Les leçons du vol 253 –
La faillite du système des bases de données du renseignement

par Arnaud Palisson

Février 2010

[Deuxième volet de l'étude consacrée à l'attentat manqué contre le vol 253]

Avant l'attentat manqué du 25 décembre 2009 contre le Vol Amsterdam-Détroit, la communauté américaine du renseignement avait collecté plusieurs informations pertinentes concernant l'implication terroriste d'Abdul Mutallab. Ce que l'on reproche principalement aujourd'hui à l'Administration, c'est son incapacité à relier les points (*connecting the dots*), à repérer et à arrêter Abdul Mutallab **avant** qu'il ne monte dans l'avion.

S'agit-il de nouvelles affres du cloisonnement entre les agences, quelques semaines après le massacre de Fort Hood (qui a mis en évidence le non-partage d'information entre l'Armée américaine et le FBI) ? Ou faut-il y voir un procès d'intention, diligenté par des politiciens médiatisés, spécialistes du "*y-avait-qu'à-fallait-qu'on*" ?

Après le 11 septembre 2001, la preuve fut faite que les agences de renseignement travaillaient en silo, sans partager l'information de sécurité nationale. On a alors instauré en 2005 l'*Office of the Director of National Intelligence* (ODNI) qui supervise les seize agences fédérales de renseignement. En son sein, a été créé le *National Counter Terrorism Center* (NCTC), dont la tâche est précisément de mettre en relation les informations pertinentes détenues par des agences différentes.

Mais en instaurant ces nouveaux organismes, l'Administration Bush a également créé un monstre bureaucratique qui a bien vite rendu inopérants les avantages techniques qu'aurait pu avoir ce changement majeur. L'affaire du vol 253 est symptomatique de cette bureaucratie.

La question n'est pas de savoir comment les États-Unis pourraient obtenir davantage de données. Les services de renseignement américains croulent littéralement sous les informations : bases de données, écoutes téléphoniques, interceptions de courriels, images de satellite et de drone, sources humaines infiltrées,... Mais il faut aussi se souvenir que *trop d'information tue l'information*. La vraie question est donc plutôt : *comment faire pour tirer de cette masse deux ou trois informations pertinentes et les mettre en relation pour en déduire l'existence d'une menace ?*

En ce qui concerne l'aviation civile, le système repose sur deux outils : les *Watch Lists* (**1**) et la récupération tous azimuts d'informations de sécurité nationale (**2**). Dans l'attentat du vol 253, les deux ont échoué. Mais pouvait-il en être autrement ?

1 Les Watch Lists

***Note** : On n'envisagera ici que les listes de surveillance concernant l'aviation civile établies aux États-Unis. Toutefois, la réflexion engagée ici est largement transposable aux listes homologues d'autres pays.*

1.1 Présentation des quatre *Watch Lists* de l'aviation civile

En ce qui concerne la seule aviation civile, on ne compte pas moins de quatre listes de surveillance d'individus susceptibles de liens avec le terrorisme :

- Le ***Terrorist Identites Datamart Environment*** **(TIDE)** est une base de données des personnes suspectées d'entretenir des liens avec le terrorisme. Tenue par le NCTC, la liste TIDE compte **550 000 noms**.[1]

- La ***Terrorist Screening Database*** **(TSDB)** (ou *Consolidated Terrorist Watch List*) est tenue par le *Terrorism Screening Center* (TSC), branche du FBI. Cette liste sert aux différentes agences américaines d'application de la loi pour établir leur propre liste de surveillance. La TSDB est établie d'après la TIDE, mais épurée et consolidée par les renseignements obtenus par le FBI. La TSDB compte **400 000 noms**.[2] Pour qu'un individu soit placé sur cette liste, il faut qu'existe un **soupçon raisonnable** qu'il a été ou est impliqué dans des activités terroristes. Timothy Healy, directeur du TSC, définit ainsi ce concept :

  > *Reasonable suspicion requires 'articulable' facts which, taken together with rational inferences, reasonably warrant a determination that an individual is known or suspected to be or has been engaged in conduct constituting, in preparation for, in aid of, or related to, terrorism and terrorist activities, and is based on the totality of theses circumstances. Mere guesses or inarticulate 'hunches' are not enough to constitute reasonable suspicion.*[3]

- La ***Secondary Security Screening Selectee List*** **(SSSS)** est la liste des personnes censées passer au contrôle secondaire lors d'un voyage par avion. Elle est établie par le *Department of Homeland Security* (DHS). Les critères de sélection sont multiples : passagers qui ont un billet aller simple, qui paient leur billet en liquide, qui réservent leur vol le jour même, qui n'ont pas de document d'identité, qui sont choisis au hasard,... Cette liste contient **14 000 noms**.[4] Elle est distribuée aux compagnies aériennes qui doivent, sous peine d'amende, signaler sur la carte d'embarquement

[1] http://www.foxnews.com/story/0,2933,581193,00.html

[2] http://www.foxnews.com/story/0,2933,581193,00.html

[3] http://online.wsj.com/article/SB10001424052748704065404574636130361837754.html

[4] http://www.foxnews.com/story/0,2933,581193,00.html

que la personne doit passer au contrôle secondaire, généralement par l'apposition d'une inscription "SSSS".

- La ***No-Fly List*** est établie par le DHS. Elle répertorie les noms de personnes présentant une menace pour les États-Unis et à qui il est interdit de monter à bord d'un avion qui s'y rend ou qui va en survoler le territoire. Elle est distribuée aux compagnies aériennes qui doivent, sous peine d'amende, refuser de délivrer une carte d'embarquement à toute personne qui y figure. Fin 2009, cette liste comprenait **4 000 noms**.[5]

1.2 L'inadéquation des listes en général

La première question à jaillir lorsque l'on considère cette pluralité de listes est la suivante : quel intérêt d'avoir des *Watch Lists* différentes de la *No-Fly List* ? En effet, s'il s'agit d'individus susceptibles de commettre des attentats terroristes, pourquoi ne pas **tous** les interdire de vol ?

En fait, en matière de renseignement, il est important que les services soient capables de surveiller les allées et venues de certaines personnes sans éveiller leur attention. Le passage par un aéroport d'un individu placé sur une *Watch List* permet de savoir que, tel jour, il s'est rendu de tel point à tel autre, éventuellement avec telle autre personne. Il s'agit là d'outils importants dans la collecte d'informations de sécurité nationale. Ils s'inscrivent dans une démarche de renseignement, sur le long terme.

Mais ce système de liste présente un intérêt très limité pour ce qui est d'assurer la sureté de l'aviation civile au niveau tactique.

S'il faut en croire les différents gestionnaires de service de renseignement interrogés sur le sujet, une personne n'est placée sur une liste de surveillance que s'il existe des informations suffisamment fiables pour estimer que cette personne constitue une menace pour les États-Unis. Malheureusement, de nombreuses personnes, parfaitement exemptes de tout lien avec le terrorisme, sont régulièrement victimes de ce système de listes nominatives. Les exemples abondent, notamment :

- En février 2006, une certaine Catherine Stevens (épouse d'un parlementaire américain) était interrogée avant d'embarquer pour savoir si elle était « Cat Stevens ».[6] On ignore par ailleurs s'il s'agit en fait du nom du chanteur folk américain converti à l'islam et rebaptisé Yussuf Islam, qui fut lui-même interdit de vol en raison de cette liste en 2004.[7]

[5] http://www.foxnews.com/story/0,2933,581193,00.html

[6] http://travel2.nytimes.com/2006/02/14/business/14road.html

[7] http://abcnews.go.com/2020/News/story?id=139607&page=1

- En 2004, le parlementaire américain Don Young était stoppé avant d'embarquer car il avait été confondu avec un certain Donald Lee Young.[8]
- Plusieurs *U.S. Air Marshals* ont été interdits de monter à bord des vols qu'ils devaient protéger, en raison d'un nom similaire figurant sur la *No-Fly List*.
- Jusqu'en 2008, Nelson Mandela et d'autres membres de l'African National Congress (ANC) figuraient encore sur la *No-Fly List*.[9]
- *Idem* pour le président de la république bolivienne, Evo Morales.[10]

- Mais l'exemple le plus connu (et le plus caractéristique) des limites de ce système de liste nominative est celui de Michael Hicks. Ce nom figure sur la *SSSS List.* En 2003, Michael Hicks a été pour la première fois contraint de subir une palpation de sécurité avant de prendre l'avion. Premier problème : Michael Hicks avait alors... 2 ans. Second problème : Michael Hicks a aujourd'hui 8 ans et il subit **toujours** un contrôle secondaire avant de monter dans un avion.

Comment expliquer une telle aberration ? Interrogée à ce sujet, la *Transportation Security Administration* (TSA) se livre à un exercice de noyade de poisson d'une **mauvaise foi sidérante** :

> *« There is no children on the No Fly or Selectee lists. What happens is a match or similar match to an actual individual on the No Fly or Selectee Watch List* (…) *Airlines can and should automatically de-select any 8-year-olds out there that appear to be on a Watch List.*[11]

Autrement dit, ce n'est pas l'enfant qui est sur la liste mais une personne qui porte le même nom. Mais comment la compagnie aérienne peut-elle « désélectionner » une personne si son agent au comptoir d'enregistrement ne dispose d'**aucun autre élément qu'un nom** ?

Et pourquoi la TSA n'a jamais rien fait pour enlever Michael Hicks de la liste qu'elle établit ? Parce qu'enlever le jeune Michael Hicks de la *SSSS List* reviendrait à en ôter également le vilain Michael Hicks.

Mais, comme le rappelle fort justement le *New York Times*,[12] il existe 1 600 Michael Hicks rien que dans le répertoire téléphonique des États-Unis.

---

[8] Comme quoi l'approximation des listes est vraie dans les deux sens.

[9] http://www.usatoday.com/news/world/2008-04-30-watchlist_N.htm

[10] http://www.cbsnews.com/stories/2006/10/05/60minutes/main2066624_page2.shtml

[11] http://www.tsa.gov/blog/2010/01/there-are-no-children-on-no-fly-or.html

[12] http://www.nytimes.com/2010/01/14/nyregion/14watchlist.html

Cela soulève plusieurs questions. Le *bad guy* Michael Hicks (qui court toujours depuis au moins 6 ans) constitue-t-il une menace ? Quelle est la raison de son placement sur la liste ? Est-ce un délinquant de droit commun ou un terroriste ?

Car après tout, si la *SSSS List* le repère à un aéroport, elle ne conduira pas à son arrestation, mais juste à un contrôle secondaire au point de fouille. Cela signifie que pour simplement embêter le *bad guy* Michael Hicks, la TSA est prête à systématiquement pourrir le passage aux aéroports d'au moins 1 600 personnes (dont de jeunes enfants)... Et le cas du jeune Michael Hicks n'est malheureusement pas isolé.[13]

Au cours des trois dernières années, près de 82 000 personnes ont ainsi été contrôlées avant d'embarquer sur un vol depuis ou à destination des États-Unis, sans autre raison qu'une homonymie. Aucun terroriste recherché ne se trouvait parmi elles.

Aussi ne doit-on pas s'étonner que, rien qu'en 2007, **27 000** personnes aient été retirées de la liste TIDE.

Le programme *Secure Flight* (lancé en 2003 et aujourd'hui encore en cours d'installation au niveau national...) est censé régler le problème : chaque passager devra fournir un billet d'avion dont le nom, prénoms et initiales sont identiques à ceux figurant sur sa pièce d'identité. Mais surtout, *Secure Flight* devrait, à terme, fournir aux compagnies aériennes des informations supplémentaires (comme le sexe et la date de naissance) sur la personne effectivement recherchée.

Malheureusement, cela ne mettra pas fin à la problématique des *Watch Lists*.

En effet, ces listes ne sont efficaces que si elles sont ciblées et qu'elles ne comprennent qu'un nombre limité de personnes sur lesquelles on dispose de suffisamment d'éléments d'identification. Certes, de 2007 à fin 2009, face au nombre considérable de faux positifs, les agences de renseignement avaient commencé à épurer les listes les plus restrictives, à savoir la *SSSS List* et la *No-Fly List*. Mais après l'attentat manqué d'Abdul Mutallab, la pression politico-médiatique a été si prompte à dénoncer l'absence du Nigérian sur ces mêmes listes restrictives qu'aujourd'hui, la tendance s'est inversée. Et on déplace par wagons entiers des noms de la liste TIDE vers la TSDB afin qu'ils soient ensuite intégrés sur la *SSSS List* voire la *No-Fly List*.[14] Encore et toujours, on comble en vain par la quantité un manque flagrant de qualité.

[13] http://www.boston.com/news/nation/articles/2005/08/16/no_fly_list_grounds_some_unusual_young_suspects/ - http://www.nytimes.com/2008/09/30/business/30road.html?_r=2&oref=slogin

[14] http://online.wsj.com/article/SB126265983505315961.html

1.3 L'utilité toute… relative de la liste SSSS

C'est au niveau du comptoir d'enregistrement qu'une personne est identifiée sur cette liste. Les lettres *SSSS* sont alors imprimées sur sa carte d'embarquement.

Si vous êtes un terroriste en mission-suicide et portez sur vous des explosifs, qu'allez-vous faire ? Allez-vous tenter de passer votre bombe malgré les portiques renifleurs, le test de l'écouvillon détecteur d'explosif et une palpation de sécurité ? Si votre QI dépasse 40, **vous allez tourner les talons et quitter l'aéroport**.

À moins de savoir exactement quels types de contrôle secondaire vous attendent au point de fouille. Il faut se souvenir que le 25 décembre dernier, **Abdul Mutallab est passé avec succès au travers d'un contrôle secondaire, avec palpation de sécurité, à l'aéroport de Lagos**. Alors qu'il dissimulait sur lui la charge de penthrite... Il faut aussi rappeler qu'il s'était auparavant entrainé un mois au Yémen, notamment à leurrer le système de sureté des aéroports.

1.4 Les paradoxes de la *No-Fly List*

Un individu dont le nom apparait sur la *No-Fly List* sera avisé au comptoir d'enregistrement que la compagnie ne peut pas le laisser monter dans l'avion. Il ne lui sera pas délivré de carte d'embarquement. L'affaire s'arrête là. Dossier classé. La menace potentielle est écartée. *Dormez tranquilles, braves gens.*

Sauf que si la personne n'a absolument rien à se reprocher, cela peut avoir des conséquences scandaleuses. Imaginez la catastrophe que cela peut être pour un homme d'affaires américain qui voyage d'un bout à l'autre du pays pour raisons professionnelles. Si cette personne veut un jour pouvoir reprendre l'avion depuis ou vers les États-Unis, elle

devra faire une demande administrative ad hoc via le *Redress Process*. Et attendre des mois le bon vouloir de l'administration...

Alors bien sûr, on rétorquera que si la personne refoulée est bel et bien un terroriste, la *No-Fly List* a fait son office. Mais là encore, c'est discutable. En le refoulant au comptoir d'enregistrement, le système adresse au terroriste le message suivant : « *tu peux rentrer chez toi tranquillement et dire à tes chefs que tu es grillé et qu'ils envoient quelqu'un d'autre faire le boulot*.»

Ne serait-il pas plus avisé de le **dissuader**, lui et ses complices, de faire sauter l'avion ? Pourquoi donc ne pas laisser le terroriste repéré monter à bord après un contrôle secondaire particulièrement poussé et en lui mettant un *Air Marshal* sur le dos pendant le vol ? C'est précisément ce qu'*El Al* a fait en 2001, lorsque Richard Reid a voulu embarquer pour Israël. Le Britannique a compris ce jour-là qu'il lui serait impossible de faire exploser un avion d'*El Al*. Et il s'est tourné vers *American Airlines*...

Mais en occident, aucun haut-fonctionnaire ne prendra jamais la responsabilité de laisser monter à bord un individu considéré comme une menace. Même s'il a été passé au peigne fin... Le haut-fonctionnaire défend en effet un intérêt supérieur : sa progression de carrière.

Et puis, il y a l'autre aberration du système, mis en lumière en 2006 par l'émission de CBS, *60 Minutes*.[15] À cette occasion, les journalistes avaient établi que quelques-uns des plus dangereux terroristes au monde ne figuraient pas sur la *No-Fly List* parce que les agences américaines de renseignement qui la fournissent aux aéroports et compagnies aériennes craignent qu'elles tombent entre les mains des terroristes eux-mêmes. Cathy Berrick, alors directrice des questions de sécurité nationale et de justice pour le *General Accounting Office* (GAO, l'organe d'enquêtes et d'audit du Parlement étatsunien), avait déclaré :

> [The airlines] *are not given all the names for security reasons because the government doesn't want to have that information outside of the government.*

Si le système vise à empêcher les individus présentant une menace de monter dans un avion, pourquoi la liste ne mentionne-t-elle pas certains parmi les plus dangereux ? Cathy Berrick répondait :

> *Yeah, it's a concern. And I think if you talk to the Department of Homeland Security they would agree with that.*

Pour reprendre la formule de Bruce Schneier, expert en sécurité et célèbre détracteur de la TSA, la *No-Fly List* est une **liste de personnes trop coupables pour monter dans un avion mais trop innocentes pour être arrêtées**.

[15] http://www.cbsnews.com/stories/2006/10/05/60minutes/main2066624.shtml

1.5 La procédure d'enregistrement

Deux semaines après l'attentat manqué du vol 253, on apprenait que des douaniers américains attendaient Abdul Mutallab à sa descente d'avion à Détroit.[16] Des agents de la *U.S. Customs and Border Protection* (*CBP*) avaient apparemment découvert tardivement les liens d'Abdul Mutallab avec la mouvance extrémiste. Ils avaient quelques questions à lui poser à l'arrivée, faute d'avoir pu l'intercepter avant le décollage.

Pourtant, le manifeste de vol (la liste des passagers sur un vol déterminé) doit être envoyé 72 heures **avant** le départ du vol. Mais ce n'est apparemment pas encore suffisant...

Toujours est-il qu'à compter de mars prochain, les douanes américaines pourraient interdire l'embarquement des ressortissants de 35 pays, qui ne se sont pas préalablement enregistrés en ligne auprès de l'administration. Selon une porte-parole de la CBP, l'objet de cette nouvelle mesure de sureté est de détecter les visiteurs ayant des antécédents criminels ou d'immigration avant qu'ils n'entrent aux États-Unis.[17] Comme le dit la porte-parole de la CBP :

> *« This makes sure travelers who do not require a visa do not pose threat by traveling to the U.S.*

La CBP nous annonce que cette mesure n'est pas en lien avec l'attentat du 25 décembre (ah ! les hasards du calendrier) puisque :

1. *cette mesure est en vigueur depuis 2008.* Actuellement, les passagers non enregistrés se font contrôler par les douanes américaines à l'arrivée. La différence est qu'à partir de mars, ils pourraient être interdits de vol.
2. Abdul Mutallab avait un visa. Signalons quand même en passant que pour en obtenir un, il faut faire l'objet d'une vérification de ses antécédents (*background check)*, via des bases de données gouvernementales. Or, on ne peut pas dire que cela ait particulièrement fonctionné dans le cas du Nigérian. Mais vous êtes priés de croire que cela fonctionnera mieux pour des ressortissants qui n'ont pas besoin de visa...

On pourra rétorquer que cette mesure permettra au moins d'écarter des étrangers non soumis au visa. Mais la CBP nous annonce que l'on pourra s'enregistrer quelques heures avant d'embarquer. Or, actuellement, les services américains imposent aux compagnies aériennes de leur faire parvenir le manifeste au moins 72 heures avant le vol. Et, on l'a vu, le système en place est incapable de faire sonner l'alarme dans ce délai. En quoi un enregistrement, réalisé 3 heures avant le vol par le passager lui-même, sera-t-il en mesure de changer les choses ?

[16] http://articles.latimes.com/2010/jan/07/nation/la-na-airline-terror7-2010jan07

[17] http://www.usatoday.com/travel/flights/2010-01-24-register_N.htm

La CBP estime apparemment qu'en un délai aussi court, elle serait capable de tenir à l'écart les personnes condamnées au pénal ou qui constituent une menace pour les USA. Cela amène les remarques suivantes :

1. Comment la CBP va-t-elle s'y prendre pour consulter en si peu de temps les bases de données *ad hoc* des différents pays concernés ? Surtout lorsque ces pays sont réticents à fournir l'information.[18]
2. Une personne condamnée pour un délit mineur, même si elle a effectué sa peine, serait interdite d'entrer aux États-Unis d'Amérique, ainsi nouvellement proclamée vertueuse Utopia.

Cette procédure d'enregistrement n'est qu'un leurre de plus. La menace terroriste la plus insidieuse (et donc la plus dangereuse) ne vient pas des étrangers, avec ou sans visa. Mais d'individus détenant la nationalité étatsunienne, recrutés par les groupes terroristes. Il peut s'agir de groupes tels qu'Al-Shabab, organisation qui recrute aujourd'hui des jeunes Américains qu'elle endoctrine et forme au jihad. Mais il peut aussi s'agir – car on a tendance à l'oublier – de terroristes domestiques qui, à l'image d'un Theodore Kaczinsky (alias *Unabomber*),[19] pourraient tout-à-fait s'attaquer à l'aviation civile dans les prochaines années.

Mais toutes ces questions de noms de terroristes sur des listes deviennent obsolètes si le terroriste voyage sous une fausse identité...

1.6 La fausse identité

Ce système de listes de surveillance sert à repérer des personnes portant le même nom qu'un terroriste. Mais encore faut-il que le terroriste voyage sous son vrai nom (ou sous un alias que les services de renseignement connaissent).

Le Secrétaire général d'Interpol a été bien inspiré de déclarer très récemment que la fraude aux passeports constitue «*the biggest threat facing the world*», précisant que les bases de données de l'organisation internationale de police criminelle recensent aujourd'hui environ 11 millions de passeports manquants ou volés.[20] Une véritable aubaine pour des terroristes cherchant à éviter d'être détectés par des *Watch Lists*.

Mais il y a encore plus simple pour contourner le système : ainsi, un homme d'affaires canadien voyageant très fréquemment par avion était victime d'une homonymie. Systématiquement importuné par les agents de sécurité des aéroports, il a... changé de

[18] http://www.usatoday.com/travel/flights/2010-02-09-data-sharing_N.htm

[19] http://en.wikipedia.org/wiki/Theodore_Kaczynski

[20] http://www.dailymail.co.uk/news/worldnews/article-1247082/Passport-fraud-biggest-threat-facing-world.html

prénom.[21] Depuis, il ne subit plus de désagréments aux aéroports. Imaginez qu'un terroriste fasse de même, en faisant modifier un registre d'état-civil dans une ville africaine ou orientale qui n'a jamais vu un ordinateur et encore moins un réseau informatique. Et d'obtenir ainsi un vrai passeport sous un vrai nom inconnu des services de renseignement.

Le terroriste n'a qu'à changer d'identité et le système des listes est tenu en échec.

Mais au-delà de ces listes, la faillite du système touche également tout un système de collecte et de traitement de l'information de sécurité nationale.

2 la récupération tous azimuts d'informations de sécurité nationale

Si l'on en croit de nombreux organes de presse et plusieurs politiciens américains, Abdul Mutallab aurait dû être intercepté bien avant de monter dans l'avion. Nous connaissons tous en effet l'argument : il existait plusieurs éléments de fait qui auraient dû sonner l'alarme dans la communauté étatsunienne du renseignement.

Bienvenue au pays merveilleux de Capitol Hill, où trois Sénateurs et deux Représentants refont le monde à posteriori, le havane au bec, depuis leur fauteuil club avec vue sur le *Washington Monument*.

Des informations avaient certes été collectées. Mais comment les services compétents pouvaient-ils savoir **à priori** qu'elles étaient pertinentes ?

2.1 Un signalement à la CIA

Un mois avant la tentative d'attentat sur le vol 253, le père d'Abdul Mutallab, ancien banquier et homme d'affaires très en vue au Nigéria, contactait les autorités nigérianes puis l'ambassade des États-Unis à Abuja. Là, il expliquait à un agent de la CIA que son fils avait coupé les ponts avec sa famille, s'était radicalisé et était parti au Yémen.[22]

En fait, cet agent de liaison à Abuja aurait rédigé un rapport subséquent, adressé notamment au *National Counter Terrorism Center*. Cela eut pour conséquence de placer Abdul Mutallab sur la liste *TIDE*.

Le rapport de l'agent de la CIA à Abuja a été transmis au Département d'État, via un rapport *Visas Viper* (cf. *infra*, § 2.2). Mais les fonctionnaires diplomatiques, peu familiers avec les spécificités de l'affaire, ont estimé inutile de s'alarmer et de faire porter Abdul Mutallab sur une liste plus restrictive. Est-ce là une faute impardonnable ? Loin de là. En effet, selon Jim Arkedis, un ancien analyste du renseignement américain :

[21] http://www.nytimes.com/2010/01/14/nyregion/14watchlist.html

[22] http://www.nytimes.com/2009/12/31/us/31terror.html

> *For the record, 99 percent of the time, walk-in sources to U.S. Embassies are poor-to-unknown quality. That includes friends and family members who walk into the embassy and claim their relatives are potential dangers. Why? Family relations are tangled webs, and who really knows if your uncle just might want you arrested in revenge for that unsettled family land dispute.*[23]

2.2 Le rapport *Visas Viper*

Quelques heures après l'attentat manqué, on apprenait que le terroriste nigérian disposait d'un visa américain à entrées multiples. On peut trouver l'information choquante : pourquoi le Département d'État n'avait-il pas préalablement révoqué ce visa ? *Welcome to the real world.*

2.2.1 Un visa britannique non renouvelé

Issu d'une famille très aisée du Nigéria, Umar Farouk Abdul Mutallab a eu ce qu'il convient d'appeler une jeunesse dorée. De 2005 à 2008, il étudie à Londres, où il réside dans un luxueux appartement du centre ville (évalué à 4 millions de livres). Dès 2006, les services de renseignement britanniques l'avaient à l'œil en raison de ses liens avec la mouvance islamiste radicale. C'est apparemment dans la capitale britannique qu'il entre en contact avec l'imam radical Anwar al-Awlaqi, considéré comme un recruteur avisé de la mouvance Al-Qaida. Toutefois, les services britanniques ne le considéraient pas comme une menace et l'ont donc placé sur une liste de surveillance standard. Les informations transmises à l'époque aux services américains n'étaient donc pas de nature à éveiller chez eux un intérêt particulier.

Abdul Mutallab quitte la Grande-Bretagne en 2008. Mais il fait une nouvelle demande de visa étudiant en 2009. Celle-ci est rejetée car l'établissement dont il était censé recevoir l'enseignement s'était avéré fictif. Là encore, l'information aurait été relayée par les Britanniques outre-Atlantique, sans mentionner qu'il constituerait une menace. Pour les services américains donc, toujours pas de quoi fouetter un chat.

2.2.2 Un visa américain qui n'aurait pas été renouvelé

Le programme *Visas Viper* a été élaboré en 1993 pour permettre aux différents services diplomatiques et consulaires américains à l'étranger de transmettre au Département d'État toute information relative au terrorisme.[24] Les informations qu'il compile permettent aux agents de l'administration de décider s'il convient de lancer une procédure de révocation de visa ou simplement de non-renouvellement.

---

[23] http://www.progressivefix.com/realistic-expectations-about-the-intelligence-community

[24] http://oig.state.gov/documents/organization/107596.pdf

Le visa d'Abdul Mutallab avait été émis en juin 2008 et devait être renouvelé en mai 2010. Doit-on par conséquent s'étonner qu'il ait agi quelques mois avant l'expiration de son visa ? Car il ne fait guère de doute que ce visa n'aurait pas été renouvelé. En effet, il a été établi que les informations transmises par le père d'Abdul Mutallab avaient été intégrées dans la base de données du programme *Visas Viper*.[25] Par ailleurs, il est raisonnable de penser que le non renouvellement du visa britannique du Nigérian avait été également porté dans la base de données du Département d'État américain. Il y avait là suffisamment d'éléments pour que l'administration étatsunienne ne renouvelât pas, à l'avenir, le visa américain.

Mais pour qu'elle le **révoquât** sur-le-champ, encore eût-il fallu qu'elle disposât d'informations en ce sens en provenance du NCTC.[26] Or, il faut se souvenir qu'au lendemain de la visite du père du terroriste nigérian à l'ambassade des États-Unis à Abuja, le Département d'État avait fait des recherches dans ses bases de données. Et, selon un rapport de la Maison Blanche, en raison d'une orthographe différente, on n'y avait pas trouvé trace d'un *Umar Farouk Abdul Mutallab* détenteur d'un visa américain.[27]

Un parlementaire étatsunien ironisait à ce propos en expliquant que lorsqu'il commettait une faute de frappe ou d'orthographe dans une requête sous *Google Search*, le moteur de recherche lui proposait des orthographes alternatives. Cela peut paraitre caricatural, mais les bases de données phonétiques sont une nécessité pour les services de renseignement. D'autant plus lorsqu'ils travaillent sur des individus dont l'identification est tributaire d'une transcription approximative dans un système linguistique différent.

2.3 Une écoute téléphonique

À la mi-octobre, la NSA avait intercepté une conversation téléphonique entre des islamistes radicaux au Yemen, au cours de laquelle il était mentionné qu'un Nigérian allait bientôt mener une attaque terroriste.[28] Le 30 décembre dernier, le Président Obama déclarait à ce propos :

> *« Had this critical information been shared, it could have been compiled with other intelligence and a fuller, cleaner picture of the suspect would have emerged.* (...) *The warning signs would have triggered red flags and the suspect would have never been allowed to board that plane for America.*[29]

[25] http://blog.newsweek.com/blogs/declassified/archive/2009/12/28/what-u-s-intelligence-knew-about-the-underpants-bomber.aspx

[26] http://washingtonindependent.com/72386/state-department-for-all-practical-purposes-couldnt-have-revoked-abdulmutallabs-visa

[27] http://www.whitehouse.gov/sites/default/files/summary_of_wh_review_12-25-09.pdf, p. 5

[28] http://www.nytimes.com/2009/12/31/us/31terror.html

[29] http://www.msnbc.msn.com/id/34620122/ns/us_news-airliner_attack/

Certes, un Nigérian s'apprêterait à réaliser un attentat. Mais quel type d'attentat ? Dans quel pays ? Contre quelle cible ? Et quel Nigérian ? Selon une estimation de l'ONU en 2009, le Nigeria est le 8ème pays le plus peuplé au monde, avec plus de 154 millions de personnes,[30] auxquelles il faut ajouter 15 millions de Nigérians de la diaspora.[31] On dénombre donc environ **170 millions de Nigérians** dans le monde.[32]

Il est facile de dire à posteriori que cette information aurait dû être mise en perspective avec l'avertissement du père d'Abdul Mutallab. Mais à priori, comment faire le lien entre ces deux informations ? L'une est recueillie par la CIA, qui la retransmet au NCTC et au Département d'État. L'autre est collectée par la NSA. Cette information est-elle significative pour la NSA ? Non. Y a-t-il matière à la partager ? C'est discutable. Y a-t-il seulement un processus pour le partage d'informations aussi lacunaires ? Dispose-t-on de la technologie pour traiter ainsi **toutes** les informations que la NSA collecte chaque jour ?

2.4 Un plan de vol hors normes

On a entendu et lu un peu partout que le terroriste nigérian avait acheté un aller simple, pour Détroit. Cela laissait entendre qu'il n'avait aucune intention de rentrer chez lui. Mais, après tout, n'est-ce pas ce qu'il avait dit à son père ? Et cela signifiait-il pour autant qu'il allait faire sauter l'avion de la *NorthWest* ?

Quoi qu'il en soit, l'achat d'un billet aller simple serait un critère de sélection au sens de la liste SSSS. Personnellement, nous trouvons ce critère d'une efficacité quasi-nulle. Car il est très facile à contourner. En effet, le terroriste qui achète un billet pour se suicider ne va pas rechigner à acheter un AR juste pour économiser...

Dans ce cas pourquoi Abdul Mutallab avait-il un billet aller simple ? En fait, il ne s'agissait **pas** d'un *aller aussi simple* : le Nigérian était parti de Dubaï (Émirats arabes unis), avait fait escale à Addis-Abeba (Éthiopie) et avait débarqué à Accra (Ghana) le 9 décembre 2009. Il y avait racheté un billet puis en était reparti le 24 décembre pour Lagos. Le lendemain, il quittait le Nigeria pour Amsterdam, puis Détroit.

Mais on peut tout aussi bien rétorquer qu'un tel plan de vol aurait dû faire retentir une alarme au QG du DHS américain. En effet, il existe des vols directs Accra-Detroit. Pourquoi passer par Lagos et Amsterdam ? C'est oublier un peu vite qu'un voyageur lambda peut obtenir des réductions substantielles en empruntant des vols avec correspondance(s), notamment sur une foultitude de sites Internet de voyages à rabais. Si le DHS veut aussi

[30] http://en.wikipedia.org/wiki/List_of_countries_by_population

[31] http://www.globalpolitician.com/2682-nigeria

[32] Chiffre approximatif qui ne tient pas compte du nombre de non Nigérians résidant au Nigeria.

prendre cela en considération dans ses bases de données, nous lui souhaitons bon courage...

2.5 Un billet payé en liquide

Nous savons aujourd'hui avec certitude qu'Abdul Mutallab a payé son billet d'avion en liquide, pour un montant de 2 831 $.[33] Or, on entend dire régulièrement que l'un des critères de sélection pour intégrer la liste SSSS réside dans le fait d'acheter son billet d'avion en argent liquide.

Si ce système de contrôle existe, il ne fonctionne apparemment pas aux aéroports d'Accra et de Lagos. Pourquoi ? Notamment parce que l'économie de l'Afrique noire est largement fondée sur l'argent liquide. Payer *cash* son billet d'avion y est une pratique très courante. Placer sur liste SSSS tous ceux qui paient ainsi leur billet rendrait rapidement ingérable les contrôles de sécurité dans les aéroports africains.

2.6 Pas de manteau, pas de bagage

Autres éléments qui, selon la presse et le landerneau politique, aurait dû mettre la puce à l'oreille des agences de renseignement : Abdul Mutallab n'avait pas de manteau pour prendre son vol entre Lagos et Détroit. Selon le Représentant américain Bill Pascrell, il aurait fallu remarquer immédiatement au point de fouille qu'Abdul Mutallab n'avait pas de manteau. Et le parlementaire d'ironiser :

> *He's flying into Detroit without a coat. That's interesting if you've ever been in Detroit in December*.[34]

Mais il faut considérer qu'il aurait très bien pu placer son manteau d'hiver dans son bagage de soute pour ne pas être embarrassé dans l'avion, puis le récupérer à l'arrivée, avant de sortir de l'aéroport. Une pratique que l'auteur de ces lignes met lui-même à profit.

Sauf qu'Abdul Mutallab n'avait pas non plus de bagage de soute. Là encore, on peut déplorer que des signaux d'alarme n'aient pas retenti dans les QG de la police et du renseignement. À l'instar de Bruce McQuain qui rappelle qu'en décembre 2001, Richard Reid avait réussi à monter à bord du vol 63 d'United Airlines alors que :

> [He] *bought a one-way ticket to the US, using cash and checked no luggage.* (...) *What other than the location of the explosives changed in those 8 years?*[35]

[33] http://www.lefigaro.fr/international/2009/12/29/01003-20091229ARTFIG00410-attentat-manque-le-parcours-du-jeune-terroriste-nigerian-.php

[34] http://www.mlive.com/news/detroit/index.ssf/2010/01/congress_umar_farouk_abdulmuta.html

Mais la vraie question c'est : *comment faire apparaitre cela à temps dans une base de données de l'administration américaine ?* Seul l'agent de la compagnie aérienne, lors de l'enregistrement, est capable de voir les bagages qu'une personne enregistre avant le vol. Et si un passager n'enregistre aucun bagage et se présente directement au point de fouille, comment les agents de contrôle peuvent-ils savoir qu'il n'a pas enregistré de bagage ?

Dès lors, le système devrait être capable de virer au rouge en cas de passager n'ayant pas enregistré de bagage pour un trajet longue distance et ce, dans un délai aussi court qu'une à deux heures. Compte tenu des différentes entités concernées (compagnie aérienne, police à l'aéroport, autorité aéroportuaire, sécurité pré-embarquement,...), ce délai parait beaucoup trop court et on devrait s'attendre à des retards quasi-systématiques au décollage. Déjà que **72** heures ne suffisent pas aux Douanes pour empêcher une menace de monter à bord...

Mais il y a encore plus frustrant : dans de nombreux aéroports aujourd'hui, il est possible d'enregistrer soi-même ses bagages. Dans ce cas, la compagnie aérienne va devoir mettre en place un système supplémentaire pour repérer rapidement un passager qui n'a pas de bagage enregistré pour un vol longue distance.

On pourrait alors imaginer que dorénavant, les agents aux points de fouille vérifient :

- que le passager est habillé adéquatement pour la destination de son vol
- **ET** qu'il a bien enregistré un bagage de soute.

Comment ? En s'assurant que le passager dispose bien d'un reçu pour bagage enregistré, remis au comptoir d'enregistrement. Mais là encore, si le *bad guy* a gardé ou récupéré un reçu qui ne correspond pas au vol en partance, comment l'agent du point de fouille va-t-il s'en apercevoir ? Va-t-il devoir scanner le code barre du reçu pour obtenir confirmation ? Et quand bien même n'y aurait-il pas concordance, l'individu peut toujours prétendre qu'il s'est trompé de reçu et a jeté le nouveau en croyant se débarrasser de l'ancien...

On le voit, le processus est sans fin...

2.7 Une déficience de l'analyse de renseignement ?

En janvier dernier, devant une commission du Sénat, deux membres de l'ancienne Commission d'enquête sur les attentats du 11-Septembre ont déclaré que l'attentat d'Abdul Mutallab était le symptôme d'un échec non pas en matière de partage mais uniquement d'analyse de l'information :

[35] http://www.qando.net/?p=6403

> *The greatest single challenge that arises from this incident in our view is the urgent need to strengthen the analytic process.*[36]

Malheureusement, c'est **faux**. En effet, pour que les informations soient analysées, encore faut-il qu'elles parviennent jusqu'aux analystes. Si elles ne s'y rendent pas, c'est parce qu'elles ne se singularisent pas, qu'elles ne se signalent pas au sein de la considérable masse de données collectées chaque jour.

Faire sortir du lot une information en raison de sa possible pertinence, ce n'est pas le rôle de l'analyse, mais celui de la **validation** et de la **centralisation** de l'information.

La phase de **validation** ne relève pas des analystes du renseignement, derrière leur bureau de Langley ou du J.Edgar Hoover Building. Elle relève des agents de renseignement, c'est à dire les hommes et les femmes sur le terrain qui, après avoir collecté une information, doivent évaluer :

1. sa véracité,
2. la fiabilité de sa source.

Un exemple particulièrement parlant est l'information transmise par le père d'Abdul Mutallab aux agents de la CIA à Abuja. L'information brute est la déclaration du père selon laquelle le jeune Nigérian avait signifié à sa famille qu'il coupait définitivement les ponts et partait pour le Yémen. Le processus de validation consistait à déterminer si cette information était crédible mais aussi si l'on pouvait considérer le père comme une source fiable. À priori oui, car il s'agit en l'occurrence d'un homme d'affaires de premier plan au Nigéria. Mais cela ne signifie pas pour autant qu'il est objectif en ce qui concerne ses problèmes de famille...

La tâche des agents de renseignement aurait été de s'en assurer puis, de faire en sorte que leur rapport soit particulièrement signalé en aval de la chaine de transmission de l'information.

La phase de **centralisation**[37] consiste en la transmission de l'information dans son intégralité, au bon destinataire, en étant correctement classée, archivée et disponible, afin qu'elle puisse être **analysée** (lors de la phase suivante). C'est ce que le cycle du renseignement selon la CIA désigne sous le terme *Processing*.[38]

---

[36] http://commerce.senate.gov/public/_files/KeanandhamiltonTestimony.pdf

[37] Cette phase est généralement appelée *classement* ou *classification*, mais le terme est impropre selon nous car trop restrictif.

[38] https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html

C'est d'ailleurs bien en ce sens que s'exprime James Lewis, directeur du *Center for Strategic and International Studies*, qui déclarait à propos de l'attentat du vol 253 :

> *Dans le passé, le patron du contre-espionnage chargé de lutter contre le terrorisme disposait de 11 ordinateurs différents parce qu'aucun d'entre eux ne pouvait communiquer avec les autres. Nous avons commencé à normaliser l'acquisition de ces technologies mais nous avons encore des progrès à faire.* (…) *Dans ce cas particulier [de l'attentat du vol 253] les éléments étaient éparpillés à plusieurs endroits différents et nous ne les avons pas réunis.*[39]

Ce n'est donc pas la phase d'analyse qui est déficiente, mais celles de validation et de centralisation de l'information.

La différence est d'importance. Car si l'on veut éviter qu'un tel fiasco se reproduise, il faudra s'assurer de focaliser sur les processus déficients. Il ne manquerait plus que l'on change ceux qui fonctionnent...

*
* *

Malgré son ampleur, le système étatsunien automatisé de regroupement des informations peut être aisément tenu en échec par le terrorisme aérien.

Peut-être parce que l'on a encore tendance à confondre regroupement d'informations brutes et renseignement. On ne peut pas (pas encore, en tout cas...) demander à des ordinateurs, aussi puissants soient-ils, de faire un travail d'analyse. Cette phase est la pierre angulaire du renseignement.

Le fiasco du système le 25 décembre dernier en est la preuve évidente. On pourra renforcer autant qu'on voudra le système des *Watch Lists*, multiplier les alertes sur les modes opératoires suspects aux aéroports (à quand un repérage des passagers portant une casquette de base-ball qui ne correspond pas à la ville de départ ou d'arrivée ?). Tant que l'on ne prendra pas en considération l'importance de l'analyse de l'information, un terroriste réussira encore et toujours à monter à bord d'un avion sans être repéré.

Mais pour qu'un analyste du renseignement fasse son travail, encore faut-il qu'on lui fournisse les informations pertinentes. Or, le système automatisé du renseignement américain continue d'ignorer cette phase, sous prétexte que *tout le monde sait bien que l'analyse, c'est trop long et ça ne sert pas à grand chose*. On voit à quelles extrémités conduit cette malencontreuse et durable ellipse.

[39] http://www.lemondeinformatique.fr/actualites/lire-la-maison-blanche-denonce-les-failles-informatiques-dans-la-gestion-des-menaces-terroristes-29680.html

Il faut se souvenir que les coups les plus durement portés au terrorisme aérien l'ont été grâce à un véritable travail de renseignement, appuyé sur de sérieuses **analyses** : l'Opération *Bojinka* (1995),[40] les attentats projetés contre des lignes aériennes transatlantiques (2006),...[41] Des succès du renseignement obtenus en amont de la perpétration de l'attentat, bien avant que les terroristes n'enregistrent leur bagage à l'aéroport...

Cet article est conforme à la nouvelle orthographe.

[40] http://en.wikipedia.org/wiki/Bojinka_plot

[4141] http://en.wikipedia.org/wiki/2006_transatlantic_aircraft_plot