http://www.developpez.com/actu/108315/La-France-annonce-la-creation-d-un-cyber-commandement-soutenu-par-3-200-combattants-numeriques-et-4-400-reservistes-de-cyberdefense-d-ici-2019/

Developpez.com est un site spécialisé à destination des « développeurs » de sites internet et de personnes particulièrement intéressées par les aspects techniques. [YD]

La France annonce la création d'un cyber-commandement

Soutenu par 3 200 combattants numériques et 4 400 réservistes de cyberdéfense d'ici 2019

Le 13 décembre 2016, par Olivier Famien, Chroniqueur Actualités

En 2014, Reuters rapportait qu'un ex-hacker engagé dans l'unité spéciale de cyber espionnage de la Corée du Nord, lui aurait confié que le gouvernement nord-coréen aurait mis en place une agence gouvernementale baptisée Bureau 121 et qui contiendrait plus de 1 800 hackers aussi doués que les programmeurs de Google ou de la CIA, si ce n'est mieux.

Un an plus tard, et plus précisément en mars 2015, des documents top secret tombés entre les mains de CBC News et The Intercept ont permis de faire la lumière sur la volonté de l'agence du renseignement canadienne dénommée SEC (Communications Security Establishment Canada) de devenir plus agressive en se dotant de plusieurs outils capables de rediriger quelqu'un vers un faux site, de voler des informations privées, de surveiller les activités des internautes, de perturber les téléchargements, d'infecter la machine d'un internaute pour copier les données stockées sur son disque dur, de pirater les réseaux pour brouiller les activités de l'agence et créer des troubles sur internet en prétendant être un autre gouvernement ou un hacker et bien plus encore.

Un mois après les révélations inhérentes aux intentions de cyber armement du Canada, ce sont les États-Unis qui ont pris le devant des choses en présentant ouvertement la stratégie de son département de défense sur les cinq années à venir et qui vise à mettre en place une force de cyber mission de 6 200 personnes composées de militaires, civils, entités des autres agences de gouvernements, etc.

Ce n'est donc plus un secret que chaque pays prépare ses armes aussi bien défensives qu'offensives dans le cyberespace afin de protéger ses intérêts. La France qui n'est pas en reste a annoncé hier par la voix de son ministre de la défense, Jean-Yves Le Drian, lors de sa visite à la direction générale de l'armement — maîtrise de l'information, le renforcement de ses capacités dans le cyberespace qui passe par la définition d'une nouvelle doctrine de cyberdéfense soutenue par la création d'un cyber-commandement.

Durant cette visite, le ministre de la Défense a soutenu que « *de la même manière que l'émergence de l'aviation au début du XXe siècle a profondément transformé la doctrine militaire […], de même il me semble aujourd'hui indispensable de développer une doctrine et une stratégie cyber de défense, et d'intégrer l'ensemble des volets cyber dans notre pensée militaire* ».

Pour Le Drian cette nouvelle stratégie s'articule autour de trois missions principales, à savoir « les missions de renseignement et investigation, celles de protection/défense, celles de riposte et neutralisation ».

La première mission qui est le renseignement a pour objectifs de contribuer à « *identifier nos failles ou nos vulnérabilités potentielles, détecter des actions hostiles dans le cyberespace, de les caractériser et éventuellement d'en trouver la source, de mener les investigations nécessaires pour attribuer une attaque, la caractériser, en déterminer les effets, et en découvrir les motivations, de*

participer aux actions de remédiation, de contribuer à préparer, de planifier et soutenir les actions offensives », a expliqué le ministre de la Défense.
La seconde mission qui est la cyberdéfense consiste en un ensemble des mesures prises pour réduire les risques qui peuvent concerner les systèmes utilisés sur le territoire français ou en opérations extérieures.

La troisième et dernière mission a pour objet de fournir des solutions offensives afin de riposter à une attaque et neutraliser l'ennemi. Ces armes offensives doivent permettre au ministère de la Défense française de s'introduire dans les systèmes ou les réseaux de ses ennemis, afin d'y causer « *des dommages, des interruptions de service ou des neutralisations temporaires ou définitives, justifiés par l'ouverture d'hostilité* » à son endroit. Pour justifier ses actions, le ministère de la Défense entend s'appuyer sur la réglementation française qui « *a été récemment modifiée pour permettre des actions de neutralisation, en particulier des effets d'attaques informatiques visant des systèmes d'information particulièrement sensibles* », mais aussi sur la réglementation internationale qui stipule qu'en « *cas d'attaque informatique transitant par des infrastructures ou par le territoire d'un État qui n'aurait pas empêché une telle utilisation, alors même qu'elle visait à commettre un acte internationalement illicite, la responsabilité de cet État pourrait être mise en jeu et justifier l'édiction de contre-mesures* ».

En outre, pour soutenir cette nouvelle stratégie de cyberdéfense, Le Drian a annoncé la création d'un commandement des opérations cyber (CYBERCOM) au sein du ministère de la Défense. Ce commandement « *assistera le ministre en matière de cyberdéfense et sera placé sous la responsabilité directe du chef d'état-major des armées* ». « *Il disposera d'un état-major resserré et aura autorité sur toutes les unités opérationnelles spécialisées dans la cyberdéfense du ministère, appartenant à toutes les armées, directions et services, soit 2600 personnes, c'est-à-dire 2600 combattants numériques en 2019, auxquels s'ajouteront les 600 experts de la DGA* ». En plus de ces ressources, ce commandement pourra également compter sur 4400 réservistes de cyberdéfense, soit 4 000 réservistes citoyens de cyberdéfense, et 400 réservistes opérationnels.

Source : Ministère de la Défense

Et vous ?

- Que pensez-vous de la nouvelle stratégie de cyberdéfense du ministère de la Défense française ?

- Pourra-t-elle atteindre ses objectifs ?

- Ces nouveaux types de combattants seront-ils à la hauteur face aux attaques de plus en plus sophistiquées ?

Voir aussi

- 1 800 hackers nord-coréens prêts pour une cyberguerre, ils seraient aussi compétents que les meilleurs programmeurs de Google ou de la CIA

- Cyberguerre : les États-Unis préparent leur arsenal pour riposter aux attaques, 6200 personnes seront recrutées pour répliquer

- L'arsenal de « cyberguerre » du CSEC révélé, les capacités de l'agence canadienne vont au-delà du simple espionnage

- Forum Actualités, Wiki Developpez.com, Débats Best of, FAQ Developpez.com