La note du CESA
N°16

LTT Tony Morin

02 / 2015

L'*US Air Force* et l'institutionnalisation de la cyberdéfense aux Etats-Unis

La cyberdéfense, c'est-à-dire l'action des forces armées dans le cyberespace, demeure l'une des préoccupations majeures du Department of Defense (DoD). Le terme, ou plutôt le préfixe « cyber » est apparu au début des années 1990 dans le cadre des travaux sur la Revolution in Military Affairs aux Etats-Unis. L'US Air Force a certainement été la principale bénéficiaire des nouvelles technologies, qui exploitent le cyberespace. L'USAF a ainsi mis en place une stratégie visant à acquérir le leadership sur ce secteur, au sein des forces armées américaines.

Le cyberespace : un enjeu institutionnel

- Le « *National Strategy to Secure Cyberspace* » de 2003, produit par la Maison Blanche, est le premier document officiel à évoquer l'idée d'une institutionnalisation de ce secteur.

- S'intéressant de près à toute initiative sur ce secteur et voulant signifier sa démarche proactive, l'*USAF* change en 2005 sa devise qui devient : *to fly and fight in air, space* ***and cyberspace.***

- Toutefois, l'*USAF* n'est pas la seule institution à s'intéresser au cyberespace. L'*US Navy*, l'*US Army* et la *NSA* lancent également des initiatives. Ces différents projets ont véritablement été perçus comme menaçants par l'*USAF*, qui craignait de se voir retirer un domaine d'activité qu'elle considère comme stratégique.

- Ce sentiment se fonde sur une double perception, structurelle et conjoncturelle. Structurelle car l'*USAF* entretient un complexe d'infériorité (idée présente dans de nombreuses études sur cette institution) par rapport aux autres armées (*Army* et *Navy*). Conjoncturelle car l'*USAF*, depuis le début des années 2000, a vu progressivement sa flotte de drones passer sous le contrôle d'autres institutions.

L'échec de l'*USAF* et la création du *US Cyber Command*

DR

- Elle entreprend donc plusieurs initiatives afin de sécuriser sa position dans le secteur du cyberespace. Ainsi, lors d'une conférence de presse en 2006, le secrétaire de l'*USAF* annonce la création de l'*Air Force Cyber Command.*

- Le projet est très ambitieux et mobilise un grand nombre de ressources, financières et humaines. Le Congrès (qui valide les budgets) est également concerné, à travers divers projets d'implantation pour le nouveau commandement. Une campagne de recrutement est lancée.

- Cependant, les objectifs et les missions de l'*AFCYBER* sont mal définis. Les déclarations des différents responsables de l'*USAF* sur le sujet sont par ailleurs contradictoires, entre la vocation offensive ou défensive de la structure notamment. Ces ambiguïtés couplées à différentes crises (problème de gestion de la flotte de *F-22*, incident nucléaire sur la base de Barksdale, etc.) conduisent à l'annulation du projet.

- Suite à cet échec, le Pentagone reprend l'initiative et crée en 2010 une structure dédiée au cyber espace : l'*US Cyber Command*, dépendant de l'*US Strategic Command* et fonctionnellement rattaché à la *NSA* (le directeur de la *NSA* est aussi chef du *Cyber Command*). Au même titre que les autres branches de l'armée, l'*USAF* y dispose d'une structure « air » nommé *AFCYBER*. Elle est mise en œuvre par la *24th Air Force*.

Si l'USAF a échoué dans sa tentative de s'approprier la cyberdéfense « par le haut », elle n'a pour autant pas abandonné ses prétentions. Elle tente désormais une approche « par le bas », en renforçant sa contribution en ressources humaines pour le Cyber Command ainsi qu'en R&D. Une approche payante puisque, pour l'année fiscale 2015, elle bénéficie du budget le plus important des 3 armées dans ce secteur. Plus symboliquement, elle a conservé la référence au cyberespace dans sa devise. Toutefois, l'absence d'une institution dédiée ne signifie pas une absence d'action des Etats-Unis en termes de cyberdéfense, comme le démontrent le programme Olympic games, lancé en 2006 et la création du virus Stuxnet.