuvent pourtant pas normalement être prélevées des ordinateurs facilement. Pour transférer de l'information de SIPRNet à des réseaux non classifiés, des analystes comme Manning utilisent des ordinateurs propriétaires appelés SNAP[5]. Environ 1.500 ordinateurs SNAP sont déployés en Irak et en Afghanistan, selon la compagnie qui les fabrique, TeleCommunications Systems.

Selon un utilisateur du système, SNAP permet à l'utilisateur de transférer en toute sécurité des données d'un réseau classifié à un réseau non-classifié et vice-versa. L'utilisateur peut ensuite transférer les données sur un support amovible, les graver sur un CD ou tout simplement les envoyer par e-mail. Il est également essentiel de savoir que les câbles diplomatiques sont transmis par e-mail sur des réseaux sécurisés et stockés sur des serveurs jusqu'à leur destruction[6]. Les câbles et les comptes-rendus d'incidents provenant du terrain sont stockés sur les serveurs sous la forme de fichiers PST[7], archives d'e-mail que Microsoft Outlook utilise pour compresser et stocker les données.

- Comment Manning a-t-il pu réussir à avoir accès aux câbles diplomatiques? Ils sont transmis en fait par e-mail sous forme de fichier PDF sur un réseau du Département d'État appelé ClassNet, mais stockés sous forme de fichiers PST sur des serveurs auxquels un analyste habilité peut accéder à l'aide d'une requête. Ainsi, si l'unité de Manning avait besoin de savoir si des insurgés se procuraient de nouvelles armes auprès de l'Iran, l'information pouvait être contenue dans un câble diplomatique. Un analyste peut alors télécharger un fichier PST comprenant les câbles, les ouvrir, les transférer sur un ordinateur SNAP, les placer ensuite sur un support amovible et ensuite effacer l'historique du mouvement de fichiers sur le serveur. Il convient de rappeler que lors de la guerre d'Irak les téléchargements de quantités phénoménales de données sont monnaie courante et qu'il est difficile de déceler une conduite suspecte dans un tel contexte.

Manning aurait a priori commencé à alimenter WikiLeaks en informations au cours de l'automne 2009 et son accès aux ordinateurs n'a été coupé que fin mai 2010. Comment Manning a-t-il pu procéder aussi longtemps à ces téléchargements de fichiers sans qu'un système de sécurité quelconque ne donne l'alerte?

Pourtant, un tel système existait mais n'était tout simplement pas activé.

- Les failles du système de sécurité
- Un logiciel d'alerte était en effet en place mais désactivé. Lorsque la société BAE Systems et son sous-traitant Mc Afee ont été choisis en 2006 pour installer un système de sécurité sur des milliers d'ordinateurs du DoD, la technologie visait à stopper les menaces extérieures: agents de renseignement étrangers, pirates ou hackers voulant répandre des virus ou des malware dans les réseaux du Ministère.

Le logiciel HBSS[8] établissait des liens numériques entre les personnels responsables de la sécurité du réseau et les ordinateurs classifiés utilisés par les troupes et les analystes renseignement. Les personnels de la sécurité pouvaient ainsi contrôler à distance les ordinateurs pour s'assurer que la base de données antivirale était à jour et qu'il n'y avait aucun malware dans les ordinateurs.

Les responsables du DoD étaient tellement obnubilés par des intrusions qu'un logiciel pouvant alerter les autorités sur des téléchargements importants a été ajouté à HBSS en 2008, mais jamais autorisé et activé selon une source officielle.

Le logiciel Mc Afee faisait partie d'une amélioration plus large visant à donner aux responsables de la sécurité la possibilité de désactiver des ports de données sur des ordinateurs distants, en cas d'offensive d'un malware. Le Pentagone n'a pas encore

confirmé si HBSS était dans l'ordinateur utilisé par le suspect dans cette affaire, le 1ère classe Bradley Manning.

- Une focalisation sur les menaces extérieures

Des experts se sont émerveillés que des câbles du Département d'État se répandent sur Internet par le fait d'une seule personne pouvant avoir subtilisé autant d'informations SIPRNet sans déclencher une alerte dans tout le réseau. Quelques systèmes de surveillance étaient certes en place, mais seulement à quelques endroits. En outre, même si le logiciel HBSS était installé sur l'ordinateur de Manning, cela ne faisait aucune différence car la détection de perte de données n'était pas activée. La sécurité était en fait axée sur les menaces extérieures depuis les attaques de 2008 qui avaient ébranlé US Central Command: une tête de pont numérique avait été introduite à partir de laquelle des données pouvaient être transmises à des serveurs contrôlés par des services étrangers. Le Pentagone avait alors lancé l'Opération «Buckshot Yankee» afin de résoudre le problème. Beaucoup de responsables de la sécurité voulaient la possibilité de désactiver à distance les ports des médias amovibles, particulièrement les ports USB. Mc Afee a alors conçu un additif à HBSS permettant de désactiver les ports. Cependant, les Américains étant focalisés par les menaces extérieures, le logiciel d'alerte de téléchargement n'a pas été activé.

Une des nombreuses questions que suscite cette affaire pourrait être celle posée par un haut responsable du renseignement «Est-ce qu'un 1ère classe d'un bataillon d'infanterie en Irak doit être capable d'accéder à des câbles d'Europe de l'Est?». SIPRNet, après le 11 septembre 2001, a été peu à peu transformé par le gouvernement américain en un forum ouvert aux individus habilités, afin qu'ils puissent partager du renseignement et réfléchir puis échanger par e-mail sur des problèmes renseignements concrets. SIPRNet est devenu ainsi une sorte d'équivalent d'un Internet classifié complété par des sites.

Les conséquences

- Les mesures immédiates
- L'affaire WikiLeaks ayant mis en évidence plusieurs dysfonctionnements en termes de sécurité, l'Army a pris dès la fin de 2010 une série de mesures fermes visant à éviter qu'un tel fait se reproduise.

- L'Army a demandé ainsi à toutes les unités de réévaluer leurs mesures de sécurité et de limiter les droits administrateur. Elles doivent aussi désactiver les ports CD et USB, pour ne pas permettre trop facilement une copie de données. Les militaires du rang ne doivent avoir accès qu'à des données peu confidentielles;

- L'Army a réitéré l'interdiction d'avoir avec soi tout appareil électronique ou logiciel personnel dans une enceinte gouvernementale. En outre, les soldats ne doivent utiliser que les méthodes réglementaires pour tout transfert de données entre des ordinateurs ou réseaux de classification différente;

- Une réglementation de sécurité, remise à jour, a été publiée en octobre 2010, mettant notamment en exergue une liste d'indicateurs susceptibles de révéler un risque d'espionnage, de terrorisme et de menaces internes. Portant le nom d'«AR 381-12, Subversion et Espionnage contre l'US Army», elle est applicable depuis le 4 novembre 2010. Les signes comportementaux listés dans le manuel ont été tirés de faits réels, de soldats ou employés de l'Army qui ont divulgué illégalement des informations;

- Toutes les unités doivent désormais procéder à des contrôles inopinés, notamment dans les installations les plus sensibles. Il est également exigé que les unités revoient leurs façons de combattre les menaces internes et fassent respecter les procédures réglementaires. Les chefs de corps doivent envoyer, régulièrement, un rapport;

    - Les mesures techniques envisagées

- Un nouveau rôle pour HBSS?

L'affaire WikiLeaks a incité le Pentagone à donner un nouveau rôle à HBSS, pour lutter également contre les menaces internes.

Il est probable que HBSS et un logiciel de prévention contre la perte de données seront parmi les points principaux du plan de l'administration OBAMA suite à l'affaire WikiLeaks. Dans son unique commentaire détaillé sur cette affaire, le Pentagone a souligné que HBSS est désormais installé sur 60% des ordinateurs du DoD reliés au réseau d'où la fuite est venue, le SIPRNet.

Même avant le dernier incident WikiLeaks, les officiels de la défense élaboraient un appel d'offres pour déterminer le prochain fournisseur du successeur de HBSS, le contrat actuel expirant en août 2011. Les mesures prises par la Maison Blanche, en plus de la prévention contre la perte de données, devraient porter sur le renforcement de la sécurité: authentification à l'accès, système d'alerte et des technologies pour compartimenter l'accès à l'information secrète, sans pour autant compromettre le partage du renseignement en vigueur depuis le 11 septembre 2001. En fait WikiLeaks ne fait qu'accélérer des mesures déjà envisagées.

Après le dernier incident WikiLeaks, le Pentagone a annoncé qu'il avait étendu le logiciel de contrôle des ports aux ordinateurs de Central Command. Cependant, pour beaucoup, désactiver les ports USB ou lecteurs CD-DVD ne semble pas être l'option à privilégier: ils sont en effet nécessaires pour que beaucoup de personnes fassent leur travail. En effet, les trois principaux réseaux de la communauté du renseignement[9] sont séparés les uns des autres et les analystes renseignement ont forcément besoin de déplacer des données non classifiées pour les placer par exemple dans un rapport classifié.

- Le partage du renseignement remis en question?

Beaucoup de hauts responsables du renseignement craignent encore une sur-réaction suite à l'affaire WikiLeaks, et notamment que toutes les avancées accomplies en terme de partage du renseignement soient remises en question. Dans la communauté renseignement en général, de nombreux témoignages faisaient référence à la crainte d'un retour à l'époque où il fallait «montrer patte blanche» pour la moindre requête. Même si cela ne semble pas être le cas, beaucoup d'officiels militaires comme industriels attendent néanmoins des changements dans la façon de partager le renseignement. Le Département d'État a ainsi presque immédiatement fermé ses sites SIPRNet, ce qui n'est qu'une solution temporaire, les analystes ayant besoin d'y accéder pour leurs rapports.

Les déclarations des responsables américains laissent entendre qu'une plus grande attention sera portée à ceux qui utilisent SIPRNet et surtout comment ils l'utilisent. Protéger les secrets sans pour autant sacrifier le partage du renseignement va devoir nécessiter des solutions techniques et politiques qui, à long terme, vont coûter cher, selon un général américain.

Une des solutions pourrait venir de l'agence DARPA[10] qui a fait récemment connaître

une initiative visant à développer un logiciel qui identifierait et expulserait les personnes dérobant des secrets des réseaux classifiés. Le Cyber Insider Threat program ou CINDER augmenterait la précision, le taux et la vitesse de détection des menaces internes et empêcherait les adversaires d'opérer en toute impunité dans les réseaux militaires et gouvernementaux. Ce programme, dirigé par un ancien hacker, Peiter "Mudge" ZATKO, désormais responsable chez DARPA, était en gestation mais est devenu une priorité depuis l'affaire WikiLeaks.

- Une affaire qui dérange?
- Ou un ensemble d'affaires qui dérange?

L'affaire WikiLeaks est devenu au fil du temps «les affaires» WikiLeaks: le site fait la une des grands journaux environ tous les deux mois depuis juillet 2010, plongeant à chaque fois le Pentagone et la Maison Blanche dans l'embarras, tant les révélations sont croustillantes.

En outre, les fuites révélées par WikiLeaks interviennent dans un contexte déjà marqué par d'autres affaires récentes, qui ont porté une atteinte sérieuse à la crédibilité des services de renseignement américains. Ainsi, alors que l'affaire des documents classifiés dévoilés par ce site prenait déjà une ampleur considérable en 2010, une autre affaire, la parution prévue de «Operation Dark Heart», avait encore semé le trouble à Washington. Ce livre traitant de l'Afghanistan a été écrit par le lieutenant-colonel de réserve Anthony Shaffer, lorsqu'il servait à la Defense Intelligence Agency en qualité d'analyste. Shaffer a été déployé 5 mois en Afghanistan sur la base américaine de Bagram en 2003. Après avoir perdu ses accréditations auprès de la DIA, il a été révoqué, suite à plusieurs affaires de violation des règles de sécurité, et occupe actuellement un poste de recherche au Center for Advanced Defense Studies.

Pourtant approuvé par de nombreux lecteurs officiels, d'autres lecteurs des différentes agences de renseignement estimaient que ce livre avait plus de 200 passages contenant des informations protégées. Selon le directeur de la DIA, des révélations concernant les opérations clandestines en Afghanistan pouvaient ainsi nuire à la sécurité nationale. Le livre révélait notamment des détails compromettants, comme les noms d'agents de la CIA ou de la NSA agissant en Afghanistan ainsi que sur les réseaux d'espionnage américain au Pakistan.

Le Pentagone a racheté la quasi-totalité des 10.000 exemplaires afin de les détruire mais plusieurs douzaines d'ouvrages non expurgés sont encore en circulation. Plusieurs revues ou journaux, comme le New York Times, ont pu s'en procurer via internet. En outre, certains commentateurs estiment que le Pentagone a fait une publicité énorme à un livre qui serait sinon peut-être passé inaperçu…

Un autre exemple est celui d'une autre série de fuites récentes dans les médias, qui a conduit le directeur du renseignement national à demander à ses agents de «la fermer». Le directeur, James R. Clapper, a déclaré qu'il était inquiet suite aux révélations d'informations confidentielles dans la presse.

- Une affaire qui suscite un débat passionnel

L'administration OBAMA a certes condamné sévèrement les fuites de télégrammes diplomatiques exploités par le site WikiLeaks et publiés par de nombreux médias internationaux. La Secrétaire d'État Hillary Clinton a ainsi affirmé que ces publications

constituaient «une attaque contre les intérêts américains» mais aussi «contre la communauté internationale». Mais si cette affaire est encore loin de diviser l'opinion américaine, elle n'en a pas moins suscité un débat souvent passionnel, comme en témoignent les nombreux articles et autres déclarations parus ces derniers mois.

Conclusion

L'ampleur des documents téléchargés, qui se comptent en centaines de milliers, par un seul jeune Militaire du Rang, s'explique en partie par des failles de sécurité que d'aucuns jugent inadmissibles. Les Américains, traumatisés par les événements du 11 septembre 2001, se focalisaient sur les menaces extérieures et n'avaient donc pas jugé utile d'activer des systèmes d'alerte existants. En outre, ces affaires ont également mis au grand jour le nombre impressionnant d'individus et d'agences ayant accès aux réseaux sécurisés[11].

Le véritable défi pour les Américains va désormais être de trouver l'équilibre entre la sécurité et la nécessiter de donner aux unités les renseignements dont elles ont besoin.

[1] Il s'agit ici des causes essentiellement techniques.

[2] Adrian LAMO

[3] Joint Worldwide Intelligence Communications System

[4] Secure Internet Protocol Router Network

[5] SIPR-NIPR Access Point

[6] Les documents du Département d'État seraient stockés sur la base de données appelée "Net Centric Diplomacy Data Base" (NCD) placée sur SIPRNet.

[7] PST = Personal Storage

[8] Host Based Security System

[9] Non Classified Internet Protocol Router Network; Secret SIPRNet et TOP-Secret Joint Worldwide Intelligence Communications Systems

[10] Defense Advanced Research Projects Agency

[11] Près de 2 millions d'individus auraient accès à SIPRNet.

Le Lieutenant-colonel Yannick LEGRAND, engagé au titre de l'artillerie (officier de reconnaissance au 53°RA) est admis à l'École Militaire du Corps Technique et Administratif en 1992. Au cours de sa carrière, il sert notamment à l'EAI, puis au 44°RT puis à la Brigade de Renseignement. Il est actuellement officier de liaison à l'United States Army Intelligence Center of Excellence à Fort Huachuca (Arizona). Titulaire d'un mastère de sciences politiques et ancien stagiaire du CID (2005-2006), il a effectué deux séjours au Kosovo à Pristina (2001-2002) et à Novo Selo (2009-2010 Multinational Task Force North ISR BAT Commander).

Titre : le Lieutenant-colonel LEGRAND

Auteur(s) : le Lieutenant-colonel LEGRAND