UNE FUITE À LA WIKILEAKS EST-ELLE POSSIBLE EN FRANCE?

LE 17 FÉVRIER 2011 ***DAVID SERVENAY ET OLIVIER TESQUET***

Après la "plus grande fuite d'informations de l'histoire" orchestrée par WikiLeaks, tous les gouvernements prennent conscience de leurs faiblesses structurelles. En France, Owni a mené l'enquête.

Quelques jours après la fuite des mémos diplomatiques américains organisée par WikiLeaks, le dimanche 28 novembre 2010, la Direction générale de la sécurité extérieure (DGSE) a décidé d'activer une cellule de réflexion sur cette nouvelle effraction dans le paysage de l'information. Les analystes des services secrets français ont pour mission de répondre à deux questions:

> ***Cette fuite subie par les États-Unis est-elle susceptible de se produire en France ?***
> ***Le "modèle WikiLeaks" – des informations secrètes diffusées par un whistleblower – peut-il faire des émules, ici ou ailleurs ?***

Très vite, les hommes de la DGSE comprennent qu'il leur faudra répondre "non" à la première interrogation et "oui" à la seconde. Ou plutôt, trouver de solides arguments pour étayer de telles réponses. L'exercice n'est pas facile, car si la seconde assertion est très probable, la première est nettement moins certaine. Il faut dire que Le Monde, tout comme quatre grands journaux étrangers, multiplie alors les Unes tonitruantes sur les "fuites" de WikiLeaks. Sans interruption pendant au moins deux semaines. Cela agace le pouvoir.

Dès les premiers jours, un joli choeur de dinosaures digne de la guerre froide se fait entendre pour condamner la *"plus grande fuite d'informations"* jamais organisée. Bernard Guetta, le chroniqueur international de France Inter, vilipende dans Libération ***"la presse et la transparence informatique"***; sur Europe 1, la journaliste Catherine Nay **compare Internet à la Stasi**, *"parce que rien n'y est jamais effacé"* ; Hubert Védrine, ancien ministre des Affaires étrangères et gardien du temple mitterrandien, dénonce un *"Big Brother électronique"*. Mais le politique a aussi mis le doigt sur la profondeur historique du changement. Le 30 novembre, **dans Libération**, il soutient que *"la sécurité électronique sera renforcée [et que] les échanges passeront par d'autres canaux"*. Alors, une Wiki-fuite hexagonale est-elle possible?

Trois couches de sécurité

La France présente un profil de victime idéale. Deuxième puissance diplomatique derrière les États-Unis, elle échange 180.000 télégrammes par an. Le ministère des Affaires étrangères est le plus attaqué du pays, et il doit essuyer plusieurs assauts par semaine, à tel point que les équipes refusent d'avancer le moindre chiffre.

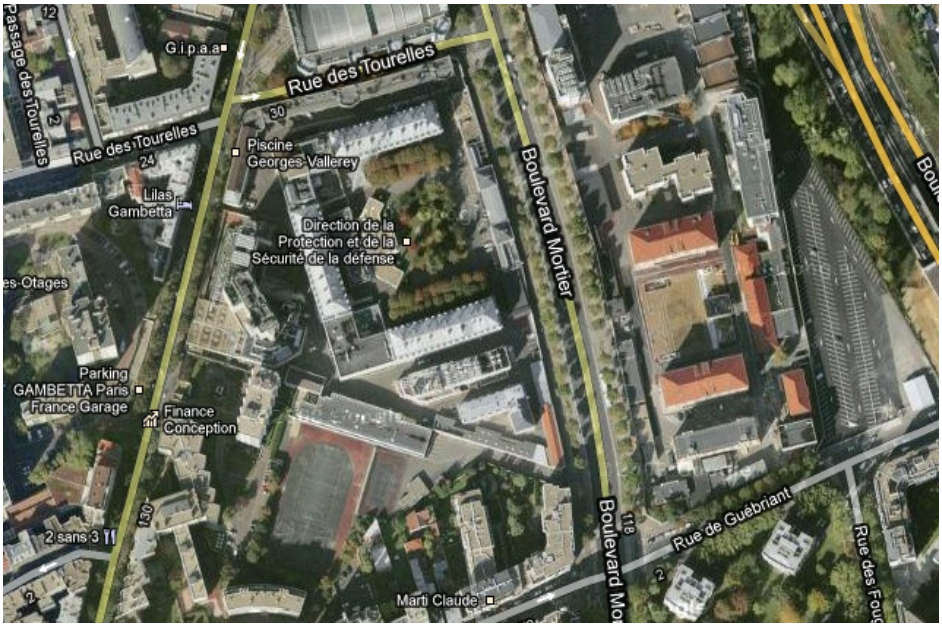
D'emblée, les responsables des systèmes d'information du MAE tiennent à se démarquer de leurs homologues américains en invoquant des choix techniques différents. *"Après le 11-Septembre, les États-Unis ont fait le choix de la mutualisation en multipliant les droits d'accès"*, explique l'un d'entre eux. Ce n'est pas faux. Outre **Intellipedia**, la plate-forme collaborative créée en 2005 pour agréger les 16 agences de renseignement, le gouvernement US a délivré pas moins de 854.000 accréditations "top secret" à des fonctionnaires, chiffre astronomique que révélait le Washington Post dans son enquête interactive **"Top Secret America"**.

Pour autant, l'architecture française est-elle totalement imperméable ? Coïncidence ou hasard, en septembre 2010, après dix ans de développement, Schuman a enfin été déployé au sein du ministère, pour remplacer Sartre. Schuman est le nouveau système de transmissions de données du Quai d'Orsay. Il fonctionne en trois "couches":

La couche horizontale, la plus ouverte, se présente sous la forme d'une messagerie Outlook, où transite en clair 80% de l'information
La messagerie sécurisée pour les télégrammes diplomatiques (TD), jusqu'au stade "diffusion restreinte", premier niveau de classification du secret défense. Très utile pour les communications interministérielles, qu'il s'agisse de l'Elysée, de Matignon ou de Bercy, cette deuxième est chiffrée selon le standard AES 256. Réputé pour sa solidité (même s'il n'est **pas incassable**), il a été approuvé par la NSA aux États-Unis et même utilisé par WikiLeaks pour son fameux fichier Insurance.
Les TD contenant *"de l'information à haute valeur ajoutée politique"* , comme le formulent les diplomates en charge de la sécurité du système, sont les derniers à avoir franchi le cap de la dématérialisation. Mise en place entre janvier 2010 et janvier 2011, cette couche nécessite une carte à puce personnalisée pour y accéder. Ce Schuman-C (pour confidentiel) sera totalement opérationnel d'ici à la fin de l'année : 2.800 personnes seront accréditées, et seuls douze chiffreurs, habilités au plus haut niveau et en rotation 24 heures sur 24, disposeront de droits d'administrateur sur l'ensemble du réseau.
Présentée comme telle, cette construction en silo semble adaptée aux exigences du moment. Problème : les trois couches du système sont installées physiquement sur les mêmes postes, eux-mêmes équipés de ports USB, de graveurs et surtout, d'une connexion Internet. Pour schématiser, un diplomate traite le tout-venant et la sécurité nationale sur la même machine, ce qu'un Julian Assange s'interdit formellement. Commentaire d'un M. Sécurité :

> ***La bunkerisation n'a aucun sens pour une administration qui travaille vers l'extérieur.***

Les “machines blanches” de la DGSE



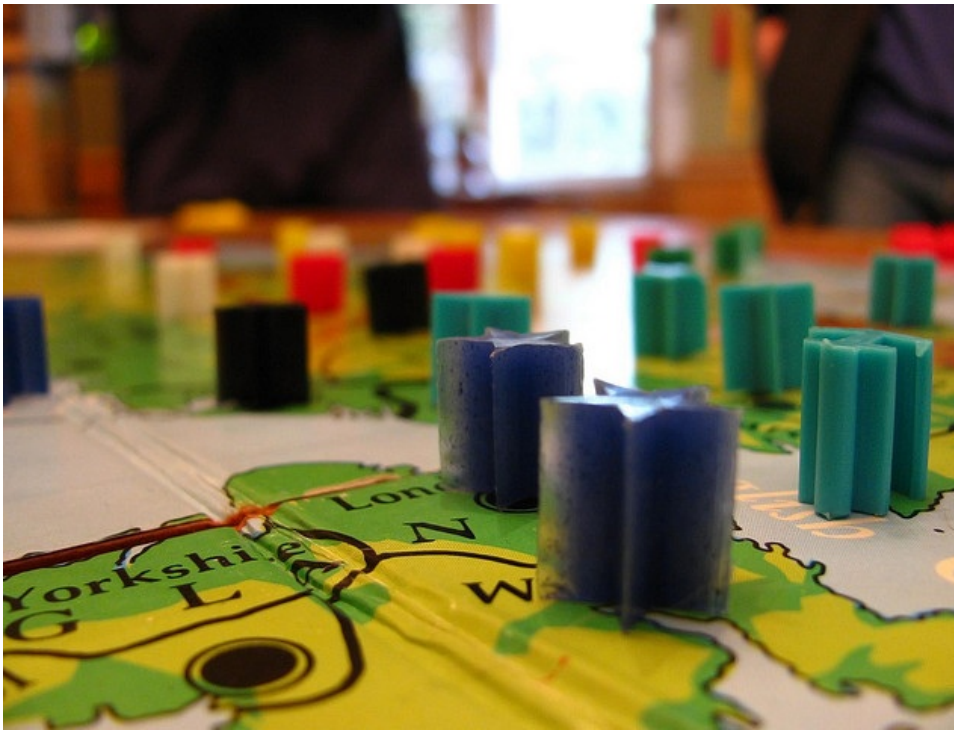
Pour les espions, les diplomates du “département” (surnom du Quai d’Orsay) font figure d’aimables amateurs. Il faut dire que la “boîte” (surnom de la DGSE) fonctionne grâce à un réseau étanche avec:

Un réseau chiffré indépendant, dont la clef algorithmique change toutes les secondes.
Des “machines blanches”, sans ports externes, installées dans des salles dédiées, pour la consultation des notes classifiées.
Un système de réquisition écrite et traçable pour la consultation des archives.
Aux yeux d’Alain Chouet, ancien directeur du renseignement de sécurité de la DGSE, le maillon le plus vulnérable est celui des diplomates :

> ***Du côté des militaires, nous sommes plus étanches et mieux protégés que les Américains. Pour le reste, c’est la Bérézina… L’administration est vulnérable au recueil de données et pire, au sabotage informatique. Foutre en l’air le système informatique de la Sécurité sociale pour six mois, cela ferait des dégâts !***

C’est d’ailleurs le scénario que redoutent le plus les directeurs des systèmes d’information du Quai d’Orsay: *“Plus que l’extraction, le vrai danger, c’est que l’outil soit corrompu ou que quelqu’un y injecte des données”*. En filigrane, c’est le facteur physique qui est mis en cause.

Si le ministère préfère évacuer la question de la faille humaine dans une rhétorique de *“fuite résiduelle acceptable”*, certains connaisseurs du sérail rechignent moins à livrer quelques pistes. François Nicoullaud, ancien ambassadeur de France en Iran et auteur d’une **tribune anti-WikiLeaks** dans le Figaro début janvier, pointe ainsi du doigt les *“négligences individuelles qui peuvent ponctuellement créer des problèmes”*, et identifie notamment deux erreurs. *“Parfois, un diplomate va envoyer un projet de télégramme en clair, même si c’est normalement proscrit”*, déplore-t-il. *“Mais le plus dangereux, c’est la dissémination. Même si le nombre d’accréditations est limité, les cabinets ministériels font toujours des photocopies, laissent traîner des papiers. C’est comme le lectorat d’un journal, des informations traînent sur une table.”* Au MAE, on se gargarise de l’équation suivante: *“C’est très différent de donner un document à 4 personnes ou à 16 personnes”*. Mais si ledit document est reproductible, qu’advient-il de ce calcul?



Le défi de la mobilité

Dans le monde post-WikiLeaks, sécuriser ses canaux de transmission traditionnels ne suffit plus, et le Quai d'Orsay doit relever un autre défi, celui de la mobilité. De ce côté, l'aveu est inquiétant. Équipés de téléphones sécurisés "Hermès" jusqu'au niveau de directeur adjoint, comme à l'Elysée et Matignon, les diplomates n'ont pas le droit d'utiliser de Blackberry et l'iPhone est vivement déconseillé. Et pourtant, à ce jour, ils ne disposent d'aucun système de consultation embarqué, qu'il s'agisse d'une tablette ou d'un ordinateur portable. Lorsqu'ils s'envolent pour un sommet ou une grande conférence internationale, ils n'ont que… du papier, premier véhicule de l'erreur humaine.

"Si vous écrivez que nous sommes le maillon faible, vous serez ridicules" , s'offusque l'un des responsables de la sécurité du ministère des Affaires étrangères. Néanmoins, son équipe reconnaît que le système actuel n'est pas parfait :

> ***Après WikiLeaks, nous avons réalisé un audit pour déterminer les failles. Notre réponse est que ce système ne permet pas une copie rapide et facile des milliers de télégrammes en circulation. Est-ce que ça peut nous arriver ? Peut-on en avoir autant dehors ? La réponse est non. Mais nous avons besoin de réponses adaptées. Les personnels doivent être conscients de ce qu'ils écrivent, des individus qu'ils nomment dans leurs rapports.***

Pour lutter contre les fuites, la sécurité du Quai d'Orsay doit piocher dans une enveloppe globale de 40 millions d'euros. *"Il n'y a pas d'économie dans ce secteur (celui de la sécurité informatique"*, précise-t-elle, en refusant de fournir le détail de la somme allouée au chiffrement ou à l'achat de postes sécurisés. Dans la course aux armements qui oppose les gouvernements aux hackers de tous bords, le ministère n'est pas peu fier d'avoir momentanément tari quelques sources, notamment celle qui alimentait les billets hebdomadaires de Claude Angeli dans le Canard Enchaîné. Jusqu'ici, tout va bien. ***"Mais l'important, c'est pas la chute, c'est l'atterrissage"***.

—

Crédits photo: Flickr CC ***Husky***, ***Theoddnote***, ***pj_vanf***

JMAX
le 17 février 2011 - 20:34 • SIGNALER UN ABUS - PERMALINK

Oulook en messagerie ? ils n'ont vraiment pas peur. Quand on pense que le ministère français de la Défense a financé des extensions sécurité à Thunderbid, cela serait plus judicieux de les utiliser.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

IBLIS
le 18 février 2011 - 1:12 • SIGNALER UN ABUS - PERMALINK

@jmax : je pense plutot que l'auteur voulait dire que le systeme s'apparente a un systeme de messagerie classique (qui ressemblerai à outlook)
*Enfin j'espère ^^*

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

OLIVIER TESQUET
le 18 février 2011 - 1:19 • SIGNALER UN ABUS - PERMALINK

@jmax @Iblis: Non non, il s'agit bel et bien d'une version d'Outlook…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

KOKOMINUTMAN
le 18 février 2011 - 11:13 • SIGNALER UN ABUS - PERMALINK

L'article répond à ses objectifs : détailler les mesures et les menaces sur les instruments officiels de traitements d'infos "sensibles".
Pourquoi un léger malaise sur lequel j'ai du mal à mettre des mots ?

Un petit "brainstorming" :

Technologie toute-puissante
fausse objectivité
citoyenneté absente
contre-pouvoir refusé

démocratie

démocratie ?

démocratie !

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

PATWOPER
le 19 février 2011 - 10:44 • SIGNALER UN ABUS - PERMALINK

Le maillon faible étant toujours le facteur humain, je suis tenté de citer ce bon vieux Thucydide " L épaisseur d'un rempart compte moins que a volonté de le défendre"..Formule toujours d'actualité…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

ROUVRAIS
le 22 février 2011 - 18:54 • SIGNALER UN ABUS - PERMALINK

Bonjour je trouve que votre existence est nécesssaire les contres pouvoirs ont toujours permis de faire avancer la démocratie. Je vous signale que dans notre département des Landes 40 la main mise politique, économique et d'informations par le président Henry EMMANUELI frise l'autocrarie. Nous sommes un association

MACSINITIATIVES qui a pour but des surveiller les comptes et initiatives des nos élus de la communauté de communes dit Mer Adour Côte Sud 23 communes.Les budgets sont démesurés et la prise de décision n'implique jamais les populations.Si ce type d'informations vous intéresses,car impossible de faire passer des infos sur notre journal local Sud-Ouest qui sourd à nos articles,nous sommes prêts à vous les envoyer.
Salutations

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

ARAKIEL
le 23 février 2011 - 15:54 • SIGNALER UN ABUS - PERMALINK

En informatique, rien n'est impossible, malheureusement, ou heureusement. ;-)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

PLS
le 24 février 2011 - 10:00 • SIGNALER UN ABUS - PERMALINK

Par pitié, arretez de faire un amalgame constant entre hacker et pirate. D'autant plus que des articles parus sur owni ne le faisaient pas, voire même expliquaient la différence fondamentale entre ces deux termes.
Vous arrive-t-il de confondre un revendeur et un receleur ?
un pilote de course et un chauffard ?
un imprimeur et un faussaire ?

Arretez s'il-vous plait. Après tant d'années, non seulement c'était lassant, mais cela commence à devenir énervant.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

OLIVIER TESQUET
le 24 février 2011 - 11:49 • SIGNALER UN ABUS - PERMALINK

@pls: Si je ne m'abuse, le terme "pirate" n'apparaît pas dans l'article. Quand bien même, je fais moins le distinguo entre "pirate" et "hacker" (qui sont pour moi voisins, sinon semblables dans l'idéologie) qu'entre "hacker" et "cybercriminel" (le véritable abus de langage, idéologiquement faux).
OT

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

ARNAUD
le 28 février 2011 - 11:56 • SIGNALER UN ABUS - PERMALINK

Ce ne serait pas plutôt des téléphone sécurisés "Thalès", et non "Hermès" ?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

OLIVIER TESQUET
le 28 février 2011 - 12:04 • SIGNALER UN ABUS - PERMALINK

@Arnaud: Hermès est le nom du système d'exploitation de ces téléphones sécurisés. Ils équipent également l'Elysée et Matignon.
OT

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

1 ping

Les tweets qui mentionnent Diplomatie française: point de fuite? » Article » OWNI, Digital Journalism -- Topsy.com le 17 février 2011 - 18:41

[...] Ce billet était mentionné sur Twitter par Nicolas Voisin, damien douani, Sane Lebrun, Karine Quarant, Owni et des autres. Owni a dit: [#owni] Diplomatie française: point de fuite? http://bit.ly/eWANyD l'enquête de David Servenay et @oliviertesquet [...]