

Tribune sur la « Cyber défense »

Mars 2010

Par Anselme Trochu, Webconsultant.

Récemment de nombreux medias occidentaux ont évoqué une nouvelle menace sur les systèmes informatiques, popularisant ainsi la notion de « cyber attaque ».

Une folie médiatique s'est en effet déclenchée courant janvier 2010 à la suite de l'affaire concernant le moteur de recherche Google. Le géant américain a accusé presque ouvertement le gouvernement chinois d'être à l'origine de « cyber attaques » qui auraient réussi à pénétrer son réseau ainsi que de nombreuses entreprises nord-américaines et des organisations non gouvernementales de premier plan. Certains experts en sécurité informatique soupçonneraient même les Chinois d'avoir volé une partie de l'algorithme à la base du moteur de recherche de Google. Cet algorithme, l'un des secrets industriels les plus importants du 21eme siècle, est responsable en grande partie de la valorisation de la société.¹

Ce possible vol « virtuel » d'une information ultra sensible expliquerait sans doute la réaction aussi virulente de Google, car c'est la première fois que le leader de l'internet, qui fait l'objet de plusieurs centaines de tentatives d'attaques par jour, réagit aussi fortement

Il est intéressant d'observer les réactions en chaîne qu'a déclenchée cette affaire, et qui ont finalement participé au refroidissement actuel des relations diplomatiques sino-américaines.

Pourtant de nombreux rapports, tel le rapport Grumann² en 2009, avaient bien annoncé que les géants de l'économie américaine avaient déjà subi des attaques, dont certaines avaient réussi. La notion de cyber-attaque n'est pas quelque chose de nouveau, mais pour la première fois depuis quelques années elle commence à être prise au sérieux par la classe politique ; et les medias généralistes commencent aussi à s'y intéresser de près.

Des menaces qui ne sont pas si récentes

Pour se rendre compte des principaux enjeux de la sécurité des systèmes informatiques, il convient de faire un bref rappel chronologique. Des événements clés, officiels ou officieux, ont conduit petit à petit à l'élaboration de nouvelles politiques de « cyber défense ».

En 1982, un pipeline explose dans le Caucase russe suite à une pression anormale. Selon Thomas Reed cette attaque a été commanditée par la CIA, a été rendue possible grâce à l'intrusion de virus informatiques dans le système informatique qui gérait la maintenance du pipeline. Néanmoins cette affirmation a été plusieurs fois mise en doute par des experts en

¹ <http://www.wired.com/threatlevel/2010/02/apt-hacks/>

² http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

sécurité informatique: l'usage de vers informatique pour l'époque semble suspect, qui plus est sur des infrastructures pétrolières qui n'étaient pas autant informatisées qu'aujourd'hui.³

Les Etats-Unis, qui avaient tendance depuis ces dernières années à se considérer comme les leaders dans la sécurité des équipements informatiques, se sont rendu compte que la sécurité de leurs matériels militaires n'était pas aussi avérée.

Ainsi en octobre 2009, l'analyse d'un ordinateur portable d'un insurgé chiite irakien a permis de découvrir des images vidéos filmées par un drone Predator ancienne génération et qui avaient été interceptées par les terroristes par le biais de scans radar sur la fréquence de transmission du drone. En effet ce drone ne cryptait pas sa transmission vidéo.⁴

Ce qui a été surprenant a été tout d'abord de découvrir la vulnérabilité de cet équipement américain qui ne cryptait pas la transmission de données ; mais la surprise a été aussi de constater les capacités de l'ennemi insurgé, estimé jusque là comme ne disposant que de moyens artisanaux. Même si, pour un expert du domaine informatique, le fait d'intercepter des flux d'images non cryptés ne semble pas compliqué, cette action montre une connaissance technique des systèmes d'informations et de transmissions de données qui ne sont pas du domaine du grand public dans les pays du Moyen-Orient.

En 2007, l'Estonie, au cœur d'un conflit diplomatique avec la Russie, est soudain victime d'attaques informatiques violentes qui entraînent la perturbation des sites internet gouvernementaux, jusqu'à causer leur arrêt complet par le biais d'attaques DoS. Même si ces attaques ne sont pas d'une technicité impressionnante pour l'époque, elles révèlent pour la première fois des cybers attaques provenant non plus de groupuscules de la mouvance hacker « black hat » mais plutôt en lien avec des entités visant la réalisation d'objectifs politiques. Le terme d'Advanced Persistent Threat (APT) apparaît petit à petit dans l'univers des entreprises spécialisées en sécurité informatique.

A la suite de cette attaque, l'Estonie a accusé la Russie, réputée particulièrement compétente dans le domaine des attaques informatiques. Cependant, il est à l'heure actuelle difficile d'établir des preuves et une traçabilité fiable en termes de sécurité informatique. C'est ainsi que les accusations de l'Estonie n'ont jamais pu être confirmées par l'Otan.

Les coupures d'électricité qui ont plongé plusieurs millions de personnes dans le noir au Brésil en 2005 et 2007 sont suspectées d'avoir été réalisées par un groupuscule de « hackers indépendants » faisant du chantage au gouvernement de l'époque. Les coupures plus récentes qui ont frappé également le Brésil en novembre 2009, privant d'électricité plus de 50 millions de foyers, ont certes été expliquées officiellement, mais au vu des événements passés et des justifications techniques peu crédibles, certaines personnes supposent une nouvelle fois qu'il s'agissait d'une attaque extérieure.

Ces événements au Brésil ont été fortement médiatisés par un documentaire grand public sur CBS qui développe la thèse des attaques informatiques. Des doutes ont été cependant émis par

³ <http://archives.neohapsis.com/archives/isn/2006-q4/0015.html>

⁴ <http://www.wired.com/dangerroom/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/>

de nombreux experts de la sécurité informatique sur la possibilité d'une véritable cyber attaque.⁵ Quoiqu'il en soit, comme l'écrit Richard Bejtlich⁶, Directeur du département « Incident Response » chez General Electric, aujourd'hui bon nombre d'infrastructures informatiques d'équipements stratégiques demeurent vulnérables face à des experts en attaque informatique.

Enfin, le mardi 15 février 2010, les Etats-Unis font une simulation grandeur nature de « cyber attaques », sous le nom de code « Cyber ShockWave ».⁷ Cette simulation d'attaque, fortement médiatisée, a montré une fois de plus la vulnérabilité de certaines infrastructures (téléphonie, électricité, finances...) aux Etats-Unis.

Des menaces déjà bien identifiées par de nombreux rapports

Des menaces sur la sécurité informatique existent donc bien aujourd'hui et ce n'est que dernièrement qu'elles ont commencé à inquiéter les dirigeants de certains pays. De nombreux rapports ont pourtant mis en avant la nécessité d'établir de nouvelles politiques de « Cyber défense ».

En France, le rapport du sénateur Roger Romani,⁸ de la commission des affaires étrangères et de la défense du Sénat, étudie la réalité de certaines menaces informatiques et insiste sur la nécessité de renforcer la lutte et la protection de manière cohérente dans ce domaine.

Ce rapport revient également sur le manque de moyens déployés par la France, en la comparant à certains voisins européens. Il préconise enfin la mise en place d'une politique nationale puissante et coordonnée.

Dès 2006, le rapport réalisé par le député Laborde montrait également la nécessité de renforcer les moyens dans la sécurisation des réseaux, des équipements stratégiques et des systèmes d'informations.

Le Livre Blanc de 2008 sur la sécurité et la défense nationale a donc prévu le renforcement des moyens de lutte informatique et la mise en place d'une politique de cyber défense, avec la création d'une Agence Nationale de la Sécurité des systèmes d'informations, en charge de diverses missions que nous évoquerons ensuite.

⁵ <http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml>

⁶ <http://taosecurity.blogspot.com/2009/11/reaction-to-60-minutes-story.html>

⁷ <http://www.bipartisanpolicy.org/events/cyber2010>

⁸ Rapport d'information n° 449 (2007-2008) de M. Roger ROMANI, fait au nom de la commission des affaires étrangères, déposé le 8 juillet 2008

Le rapport rédigé pour la commission gouvernementale américaine « US-China Economic and Security Review Commission »⁹ explique très bien que la Chine et la Russie ont déjà plusieurs années d'avance, alors que les Etats-Unis et certaines puissances ne sont qu'au début de la mise en place. D'une certaine manière, l'affaire Google a donné raison à ce rapport.

Malgré ces différents rapports et les propos rassurants des médias sur les capacités de cyber défense des pays occidentaux¹⁰, ces pays manquent encore cruellement de moyens; certains dispositifs sont simplement en cours de mise en place, mais ne sont pas opérationnels. Par exemple, ce n'est qu'au courant de l'année 2010 que sera mis en place en France le centre de détection annoncé dans le Livre Blanc sur la défense et la sécurité, au sein de l'Agence Nationale de la sécurité des systèmes d'information.

On peut aussi supposer que les Etats-Unis ne sont pas encore prêts dans ce domaine. Ce n'est qu'en 2008 que les Etats-Unis ont envisagé la possible création de réseaux botnet. De nombreux experts de la sécurité informatique considèrent les réseaux informatiques des Etats-Unis comme non sécurisés.¹¹

La Lettre hebdomadaire d'informations stratégiques TTU du 20 janvier 2010, rapporte l'avis d'un spécialiste français selon lequel un cyber bataillon de l'armée populaire de libération chinoise serait impliqué dans les attaques contre Google. L'article de TTU reconnaît l'avancée chinoise et la maîtrise par la Chine des différents outils d'une potentielle « cyber guerre ».

Le rapport de septembre 2009 de la société de Sécurité Informatique McAfee met également en avant la grande vulnérabilité des infrastructures informatiques stratégiques¹². Il reconnaît le retard des puissances occidentales face à la Chine et la Russie. Il montre aussi la nécessité d'une relation plus étroite entre gouvernements et experts de la sécurité informatique (comme c'est déjà le cas en Chine) qui permettrait d'améliorer sensiblement les politiques de cyber défense.

En janvier 2010, la société M-trends publie un rapport sur les Advanced Persistent Threat (APT), et attribue les attaques informatiques touchant les gouvernements et les sociétés, non plus à des groupuscules de hackers mais à des Etats. Ce rapport décrit de façon synthétique les méthodes et processus de ces APT.¹³

⁹ "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation" préparé par Northrop Grumman Corporation

¹⁰ http://tempsreel.nouvelobs.com/actualites/vu_sur_le_web/20091118.OBS8148/la_france_aurait_mis_au_point_des_armes_cybernetiques.html

¹¹ http://newsroom.mcafee.com/article_display.cfm?article_id=3617

¹² http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf

¹³ <http://www.mandiant.com/products/services/m-trends>

L'ère du Cloud computing

La « digitalisation » (ou dématérialisation) de l'information et la fameuse tendance « Cloud computing » sont en train de bâtir un monde basé sur l'Internet. En effet tous les secteurs de services en pleine croissance commencent à externaliser leurs données dans la mouvance du Cloud Computing. Jamais le e-commerce ne se sera aussi bien porté et jamais les entreprises n'auront autant communiqué entre elles que par le biais de technologies de réseaux informatiques.

Au début des années 2000 le web était un monde atomisé comprenant de multiples petits acteurs plus ou moins indépendants, avec différentes innovations : période où les start-up avec leurs multiples levées de fond ont fait des fortunés et des malchanceux.

Depuis 2005 le web a commencé à se hiérarchiser et des acteurs très puissants ont émergé en faisant l'acquisition de nombreuses start-up à fort potentiel.

Aujourd'hui, les géants de l'internet, en particulier Microsoft et Google, se livrent à une guerre stratégique. Les fameux réseaux sociaux communautaires ont connu au cours des deux dernières années des valorisations phénoménales, provoquant de nouvelles tendances dans notre manière d'utiliser internet et influençant le développement du Cloud computing.

Les géants de l'internet offrent aujourd'hui principalement des solutions d'hébergement qui sont la base du Cloud Computing. En France par exemple, des clients tels que le Crédit Agricole, TF1, Bouygues Telecom ou le Crédit Immobilier de France hébergent une partie de leurs données grâce à une solution d'hébergement proposée par Microsoft.

On sait également que la suite bureautique Microsoft Office 2010, utilisée par la majorité des entreprises, fonctionnera en ligne.

Beaucoup moins coûteuse pour les entreprises, la tendance du Cloud n'est pas à remettre en question. De plus le phénomène est inéluctable, les poids lourds du web, tels Google, Microsoft, IBM ou HP, considèrent le Cloud comme un nouveau champ de bataille stratégique.¹⁴ En basant en partie sur l'Internet notre façon de consommer et le transfert de l'information numérique, nous dynamisons les échanges et favorisons l'essor du secteur tertiaire.

¹⁴ <http://www.microsoft.com/France/InformationsPresse/Fiche-Communique.aspx?EID=c44959a9-91c1-49c8-8049-3645524c0399>

La nécessité d'une politique de protection d'internet globale et coordonnée.

La tendance du « Cloud » reste néanmoins dangereuse car nous sommes en train d'externaliser les données et les technologies vers un nombre restreint d'acteurs de plus en plus puissants. Le problème n'est pas tant la restriction du nombre d'acteurs mais leur vulnérabilité. Si très peu d'acteurs détiennent au final l'information, comment fera-t-on si l'information n'est soudainement plus disponible ? On peut imaginer la catastrophe économique qui arriverait si, pendant seulement une journée, le service de messagerie proposé aux entreprises par la formule « Google Apps » tombait sous le contrôle d'une cyber puissance mal intentionnée ...

La récente affaire touchant le géant américain Google a peut-être fait comprendre aux différents gouvernements la nécessité de prendre des mesures concrètes vis-à-vis de la sécurité informatique. L'attaque contre Google a ainsi conduit à une nouvelle étroite collaboration entre Google et la National Security Agency.¹⁵

Les cyber-attaques ou APT ne sont plus le fait de groupuscules indépendants illégaux, issus de la mouvance « hacker » mais proviennent de gouvernements dotés d'outils militaires dans le domaine informatique. Désormais c'est de façon quotidienne et non officielle que des Etats sont la cible de cyber attaques de grande envergure. La nécessité d'organismes permettant de définir une politique globale et coordonnée de sécurité informatique apparaît donc évidente.

Bien entendu de nombreuses organisations existent au niveau national.

Au niveau militaire deux programmes importants apparaissent intéressants à citer.

En Juillet 2009 a été créée l'Agence Nationale de la Sécurité des Systèmes d'Informations, dont les effectifs montent en puissance, et qui compte à l'heure actuelle une centaine de personnes. Rattachée au secrétaire générale de la défense nationale ses missions sont multiples. C'est cette agence qui est censé « proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées »¹⁶.

L'OTAN travaille aussi sur la cyber défense par le biais de deux programmes :

- Cyber Defense Management Authority – (CDMA).
- Cyber Defence Centre of Excellence (CCD CoE).

Dans une démarche qui n'est plus militaire mais civile, il existe les « Computer Emergency Response Team » (CERT), qui ont un rôle d'assistance suite aux incidents de sécurité

¹⁵ <http://www.wired.com/threatlevel/2010/02/google-seeks-nsa-help/>

¹⁶ Site officiel : http://www.ssi.gouv.fr/site_article17.html

informatique. Ils sont chapeautés par un organe de coopération qui est le « Forum of incident response and security teams » (FIRST). Leurs compétences à l'heure actuelle sont plus que limitées et en règle générale, les CERT ont une démarche de réaction et non pas d'anticipation.

Des améliorations nécessaires.

Au vu des « cyber attaques » récentes, et même si la crise financière risque de restreindre les moyens alloués aux politiques de cyber défense, un effort rapide est nécessaire en France pour combler le retard face à une menace qui évolue très rapidement. Malgré la présence d'agences aux seins des gouvernements occidentaux, de nombreux challenges restent à relever.

En avril 2009, Rex B. Hughes publie un rapport sur les avancées¹⁷ des objectifs des programmes de cyber défense de l'OTAN rassurant les puissances membres. Il est important de rappeler que ce rapport souligne la récente mise en place de deux unités ; le développement opérationnel n'est donc qu'en train de commencer. Les organismes sont en train d'augmenter leurs effectifs.

L'ANSSI qui est supposé être l'agence gérant la politique de cyber défense au niveau national, n'a pas encore établi le « centre de détection des attaques informatiques » qui semble être la base opérationnelle d'une politique de cyber défense.

Elle ne compterait à l'heure actuelle qu'une centaine d'effectifs, ce qui paraît largement insuffisant pour toutes les missions dont elle est chargée.¹⁸ De plus l'ANSSI ne parle actuellement que de protections des réseaux de l'Etat. Mais qu'en est-il des réseaux informatiques des entreprises privées ayant une forte influence sur notre économie ?

Face à l'avancée considérable des politiques de « cyber attaque » que la Chine semble avoir mis en place, comme l'a rappelé l'affaire Google, il apparaît urgent de prioriser et d'intensifier les missions de l'ANSSI ou d'une autre institution.

La sécurité informatique des équipements stratégiques vitaux pour notre économie nationale, qu'ils soient civils ou étatiques, doit être assurée de façon coordonnée.

Pour cela, L'ANSSI doit continuer sa politique de labellisations de produits de sécurité et de protection des réseaux mais aussi l'élargir au domaine des entreprises privées ayant une forte influence sur Internet. (cf. : collaboration Google et NSA)

¹⁷ <http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf>

¹⁸ <http://www.ttu.fr/francais/frdocpdf/nouvellesmenaces3.pdf>

Au niveau du centre de détection annoncé par le livre blanc et qui apparaît comme l'organe le plus important pour la cyberdéfense, l'agence devra s'immerger complètement dans l'univers de la sécurité informatique. Il faudra donc également prendre en considération la mouvance underground « hacker », qui n'est d'ailleurs pas forcément illégale, dont l'image est négative, et qui n'a jamais fait l'objet d'études sérieuses par une agence étatique jusqu'à présent. Cette mouvance, bien qu'incontrôlable est néanmoins un facteur d'innovation pour la sécurité informatique et contribue régulièrement au développement de technologies. C'est elle qui découvre une grande partie des vulnérabilités informatiques et parfois développe les outils permettant à certains de les exploiter. Un travail de veille et de renseignement doit être effectué. Cependant il ne doit pas être répressif.

L'agence devra également réussir à réunifier l'univers très technique de la sécurité informatique avec les politiques gouvernementales de façon cohérente. (cf. conférence Read write web « les hackers sortent du bois »¹⁹). En effet, une certaine partie de la classe politique française semble complètement déconnectée des innovations et des enjeux concernant la sécurité informatique se laissant guider par des lobbies industrielles pour voter des lois qui sont qualifiées comme absurdes techniquement par des experts de la sécurité. Ainsi la loi Hadopi, a été fortement critiquée en Grande Bretagne par le MI5, car elle rendait plus difficile la recherche de cybercriminels, popularisant les méthodes d'anonymat sur Internet.

Ces quelques rapides suggestions donnent une idée des challenges à relever. Les dernières années ont permis de prendre conscience de la nécessité de réfléchir de façon globale à la sécurité Informatique. L'affaire du « Google gate » a eu le mérite de mettre le débat sur la place publique et de nous faire réaliser la fragilité du monde informatique que nous construisons. Cette affaire a également permis de réaliser que malgré les dires de certains médias mal informés, l'univers du web est vulnérable .

De plus à l'heure actuelle les politiques de cyber défense relèvent du domaine militaire, de par leurs intérêts stratégiques. Il est illusoire de penser que ces politiques, dès qu'elles auront réussi à être opérationnelles, ne développeront pas des technologies de cyber attaque. Ceci n'est pas à remettre en question et est de toute façon inéluctable.

Néanmoins peut-être peut-on imaginer que dans les 10 prochaines années, on pourra observer la mise en place d'un organisme neutre, mandaté par une organisation internationale pour contrôler le développement des technologies numériques et les politiques de sécurisation des réseaux. Une institution ressemblant au fonctionnement et aux missions l'International Atomic Energy Agency mais dans le domaine de l'Internet.

Il n'existe à ma connaissance, aucune institution mondiale, non militaire, indépendante qui permettrait de coordonner les missions évoqués avec de réels moyens.

Anselme Trochu

¹⁹ <http://fr.readwriteweb.com/2009/11/14/analyse/les-hackers-sortent-du-bois-webtv/>

Bibliographie

Rapport d'information de M. Roger ROMANI, fait au nom de la commission des affaires étrangères
n° 449 (2007-2008) - 8 juillet 2008

<http://www.senat.fr/rap/r07-449/r07-449.html>

Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network, Exploitation Prepared for The US-China Economic and Security Review Commission – 9 octobre 2009
http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

In the Crossfire Critical Infrastructure in the Age of Cyber War, Report prepared by Stewart Baker, distinguished visiting fellow, CSIS; partner, Steptoe & Johnson Shaun Waterman, writer and researcher, CSIS George Ivanov, researcher, CSIS - Survey prepared in September 2009
http://newsroom.mcafee.com/images/10039/In%20the%20Crossfire_CIP%20report.pdf

NATO and CyberDefence, Letter prepared by Rex B. Hughes in April 2009
<http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf>

McAfee, Inc. Report Reveals Cyber Coldwar, with Critical Infrastructure Under Constant Cyberattack Causing Widespread Damage - Mc Afee inc, 28 Janvier 2010
http://newsroom.mcafee.com/article_display.cfm?article_id=3617

M-trends report - Report made by Mandiant Intelligent Resource in January 2010
<http://www.mandiant.com/products/services/m-trends>

Bésil : Panne de hacker ou blackout politique ? - Article Paru dans la revue CNIS Mag le 12 novembre 2009
<http://www.cnis-mag.com/bresil-panne-de-hacker-ou-blackout-politique.html>

Insurgents Hack U.S. Drones – Article paru sur le site Internet du Wall Street journal le 17 décembre 2009 par SIOBHAN GORMAN, YOCHI J. DREAZEN et AUGUST COLE
<http://online.wsj.com/article/SB126102247889095011.html>

Hacking The Industrial SCADA Network – Article paru dans le magazine Pipeline and Gas Journal, vol 236 n°11, en novembre 2009 par Frank Dickman
<http://pipelineandgasjournal.com/hacking-industrial-scada-network?page=2>

Conférence Tedx Paris : Rétrospective sur Guy Philippe Goldstein – Paru le site d'information read write web le 15 février 2010.
<http://fr.readwriteweb.com/2010/02/15/divers/retrospective-tedx-paris-guyphilippe-goldstein/>

Cloud Computing et services hébergés : Microsoft affiche son dynamisme sur le marché professionnel – Communiqué de presse publié par Microsoft sur son site Officiel le 8 février 2010.

<http://www.microsoft.com/France/InformationsPresse/Fiche-Communique.aspx?EID=c44959a9-91c1-49c8-8049-3645524c0399>

The Complete Guide To Microsoft's Office 2010 – Article publié par Leena Rao sur le site Tech Crunch le 13 juillet 2009.

<http://techcrunch.com/2009/07/13/the-complete-guide-to-microsofts-office-2010/>

Page official du service de messagerie gratuite à distance de Google Apps propose a plus de 2 millions d'entreprises.

http://www.google.com/apps/intl/fr/business/index.html#utm_campaign=fr&utm_source=fr-ha-emea-fr-bk&utm_medium=ha&utm_term=google%20apps

Google Asks NSA to Help Secure Its Network – Article de Kim Zetter paru le 4 février 2010 sur le site Internet Wired.

<http://www.wired.com/threatlevel/2010/02/google-seeks-nsa-help/>

Les Hackers sortent du bois #webtv – Emission réalisé par techtoch tv publié par ReadWriteWeb le 14 novembre 2009

<http://fr.readwriteweb.com/2009/11/14/analyse/les-hackers-sortent-du-bois-webtv/>

Infrastructure vulnerable to hacker attacks - Article de Bob Keefe paru dans le Atlantic Journal Constitution le 10 Janvier 2006

<http://archives.neohapsis.com/archives/isn/2006-q4/0015.html>

Les nouveaux agents de la Guerre froide numérique – Article paru sur Slate.fr par Olivier tesquet le 7 février 2010.

<http://blog.slate.fr/declassifies/2010/02/07/les-nouveaux-agents-de-la-guerre-froide-numerique/>

Insurgents Intercept Drone Video in King-Size Security Breach (Updated, with Video) - Article paru sur Wired.com le 17 décembre 2009 par Noah Shachtman

<http://www.wired.com/dangerroom/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/>

Hadopi freine la lutte contre le piratage, selon le MI5 – Article paru sur Slate.fr le 29 octobre 2009

<http://www.slate.fr/story/12353/hadopi-freine-la-lutte-contre-le-piratage-selon-le-mi5>

Mission de l'ANSSI – Site Officiel de l'ANSSI

http://www.ssi.gouv.fr/site_article17.html

Pentagon signs off on Cyber Command – Article paru le 24 juin 2009 sur Security focus par Robert Lemos

<http://www.securityfocus.com/brief/978>