

## La cybersécurité, priorité de l'année 2013 ?

Publié le vendredi 1er février 2013

Voir en ligne : <https://www.france-science.org/La-cybersecurite-priorite-de-l.html>

Nouvelle année, nouveaux mandats. Les résolutions sont donc de mise et le Congrès n'y échappe pas non plus. Pourtant, les élections ont quelque peu bouleversé le Sénat et la Chambre des Représentants, dont le renouvellement s'est effectué en même temps que l'élection présidentielle, c'est-à-dire début novembre 2012. Malgré l'absence du sénateur Joe Lieberman (Indépendant - Connecticut), grand partisan du projet de loi sur la cybersécurité (voir BE Etats-Unis 302, Cybersécurité : le prochain 11 septembre sera numérique" [1]) qui a failli passer lors de la dernière session 2012 du Congrès et depuis succédé par le sénateur Chris Murphy (Démocrate - Connecticut), la cybersécurité refait surface dans le Capitole. Cette fois-ci, ce sont quelques sept sénateurs démocrates, dont les sénateurs John D. Rockefeller VI (Démocrate - West Virginia), Tom Carper (Démocrate - Delaware) et Dianne Feinstein (Démocrate - California), qui ont relancé le débat.

### S.21, le congrès invité à étudier une loi sur la cybersécurité

En diffusant la déclaration (Statement 21 [2]) sur la "Loi sur la Cybersécurité et la Cyber Compétitivité Américaine de 2013", le sénateur Rockefeller souhaite que le nouveau Congrès saisisse l'opportunité d'obtenir un consensus bipartisan législatif afin de renforcer la cybersécurité de la Nation [3]. Cette déclaration souligne le fait que les secteurs privés et publics doivent travailler ensemble pour traiter des dangers liés aux cyber-attaques. Elle insiste sur le fait que les brèches concernant la législation sur le domaine de la cybersécurité posent "une des menaces les plus sérieuses et grandissantes au niveau de la sécurité nationale ainsi que de l'économie des Etats-Unis".

Afin de renforcer sa proposition, le sénateur Rockefeller IV a écrit aux PDG de chacune des entreprises du classement Fortune 500 afin de recueillir leurs points de vue sur le sujet [4]. Selon lui, les réponses ainsi obtenues semblent appuyer le fait que "les cyber menaces auxquelles nous faisons face sont réelles et que le gouvernement fédéral doit jouer un rôle important en matière d'évolution de la cybersécurité pour la nation". La proposition a aussi obtenu le soutien de personnalités importantes de l'administration telles que la Secrétaire du DHS (Département de la Sécurité Intérieure) Janet Napolitano, le secrétaire du Département de la Défense (DoD) Leon Panetta ou encore le Directeur de la NSA (Agence de Sécurité Nationale) le Général Keith Alexander, qui s'inquiètent de la sécurité des infrastructures critiques [5]. Car en parallèle des réseaux gouvernementaux, les réseaux des installations de companies pétrolières ou gazières, des banques, des centrales électriques, ou nucléaires sont aussi régulièrement attaqués.

### La Cybersécurité est un secteur de la Défense à part entière

Les efforts du congrès ainsi que des diverses agences impliquées dans la cybersécurité pour sensibiliser les autorités semblent porter leurs fruits. Ainsi, Obama a ratifié le 3 janvier la National Defense Authorization Act (NDAA), une loi annuelle spécifiant le budget et les dépenses du Département de la Défense américaine pour l'année fiscale. Cette loi approuve donc un budget total de 633 milliards de dollars alloué au Département de la Défense, dont 3,4 milliards de dollars dédiés aux activités liées au cyberspace [6]. Cette loi impose aussi au Département de la Défense de rapporter au Congrès chaque trimestre toutes les attaques initiées ainsi que les principales opérations défensives liées à la cybersécurité.

Lors de la conférence sur la sécurité analytique d'IBM le 15 janvier dernier, John McLaughlin, Architecte Sécurité chez IBM, présentait la sécybersécurité comme "le cinquième département du Département de la Défense, au même titre que le département de l'Armée (Us Army), de la Marine (US Navy), de la Force Aérienne (US Air Force) ou de l'Agence Spaciale (NASA)". Ainsi, le département de la cybersécurité serait lui-même composé de trois grands secteurs : la protection des systèmes d'information nationaux et industriels, la protection des réseaux gouvernementaux ainsi qu'un secteur de mission de combat qui serait destiné à porter des attaques à l'extérieur.

Ces trois secteurs définiront ainsi les nouvelles divisions du US Cyber Command, le commandement chargé de la sécurité de l'Information de l'armée. C'est d'ailleurs le Général Keith Alexander, Directeur de la NSA, qui en a la charge. Comportant près de 900 personnes à l'heure actuelle, le Département de la Défense est sur le point de multiplier par cinq le nombre de ces employés [7]. Ainsi dans les cinq prochaines années, c'est quelques 4900 personnes qui pourraient être affectées à la cybersécurité afin de préparer les futures armes numériques et autres cyberdéfenses. Ce "cinquième département" sera composé d'experts en sécurité civils et militaires qui travailleront donc autant sur des opérations offensives que sur le renforcement des protections des réseaux critiques.

Cette information n'a pas encore été officialisée par le Département de la Défense [8], mais elle soulève déjà quelques interrogations. Où trouver 4000 talentueux experts en cybersécurité ? Car si les besoins en personnels qualifiés sont bien réels, ceux-ci sont peu nombreux et hautement sollicités, autant par les agences fédérales que par les industriels [9]. C'est ce que rappelait plutôt ce mois-ci Mark Weatherford, sous-secrétaire adjoint à la cybersécurité au DHS : "Nous ne formons pas assez d'experts en cybersécurité. Nous manquons donc de jeunes talents et ceci est un problème d'envergure nationale. Il nous faut essayer de former de jeunes gens qui puissent être capables de penser comme les hackers mal intentionnés".

La cybersécurité est donc une des grandes préoccupations de ce début d'année. Pas une seule conférence informatique ne se déroule sans y faire référence. L'ampleur des risques est encore certainement sous-estimée lorsque l'on voit que certains malwares découverts récemment frappaient impunément les réseaux du monde entier depuis plusieurs années. Le dernier en date, Octobre rouge [10], sévissait ainsi depuis plus de cinq ans. Combien d'autres sont à découvrir ? Combien d'autres seront créés d'ici là ? Et l'alerte lancée par de multiples personnalités sur la formation d'experts en cybersécurité n'est pas nouvelle, mais elle s'intensifie à mesure que les autorités réalisent l'ampleur des travaux à engager. L'informatique semble écrire un nouveau chapitre de l'Histoire, et l'histoire semble bien ne faire que commencer...

#### Sources :

- "Democrats : Cybersecurity legislation a priority in New Congress" - Hillicon Valley - 23/01/2013 - <http://thehill.com/blogs/hillicon-valley/technology/278879-democrats-cybersecurity-legislation-a-priority-in-new-congress>
- "Obama signs 2013 National Defense Authorization Act" - Alabama.com - 03/2013 - [http://blog.al.com/huntsville-times-business/2013/01/obama\\_signs\\_2013\\_national\\_defe.html](http://blog.al.com/huntsville-times-business/2013/01/obama_signs_2013_national_defe.html)
- "New Defense Budget Aims To Improve Cybersecurity" - InformationWeek - 04/01/2013 - <http://www.informationweek.com/government/security/new-defense-budget-aims-to-improve-cyber/240145571>

#### Pour en savoir plus, contacts :

- [1] "Cybersécurité : le prochain 11 septembre sera numérique" - BE Etats-Unis 302 - 14/09/2012 - <http://www.bulletins-electroniques.com/actualites/70957.htm>
- [2] "S.21, the Cybersecurity and American Cyber Competitiveness Act of 2013." - Site Internet de la Commission du Sénat sur le Commerce, la Science et le Transport - 23/01/2012 - [http://commerce.senate.gov/public/?a=Files.Serve&File\\_id=b678eb9a-b5c1-4540-aca3-3e857c7627da](http://commerce.senate.gov/public/?a=Files.Serve&File_id=b678eb9a-b5c1-4540-aca3-3e857c7627da)
- [3] "Comprehensive Cybersecurity Bill Will Be Priority This Congress"- Site Internet de la Commission du Sénat sur le Commerce, la Science et le Transport- 23/01/2013 - [http://commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord\\_id=7a7124d7-190c-4160-abf3-4012c2db737c](http://commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=7a7124d7-190c-4160-abf3-4012c2db737c)
- [4] "Fortune 500 Companies to Rockefeller : Cybersecurity is a priority" - Site Internet de la Commission du Sénat sur le Commerce, la Science et le Transport - 30/01/2013 - [http://commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord\\_id=a7724495-5435-438d-8fc6-286219a5cf1d](http://commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=a7724495-5435-438d-8fc6-286219a5cf1d)
- [5] "Report : Pentagon to Increase Cybersecurity Staff" - CRN - 28/01/2013 - <http://www.crn.com/news/security/240147142/report-pentagon-to-increase-cybersecurity-staff.htm>
- [6] "Cybersecurity News Round-Up : 2013 Defense Budget Outlines New Mandates to Enhance Cybersecurity" - clearancejobs.com - 07/01/2013 -

<http://www.clearancejobs.com/defense-news/1048/cybersecurity-news-round-up-2013-defense-budget-outline-s-new-mandates-to-enhance-cybersecurity>

- [7] "Pentagon to boost cybersecurity force" - WashingtonPost - 28/01/2013 - [http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/19/d87d9dc2-5fec-11e2-b05a-605528f6b712\\_story\\_1.html](http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/19/d87d9dc2-5fec-11e2-b05a-605528f6b712_story_1.html)

- [8] "DoD : No formal decision on expanding cyber command, yet" - Foreign Policy website - 28/01/2013 - [http://killerapps.foreignpolicy.com/posts/2013/01/28/dod\\_no\\_formal\\_decision\\_on\\_expanding\\_cyber\\_command\\_yet](http://killerapps.foreignpolicy.com/posts/2013/01/28/dod_no_formal_decision_on_expanding_cyber_command_yet)

- [9] "Pentagon hiring binge won't guarantee more security" - Network World - 29/01/2013 - <http://www.networkworld.com/news/2013/012913-pentagon-hiring-binge-wont-guarantee-266215.html?page=2>

- [10] "Octobre rouge, ce malware qui volait des données depuis cinq ans" - Gizmodo.fr - 28/01/2013 - <http://www.gizmodo.fr/2013/01/28/octobre-rouge-malware-vol-donnees-cinq-ans.html>

- "FY2013 Defense Budget request" - US Department of Defense - 04/02/2012 - [http://comptroller.defense.gov/defbudget/fy2013/FY2013\\_Budget\\_Request\\_Overview\\_Book.pdf](http://comptroller.defense.gov/defbudget/fy2013/FY2013_Budget_Request_Overview_Book.pdf)

Code brève

ADIT : 72151

### **Rédacteurs :**

- Thomas Debacker (deputy-ntics@ambascience-usa.org) ;

- Retrouvez toutes nos activités sur <http://france-science.org> ;

- Suivre le secteur Nouvelles Technologies de l'Information, Communication, Sécurité sur twitter @MST\_USA\_NTICS.