CHAIRE DE
CYBERDÉFENSE ET
CYBERSECURITÉ

American military cyberdefense, an example for France?

Michel Baud

July 2013 – Article n°III.8

For many years, from a military standpoint, the official French policy in cyber-matters has focused on defensive responses to threats. To face vulnerabilities induced by digitalization of armies through its staff and equipment, this type of response seemed the most adapted.
If this conception seems sensible in civilian matters, where offensive means to face a cyberattack can hardly be considered, a purely defensive stance doesn't seem quite as obvious in a military environment. Indeed, culturally speaking, the soldier has the mission of defending the nation's interests, and is entitled to use lawful violence in the name of the state to that end, and to bear and use arms to an extent which exceeds self-defense.

In 2008, the last "White book" announced that "insofar as cyberspace has become a new battleground on which military operations are already taking place, France will have to develop a battle capacity in that space"[1], this statement was not followed by actual military implementation and the setting up of cyberoffensive units. Not having regular military units capable of performing this type of action does not mean that France doesn't have that type of capacity. During the press presentation of his report on "Cyberdefense: a global challenge, a national priority", on July 19th, 2012, Senator Jean-Marie Bockel, revealed, regarding those offensive capacities, that we were "no weaklings on that field". Unofficially, those capacities would therefore be within special service's responsibilities.

In 2013, the new White Book which defines our defense strategy stresses the need for acquiring "a cyberdefense organization, deeply rooted into forces, with defensive and offensive capacities, to prepare and accompany military operations"[2]. A new stage seems to have been reached towards the implementation of this political goal into a military organization, adapted to these challenges.

The American example

A few years behind, France therefore seems to follow Americans on the cyberdefense path. Initially hinging on defensive operations, the array of missions handed to American Armies progressively spread into offensive actions.

This policy is embodied by the 2010 creation of cybercommand. This American high command "plans, coordinates, integrates, synchronizes and manages actions to prepare operations and the defense of certain Department of Defense information networks; prepares and

[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.

If need be, leads the entire array of cyberspace military operations, so as to enable operations on all fields, ensure the freedom of action of the United States and its allies in cyberspace, and deprive our adversaries of it"[3]. Initially, upon creation of Cyber Command, the American military could lead defensive actions or block attacks only on their own networks[4].

In 2012, Pentagon suggested that military cyberspecialists may be allowed to act out of their dedicated networks, in order to defend critical American computer networks, under the condition that those operations be filtered with strict criteria, so strict that some analysts predict that they would paralyze any military capacity[5]. It is a first step to broaden the playground of this large military unit. It also highlights the acknowledgement of vulnerability on the cyber-front, a breach which cannot be solely filled with cyberdefense alone, and which requires the conception of a policy based on cyber-deterrence[6].

The situation evolved yet again in 2013, with a very clear attribution of offensive missions, not only on American soil but also on the rest of the globe. Auditioned by the American Senate, General Keith B. Alexander, Cyber Command chief, described the 13 cyber-offensive units in charge of deterrence to face the destructive cyber-attacks which could target the United States:"Let me be clear, these *Nation defense Units* are not defensive units, they are offensive units which the Department of Defense can deploy to protect the country if we are attacked within cyberspace". Additional to this first force, Cyber Command put together 27 units to assist in planning cyberoperations, in support to operational command, deployed home and abroad[7]. According to vice-admiral Michael Rogers, commander in chief of cyber forces in the American Navy, theater commanders now have the choice their mode of action between, electronic, cyber or kinetic warfare; cyber-weapons must be integrated with the other means they possess to carry their missions out[8].

A similar momentum

The American and French military therefore seem to be following the same strategy. After a defensive response, they are today developing offensive capacities, with two objectives: maintain conventional deterrence facing an adversary who would consider using cyberspace, and fit military forces with the means necessary to act on this new battlefield. To take these strategic evolutions into account, the French cyber chain will have to adapt, so as to remain able to carry out the missions it will receive.

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

[4] Ellen Nakashima, « Pentagon proposes more robust role for its cyber-specialists », *The Washington Post*, 10 août 2012, page accessed on April 8, 2013 @: <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] Interview with Lieutenant-colonel Patrice Tromparent, Strategic affairs delegation, Monday, April 15 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, March 12, 2013, accessed on April 18, 2013 @ 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*, April 9, 2013 , accessed on April 10, 2013, @

<http://killerapps.foreignpolicy.com/posts/2013/04/09/us_military_starting_to_integrate_cyber_weapons_into_commanders_arsenals#.UWUwgOWglhw.twitter>.

The French operational cyberdefense chain of command is currently under the command of a General, in charge of cyberdefense, embedded within the CPCO[9], for the planning and leadership of operations. He is assisted by a Central Computer Warfare Officer (OLID) who oversees the deployment of the cyber forces within armies, the actions of inter-army cyber entities (CALID[10]), specific to the armies. A management team implements the decisions made by the OG Cyber. In his missions, he can rely on the CALID, which is the central expertise repository for the Department of Defense. It is the readiness and reaction center for computer attacks (CERT[11]) of the Department of Defense which carries out surveillance and detection missions 24/7, seeking cyberattacks targeting the armies. The global volume of the central chain personnel is of a hundred people, which is a relatively small staff, compared to the United States which plan to reach 4.900 people in Cyber Command[12].

Finally, French armies are now confronted to the difficulty of implementing such a structure, which could take example in the Nation Defense Units from America. These units would be systematically deployed with level-1 and -2 staff, to assist them in their missions, and provide them with complete solutions on the cyber-field, both defensive and offensive. Several challenges remain, including recruitment, training and keeping computer experts, able to carry out such missions. This type of specialist is particularly coveted. The civilian world offers better pay than the military institution, which makes their recruitment tricky. Their recruitment is all the trickier by the fact that, in 2013, a high estimation of 38 000 positions were said to be unmanned in France, on the computer market.[13]

[9] Operations command and planning center

[10] Analysis center for defensive computer warfare

[11] Computer Emergency Response team.

[12] Elisabeth Bumiller, « Pentagon expanding cybersecurity force to protect networks against attacks », The New York Times, January 27, 2013, accessed on April 4, 2013 @ <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, March, 18 2013, accessed on April 4, 2013 @ <http://www.ladepeche-emploi.fr/edito/actualite-ladepeche/article/un-recrutement-sur-quatre-dans-linformatique.html>.