



La nouvelle arme CYBER se construit au sein de l'US Army

cahier de la pensée mili-Terre

le Lieutenant-colonel Hyacinthe de LAVAISSIÈRE

publié le 18/10/2018

Sciences & technologies

Le ministère de la Défense français fait depuis quelques années un effort très important sur nos capacités de lutte informatique, en liaison avec d'autres services de l'État. Cet effort est tout particulièrement pris en compte et relayé par l'armée de Terre dans le cadre de son futur modèle «Au contact!». Il a donc semblé intéressant d'informer les lecteurs des Cahiers sur l'évolution de l'US Army dans ce domaine, grâce à un article de synthèse rédigé par un de nos officiers de liaison aux États-Unis.

Lors de la conférence Augusta TechNet 2015, le Major General Stephen Fogarty, commandant l'US Army Cyber Center of Excellence de Fort Gordon, a noté que la première pierre de la nouvelle arme cyber était posée, mais qu'il fallait maintenant faire converger tous les tenants de cet effort afin de disposer d'un outil totalement intégré pour les opérations. En effet, les bases de l'arme cyber, au sens ressources humaines, sont désormais en place et le recrutement dans toutes les catégories a commencé.

Loin de phagocyter les transmissions et le renseignement, l'arme cyber doit assurer à l'US Army sur le long terme la capacité d'armer 41 équipes cyber qualifiées et entraînées, dont les combattants seront gérés individuellement. À l'inverse de la recherche d'un effet de masse, cette force sera comptée afin de garantir un haut niveau d'expertise et une unité d'action dans le cyberspace.

L'Army Cyber Force bâtie sur le modèle interarmées

Depuis 2011 et aux ordres de l'US CYBERCOM, l'US Army contribue à la Cyber Mission Force interarmées dont le volume sera d'environ 6.200 combattants.

Le commandement interarmées en a défini les missions, les structures, les rôles et les métiers. Sitôt qualifiés et entraînés, les éléments de la force ont été engagés en

opérations sans attendre la manœuvre ressource humaine. Ainsi, la création d'une arme cyber au sein de l'US Army n'a pas été imposée, mais elle a plutôt répondu à une exigence de cohérence des parcours professionnels pour l'avenir.

Alors que pour les opérations terrestres l'unité de base de l'US Army est la Brigade Combat Team, en matière de cyber la cellule de base est l'équipe. Quelle que soit l'armée d'appartenance des hommes qui arment ces équipes, ils doivent être qualifiés selon les critères de l'un des 14 workroles interarmées. Ces 14 rôles permettent de construire les différentes équipes qui composent la CMF.

L'US Army contribue à l'effort interarmées en bâtissant 41 équipes cyber sur les 133 prévues par l'US CYBERCOM. Actuellement en phase de montée en puissance, l'Army Cyber Workforce est déjà opérationnelle à 50% car elle se construit en réalité depuis 2011 à partir des armes et spécialités existantes.

La nouvelle arme cyber pour une gestion fine de la ressource

Globalement, l'essentiel des profils recherchés existe dans les armes des transmissions, du renseignement et de l'artillerie. En revanche, chaque combattant sélectionné doit suivre un cycle de formation qui nécessite jusqu'à six mois de stages d'adaptation avant d'intégrer une équipe. De fait, les 41 équipes représentent 1.899 combattants, dont 65% proviennent de l'arme du renseignement, 34% des transmissions et 1% de l'artillerie. Ce tropisme renseignement est encore plus flagrant lorsqu'il s'agit des National Teams ou des Combat Teams où le ratio dépasse 87%. En revanche, les Cyber Protection Teams sont composées à 77% de transmetteurs et seulement à 35% de personnel du renseignement, ce qui reflète le caractère défensif de leur mission. Cependant, elles disposent tout de même d'un Red Squad spécialisé dans l'étude des modes d'action de l'adversaire.

Dans cette force, il faut noter la présence de civils des spécialités 0132 (renseignement) et 2210 (systèmes d'information), qui représentent 16 % du volume total. Très présents dans les structures de l'Army, ces civils, dont plus de la moitié sont d'anciens militaires, constituent souvent une expertise cruciale. Enfin, la présence dans les équipes de 104 personnes provenant d'agences de renseignement illustre l'appui apporté par ces agences, et la force de frappe qu'elles représentent en complément de cette force cyber militaire. Ainsi, alors que le chiffre de 6.200 hommes annoncé pour la force cyber interarmées semble déjà un peu sous-évalué, il faudrait lui ajouter les effectifs de la National Security Agency et ceux d'autres agences pour évaluer la réalité de la force cyber américaine.

Considérant l'investissement en formation, l'US Army a voulu protéger cette ressource et construire des parcours professionnels complets en créant une nouvelle arme, la Cyber Branch 17. Le recrutement se fait à la fois par des reclassements et par des entrées directes comme celle des 32 sous-lieutenants arrivés cette année. Cette étape initiale étant presque achevée, la phase suivante consistera à intégrer le personnel de la guerre électronique, jusque-là géré par l'artillerie. Ce chantier est donc loin d'être achevé, d'autant que l'élaboration des parcours professionnels ne fait que commencer. À terme, la convergence transmissions – guerre électronique – renseignement – feux pourrait entraîner des changements structurels avec un impact sur la conduite des opérations.

Ainsi, si la nouvelle arme cyber est en passe d'atteindre son premier millier de combattants, sa montée en puissance devrait durer jusqu'en 2017. Presque

paradoxalement, près de 50% des 41 équipes cyber, offensives et défensives, sont déjà opérationnelles et à l'œuvre aux ordres de l'US CYBERCOM.

Le lieutenant-colonel Hyacinthe de LAVAISSIÈRE appartient au détachement de liaison terre avec l'US Army, et sert comme officier de liaison auprès du Cyber Center of Excellence de Fort Gordon

Titre :	le Lieutenant-colonel Hyacinthe de LAVAISSIÈRE
Auteur(s) :	le Lieutenant-colonel Hyacinthe de LAVAISSIÈRE
Date de parution	08/10/2018
