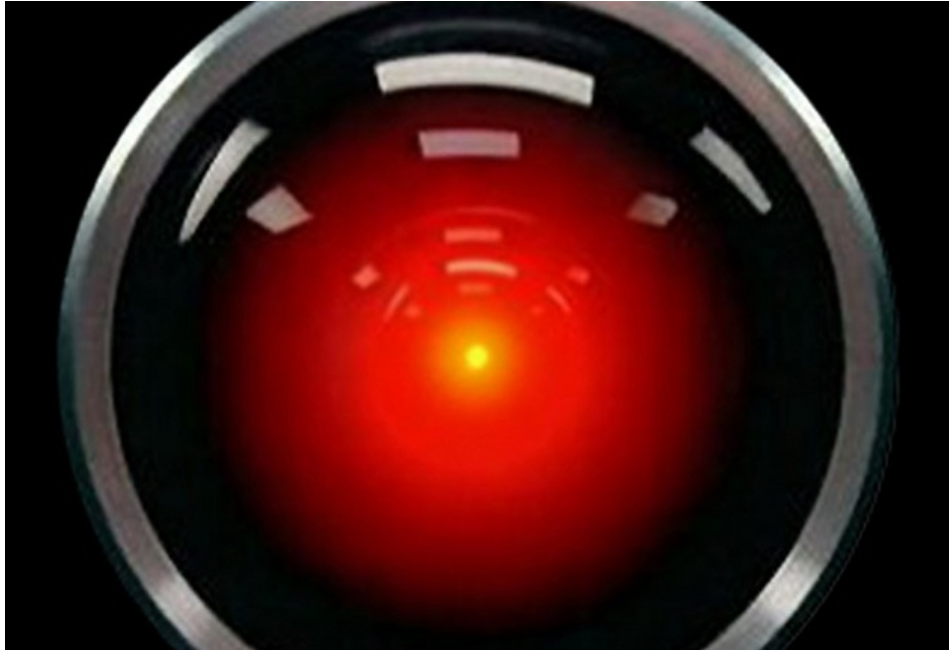


LE CYBERBLUFF A COMMENCÉ

LE 19 JUILLET 2012 PIERRE ALONSO

Le sénateur Jean-Marie Bockel a rendu public le 19 juillet un rapport sur la cyberdéfense. Le volet offensif y occupe une place de choix, en écho aux orientations fixées en 2008. Mais, d'après le rapporteur, trop peu a été fait depuis, et le plus grand secret continue d'entourer les actions offensives dans le cyberspace.



En dire un peu, mais pas trop. L'exercice avait des airs de numéro impressionniste. Le sénateur Jean-Marie Bockel a présenté ce 19 juillet **son rapport sur la cyberdéfense**. En tête des priorités et en bonne place des recommandations figurent les capacités offensives :



Priorité n°1 : (...) : S'interroger sur la pertinence de formuler une doctrine publique sur les capacités offensives. (...)

Recommandation n° 10 : poursuivre le développement de capacités offensives au sein des armées et des services spécialisés.



Le sujet n'est pas nouveau ; il n'est plus du tout tabou. Ces dernières années, les grands-messes ont régulièrement évoqué ce "*cinquième champ de bataille*" qu'est le cyberspace. En premier lieu parce que les États entendent se protéger contre cette nouvelle menace, mais pas seulement. **Le Livre blanc sur la Défense et la sécurité nationale**, rédigé en 2008, notait que "*dans le domaine informatique plus que dans tout autre milieu, il faudra, pour se défendre, savoir attaquer.*"

Doctrine

La même année, **un rapport du Sénat** reprenait cet argument "*technique*" et en ajoutait deux autres en faveur du développement des capacités offensives à "*des fins spécifiquement militaires*" :



**(...) Une telle capacité est très certainement de nature à jouer un rôle dissuasif vis-à-vis d'agresseurs potentiels ;
(...) Enfin, le cyberspace paraît inévitablement voué à devenir un domaine de lutte, au même type que les autres milieux dans lesquels interviennent nos forces armées ; il est légitime d'en tirer les conséquences.**



Jean-Marie Bockel les reprend dans son rapport et s'interroge sur la nécessité de rendre public l'utilisation de ces capacités. *"Le silence des autorités française sur cette questions depuis (...) 2008 paraît quelque peu en décalage avec l'évolution de la menace (...), et il pourrait même être de nature à entretenir des fantasmes dans l'opinion publique"* écrit-il.

Lors de la présentation, il a invité le nouveau président de la République à prendre officiellement position. Les incantations de Nicolas Sarkozy de 2008 pour que la France se dote de *"capacités défensives et offensives"* doivent maintenant être formalisée sous la forme d'une doctrine :



Il faut progresser sur le plan doctrinal d'emploi de cette force. Des discussions théoriques doivent être conduites, la défense nationale est toujours le fruit de débats doctrinaux.



Et d'ajouter sur-le-champ : *"Tout ne doit pas être sur la place publique"* . Par allusions sibyllines, Jean-Marc Bockel a évoqué ces fameuses capacités, dont l'étendue et la nature ne sont pas connue. *"La France n'est pas manchot dans ce domaine"* a-t-il répété.

Industriels

L'État travaille-t-il d'ores et déjà avec des industriels ? Pour la rédaction de son rapport, le sénateur a consulté deux poids lourds du secteur : Thalès et Cassidian, la filiale défense d'EADS. Devant les journalistes, il n'a pas démenti leur participation :



Dans la pratique, oui, il jouent un rôle. Sur le papier, non.



Au sein de l'édifice militaire français, c'est le chef de l'État major particulier, le général Benoît Puga, qui *"pilote"* le volet offensif. Des attaques ? Prudent, Jean-Marie Bockel n'a pas répondu. Sollicités par *Owni*, ni l'État major particulier, intégré à l'Élysée, ni le ministère de la Défense n'ont souhaité commenter.

[Mise à jour, le 20 juillet à 12h : L'État major des armées nous a répondu dans la soirée et renvoyé vers le Secrétariat général de la défense et sécurité nationale (SGDSN), sous l'autorité du Premier ministre. L'Élysée nous a rappelé en fin de matinée le 20 juillet, affirmant que *"les conclusions et propositions du Livre blanc étaient prises en compte"*, y compris dans le domaine offensif, même si aucun *"détail"* ne pouvait être fourni sur ce point. *"La phase de décision finale est un sujet présidentiel"* dans le domaine des cyberattaques comme *"dans les autres domaines, surtout offensifs"* a précisé la présidence par téléphone :



La mise en œuvre revient au SGDSN et à l'Agence nationale de la sécurité des systèmes d'informations (ANSSI).



Sur la doctrine, l'Élysée explique qu'un "travail en continu a été mené depuis le Livre blanc" et qu'elle doit faire la part belle à "l'anticipation".]

État de l'art mondial

Le sénateur et ancien secrétaire d'État à la Défense et aux Anciens combattants fait un état du monde, citant notamment un rapport de **Center for Strategic and International Studies**. 35 pays seraient dotés "d'une doctrine militaire en matière de 'cyberguerre'" à l'instar d'Israël où le ministère de la défense l'a rendue publique. Jean-Marie Bockel a pris ses distances avec l'expression cyberguerre, reconnaissant que ces attaques, "déstabilisatrices", pouvaient constituer "un élément des conflits, comme lors de la guerre entre la Géorgie et la Russie". En tout cas pour l'heure.

Les États-Unis précisent de plus en plus les conditions d'emploi de la force dans le cyberspace. L'année dernière, **le plan de lutte contre la cybercriminalité** publié par la Maison Blanche laissait la porte ouverte à des représailles conventionnelles après une cyberattaque. Cette année, **les révélations du New York Times** sur Olympic Games, le programme secret qui a permis le développement des virus Stuxnet et Flame, ont achevé de convaincre de l'intérêt de Washington pour les dispositifs offensifs, et mordants. Ces deux logiciels malveillants ont ralenti le programme nucléaire iranien en endommageant physiquement les centrifugeuses.

Jean-Marie Bockel était aux États-Unis juste après ces révélations. Une seule question demeurait en suspens : au-delà de la véracité des faits, qui avait intérêt à diffuser ce genre d'informations quelques mois avant l'élection présidentielle, a-t-il rappelé jeudi matin ? Washington a sorti ses muscles. Et il invite la France à faire de même.

Illustration par **Racatumba (CC-by)**

OXONIUM

le 19 juillet 2012 - 19:39 • SIGNALER UN ABUS - PERMALINK

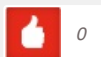


Plutôt que de se concentrer sur le volet "réplique" des cyber-attaques, il serait intéressant que la France se dote de moyens de protection, de détection... Avant même de pouvoir riposter en cas d'attaques, il faudrait s'arranger pour que des cibles de choix (telle que l'Élysée) soit plus ou moins à l'abri. L'actualité récente est édifiante...

Quoiqu'il en soit, nous avons un retard non négligeable quand il s'agit de cyber-défense, mais aussi également un problème de poids dans la gouvernance de l'Internet en général.

Hâte de voir ce qui va se mettre en place sous la nouvelle présidence ;)

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

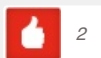
GUILLAUME

le 19 juillet 2012 - 19:51 • SIGNALER UN ABUS - PERMALINK



Il y a aussi sur la question ce petit article "made in" Reflets : <http://reflets.info/rapport-bockel-un-point-sur-la-cyberdefense-francaise/>

VOUS AIMEZ



2

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

TOTO


le 20 juillet 2012 - 16:41 • SIGNALER UN ABUS - PERMALINK



"Stuxnet et Flame[...] ont ralenti le programme nucléaire iranien en endommageant physiquement les centrifugeuses."

nop, seulement le premier, le second c'est pour du vol de data comme on les aime en mode bien gras :)

VOUS AIMEZ  0

VOUS N'AIMEZ PAS  0

LUI RÉPONDRE


JEHV

le 21 juillet 2012 - 3:20 • SIGNALER UN ABUS - PERMALINK



en 2007 ou 2088 la dgse avait aussi "monter" un commando informatique , l'article qui en parle est trouvable sur intelligence-online (payant :(), en 2002/2003 (en plus de la creation d'initiative works chez EADS) une autre initiative avait eue lieu dans la banlieue lyonnaise mais personne pour affirmer ou infirmer cet info :/

VOUS AIMEZ  0

VOUS N'AIMEZ PAS  0

LUI RÉPONDRE


GAPA IP

le 21 juillet 2012 - 9:49 • SIGNALER UN ABUS - PERMALINK



Un article très intéressant. La France a pris du retard dans la lutte contre la cybercriminalité.

VOUS AIMEZ  0

VOUS N'AIMEZ PAS  0

LUI RÉPONDRE

1 ping

Le cyberbluff a commencé. le 23 juillet 2012 - 4:12

[...] le plus grand secret continue d'entourer les actions offensives dans le cyberspace ... lire l'article de Pierre Alonso Partagez cet article : Publié dans Actualité économique, [...]