La note du CESA
N°42
11 / 2015

Nolwenn Maksyska, Camille Sanchez

La cyberdéfense, nouvelle mission pour la réserve américaine

En 2015, le Governement Accountability Office *annonce la nécessité de recruter 40 000 experts en cybersécurité pour couvrir les besoins du gouvernement américain. La Défense met ainsi en place des unités spécialisées qu'elle peine cependant à armer, faute de personnel suffisamment formé. Dans ce contexte, la réserve constitue une autre voie présentant de multiples intérêts.*

La réserve en renfort des unités cyber des forces armées

Avec la création de l'*US Cyber Command* en 2010, une coordination interagences et interarmées se met en place autour des forces cyber du *Departement of Defence* (*DoD*) jusque là fragmentées. Malgré ces efforts, plusieurs facteurs limitent leur efficacité. Au sein de *l'Air Force* par exemple, la confusion des fonctions entre les branches de la maintenance des systèmes et celle de la sécurité de l'information (*InfoSec*) est source de désorganisation, voire d'insuffisances dans l'expertise du personnel. À cela s'ajoute la fuite des talents vers le secteur privé, plus attractif. Par conséquent, en 2013, le *DoD* avait pour objectif de recruter 6 244 experts cyber. Pour autant, en 2015, cet objectif n'est qu'à moitié atteint.

Pour une meilleure gestion de son personnel, le *DoD* publie en 2013 une *Cyberspace Workforce Strategy*, puis la *Dod Cyber Strategy* en 2015. Ces documents montrent sa volonté non seulement de diversifier le recrutement des spécialistes, de mieux former et de fidéliser les civils comme les militaires, mais aussi d'améliorer ses capacités de gestion de crise. Dans ce contexte, le potentiel de la réserve, jusqu'alors peu exploité dans le cyber, passe au premier plan.

Depuis, la réserve cyber n'a cessé de monter en puissance. Très sollicités, ses membres effectuent un service compris entre quarante jours et une année complète.

Un parcours civil et militaire au service de la professionnalisation de la *cyber reserve*

Issus du milieu civil ou militaire, les réservistes sont recrutés selon des critères précis. La réserve de l'*USAF* exige ainsi de ses militaires du rang une expérience professionnelle préalable dans le domaine cyber. Pour les officiers, un parcours universitaire de quatre ans en systèmes d'information et de communication ou en *InfoSec* est requise. Ces recrues représentent un investissement sur du long terme pour les forces armées, puisqu'elles suivent après leurs classes des formations spécifiques de deux à six mois.

Ces dernières s'accompagnent de programmes d'ampleur, comme le *Army Reserve's Public Private Partnership Initiative,* qui vise à financer des formations universitaires ou professionnelles pour les réservistes. Depuis 2015 ce programme associe l'*Army Reserve*, six universités et douze entreprises telles que *Microsoft*. Parmi les 6 000 personnes qu'il regroupe, 3 500 sont des militaires.

Cette dynamique bénéficie donc à la fois à la Défense et au secteur civil, de même qu'elle favorise le développement de véritables carrières au sein de la réserve. Cette logique présentée comme « gagnant-gagnant » ainsi que l'octroi de différentes primes visent à attirer et à fidéliser les talents.

Un pilier pour les nouvelles structures militaires opérationnelles cyber

Du point de vue opérationnel, les réservistes servent en unités cyber de réserve ou au sein d'unités d'active. De même, ils sont mobilisables par l'*US Cyber Command* en fonction des besoins du Pentagone.

Cette implication varie toutefois selon les armées. En effet en 2015, les réservistes représentent 30 % des effectifs cyber de l'*Air Force* et de l'*Army*, ainsi que 15 % de ceux de la *Navy*. A cela s'ajoutent ceux de la *National Guard* et de l'*Air National Guard*. Les réserves du *Marine Corps* et du *Coast Guard* n'ont quant à elles pas prévu de participer à la force cyber interarmées, la *Cyber Mission Force*.

Le *DoD* prévoit en outre que celle-ci soit constituée de 6 000 militaires et civils, dont 2 000 réservistes. En 2018 elle formera 133 équipes réparties en fonction de quatre missions : la défense des réseaux, la défense des infrastructures critiques, la conduite cyber des opérations militaires et enfin le soutien aux trois précédentes missions.

Le DoD *élabore une stratégie ambitieuse en vue de répondre pleinement à la menace cyber d'ici 2018. Pour atteindre ses objectifs, il forme progressivement des réservistes en collaboration avec la sphère civile. Dans un même temps, les forces armées se dotent de structures d'enseignement qui leur sont propres, avec par exemple l'*US Army Cyber School *de Fort Gordon ou le futur* Air College Cyber *en Alabama en 2017.*