La cyberdéfense militaire américaine, un exemple pour la France ?

Michel Baud

Juillet 2013 – Article n°III.8

Depuis de nombreuses années, dans le cadre militaire, l'approche officielle française en matière de cyber s'est focalisée sur une réponse défensive face aux menaces. Pour faire face aux vulnérabilités introduites par la numérisation des armées au travers de ses états-majors et de ses équipements, ce type de réponse semblait le mieux adapté.
Si cette conception peut s'expliquer aisément dans le milieu civil, où il est difficilement concevable d'avoir recours à des modes d'action offensifs pour se défendre face à une cyberattaque, cette approche uniquement défensive semble moins évidente dans un cadre militaire. En effet, culturellement, le soldat qui a pour mission de défendre les intérêts de la Nation, peut faire usage de violence légitime au nom de l'État et utiliser ses armes dans un cadre qui ne se limite pas à l'auto-défense.
En 2008, si le précédent Livre blanc a annoncé que « dans la mesure où le cyberespace est devenu un nouveau champ d'action dans lequel se déroulent déjà des opérations militaires, la France devra développer une capacité de lutte dans cet espace »[1], cet engagement n'a pas eu de traduction militaire concrète par la mise sur pied d'unités cyberoffensives. Ne pas posséder d'unités militaires régulières capables de mener ce type d'action ne veut pas pour autant dire que la France ne dispose pas de ces capacités. Lors de la présentation à la presse de son rapport « la cyberdéfense : un enjeu mondial, une priorité nationale » le 19 juillet 2012, le sénateur Jean-Marie Bockel a révélé, à propos de ces capacités offensives, que « dans ce domaine, on n'est pas manchots ». Non officielles, ces capacités seraient donc actuellement mises en œuvre par les services spéciaux.
En 2013, le nouveau Livre blanc qui définit notre stratégie de défense met l'accent sur la nécessité de se doter « d'une organisation de cyberdéfense étroitement intégrée aux forces, disposant de capacités défensives et offensives pour préparer ou accompagner les opérations militaires »[2]. Une nouvelle étape semble donc franchie vers la traduction concrète de cette volonté politique par une organisation militaire adaptée à ces enjeux.

L'exemple Américain

Avec quelques années de retard la France semble donc suivre la voie ouverte par les Américains en matière de cyberdéfense. Initialement axé sur des opérations défensives, le spectre des missions dévolues aux armées des États-Unis s'est progressivement étendu aux actions offensives.
Cette politique se concrétise par la création en 2010 du Cyber Command. Ce haut commandement américain « planifie, coordonne, intègre, synchronise et conduit des actions pour commander les opérations et la défense de certains réseaux d'information du Département de la Défense ; prépare et,

[1] *Défense et Sécurité nationale, le Livre blanc*, Paris, La documentation française, 2008, page 53.
[2] *Livre blanc Défense et sécurité nationale*, Direction de l'information légale et administrative, Paris, 2013, page 94.

au besoin, conduit, tout le spectre d'opérations militaires du cyberespace dans le but de permettre des actions dans tous les domaines, assurer la liberté d'action des États-Unis et de leurs alliés dans le cyberespace, et l'interdire à nos adversaires »[3]. Initialement, à la date de création du Cyber Command, les militaires américains peuvent mener des actions défensives ou bloquer des attaques uniquement sur leurs propres réseaux[4].

En 2012, le Pentagone a proposé que les cyberspécialistes militaires puissent agir hors de leurs réseaux dédiés pour pouvoir défendre les réseaux informatiques critiques américains, à condition que ces opérations répondent à des critères très restrictifs, critères qui selon certains analystes paralysaient toute capacité d'action[5]. C'est une première étape qui élargit le domaine d'action de cette grande unité militaire. C'est aussi le constat d'une vulnérabilité face au cyber, vulnérabilité qui ne peut se résoudre par une exclusive cyberdéfense, et qui nécessite le développement d'un discours basé sur la cyber-dissuasion[6].

La situation évolue encore en 2013, avec une appropriation très claire des missions offensives, non seulement sur le territoire américain mais aussi sur le reste du globe. Auditionné par le Sénat américain, le général Keith B. Alexander, commandant du Cyber Command, décrit la mission des 13 unités cyber offensives chargées de la dissuasion face aux cyberattaques destructives dont peuvent être victimes les États-Unis : « Laissez-moi être clair, ces *Unités de défense de la Nation* ne sont pas des unités défensive, ce sont des unités offensives que le Département de la Défense peut utiliser pour défendre le pays si nous sommes attaqués dans le cyberespace ». En complément de cette première force, le Cyber Command met sur pied 27 unités qui vont fournir une assistance pour la planification de cyberopérations au profit des états-majors opérationnels déployés sur l'ensemble du globe[7]. D'après le Vice-amiral Michael Rogers, chef des forces cyber de la Marine américaine, les commandants de théâtre ont maintenant le choix dans leurs modes d'action entre la guerre électronique, le cyber ou les actions cinétiques ; les cyberarmes doivent être intégrées avec les autres outils dont ils disposent comme un moyen pour remplir leurs missions[8].

Une dynamique identique

Militaires américains et français semblent donc suivre une stratégie identique. Après une réponse défensive, ils développent aujourd'hui des capacités offensives qui ont deux objectifs : assurer une dissuasion conventionnelle face à un adversaire qui envisagerait d'utiliser le cyberespace, et doter les forces militaires de moyens d'action permettant d'agir dans ce nouveau champ de bataille. Pour tenir compte de ces évolutions stratégiques, la chaine cyber française va devoir évoluer pour être à même de remplir les nouvelles missions qui lui seront confiées.

---

[3] Us Department of Defense, U.S. Cyber Command fact sheet, published by the U.S. Department of Defense Office of Public Affairs, le 25 mai 2010.

[4] Ellen Nakashima, « Pentagon proposes more robust role for its cyber-specialists », *The Washington Post*, 10 août 2012, page consultée le 08 avril 2013 à l'adresse: <http://www.washingtonpost.com/world/national-security/pentagon-proposes-more-robust-role-for-its-cyber-specialists/2012/08/09/1e3478ca-db15-11e1-9745-d9ae6098d493_story.html>.

[5] Ellen Nakashima, Op cit.

[6] Entretien avec le Lieutenant-colonel Patrice Tromparent, Délégation aux Affaires Stratégiques, le lundi 15 avril 2013.

[7] U.S. Senate, Committee on Armed Services, « Hearing to receive testimony on U.S. strategic command and U.S. cyber command in review of the defense authorization request for fiscal year 2014 and the future years defense program », Additional statements for the record full transcript, page 08, Mardi 12 mars 2013, consulté le 18 avril 2013 à l'adresse: <http://www.armed-services.senate.gov/hearings/event.cfm?eventid=0daf354e2970a9db3a6d0023abe58a27>

[8] John Reed, *U.S. military working to integrate cyber weapons into commanders' arsenals*, *Foreign Policy / National security*, le 09 avril 2013, consulté le 10 avril 2013 à l'adresse: <http://killerapps.foreignpolicy.com/posts/2013/04/09/us_military_starting_to_integrate_cyber_weapons_into_commanders_arsenals#.UWUwgOWglhw.twitter>.

La chaîne de cyberdéfense opérationnelle française est actuellement commandée par un officier général en charge de la cyberdéfense qui est intégré au CPCO[9] pour la planification et la conduite des opérations. Il est secondé par un Officier en lutte informatique central (OLID) qui pilote la montée en puissance du domaine cyber dans les armées, l'action des entités cyber interarmées (CALID[10]) et propres aux armées. Une équipe de direction met en œuvre les décisions prises par l'OG Cyber. Dans sa mission celui-ci peut s'appuyer sur le CALID qui est le centre d'expertise du ministère de la défense. C'est le centre d'alerte et de réaction aux attaques informatiques (CERT[11]) du ministère de la défense qui assure des missions de surveillance et de détection H24 des cyberattaques visant les armées. Au total l'effectif de la chaîne centrale cyber représente une centaine de personnes, ce qui est, toutes proportions gardées, relativement modeste par rapport aux États-Unis dont l'objectif est d'atteindre un effectif de 4 900 personnes pour le Cyber Command[12].

Au final, les armées françaises sont maintenant confrontées aux difficultés de mise en place d'une telle structure, structure qui pourrait s'inspirer des *Unités de défense de la Nation* américaine. Ces unités seraient systématiquement déployées avec les états-majors de niveau 1 et 2 pour les appuyer dans leurs missions, et offrir des capacités d'action complètes dans le domaine cyber, à la fois défensives mais aussi offensives. Plusieurs défis restent à relever dont celui du recrutement, de la formation et de la fidélisation d'experts informatiques capables de mener de telles opérations. Ce type de spécialiste reste particulièrement convoité. Dans le civil le niveau de rémunération dépasse celui proposé par l'institution militaire, ce qui rend leur recrutement difficile. Recrutement d'autant plus difficile, qu'en 2013, une estimation haute donne le chiffre de 38 000 postes à pourvoir en France dans l'ensemble du secteur informatique[13].

[9] Centre de Planification et de Conduite des Opérations.
[10] Centre d'Analyse en Lutte Informatique Défensive.
[11] Computer Emergency Response team.
[12] Elisabeth Bumiller, « Pentagon expanding cybersecurity force to protect networks against attacks », The New York Times, le 27 janvier 2013, consulté le 04 avril 2013 à l'adresse: <http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html?_r=1&>.
[13] Ingrid Lemelle, « Un recrutement sur quatre dans l'informatique », La Dépêche.fr, 18 mars 2013, consulté le 04 avril 2013 à l'adresse : <http://www.ladepeche-emploi.fr/edito/actualite-ladepeche/article/un-recrutement-sur-quatre-dans-linformatique.html>.