Haut du formulaire



Bas du formulaire

****

**Barkhane : La 807e Compagnie de Transmissions contre une cyberattaque tous les 10 jours**

par [Laurent Lagneau](http://www.opex360.com/author/admin/) · 2 mars 2021

 

Les opérations de la force Barkhane ne concernent pas seulement le terrain… mais également les espaces immatériels. Ainsi, en décembre dernier, sur les réseaux sociaux, une opération d’influence attribuée aux armées françaises a été mise au jour par Facebook. Il s’agissait alors de contrer des campagnes de désinformation les visant au Sahel. Campagnes, a récemment accusé Florence Parly, la ministre des Armées, menées notamment par la Russie et la Turquie.

Mais au-delà du champ « informationnel » et de la « guerre des perceptions », Barkhane doit également faire face à des attaques informatiques. Les contrer est la mission de la 807e Compagnie de transmissions [CT], recréée à la faveur du plan « Au Contact », en 2016, au sein du commandement des systèmes d’information et de communication [COMSIC] de l’armée de Terre.

Actuellement, cette 807e CT arme en permanence deux centres de supervision [SOC – Security Operation Center] au profit des forces Chammal [Levant] et Barkhane. Ponctuellement, elle surveille également les réseaux déployés lors d’exercices multinationaux ou de missions effectuées au titre de l’Otan, comme celle appelée Lynx, dans les pays baltes. Et elle est également sollicitée par le Service de santé des armées [SSA] pour protéger les systèmes informations des hôpitaux d’instruction des armées [HIA], sous la menace de cybercriminalité qui profite de la crise sanitaire provoquée par la covid-19.

Enfin, il lui arrive de déployer des « groupes d’intervention cyber » [GIC], que ce soit à titre préventif ou pour enquêter sur une attaque. Selon [le dernier numéro](https://en.calameo.com/read/005141509d995d6946ef9) de « Transmetteurs », le magazine [officiel] du corps des Transmissions, la 807e CT « conduit 6 GIC par an, dont un en appui du [groupement de forces spéciales] Sabre en 2020 ».

Un centre de supervision déployé en opération compte six sous-officiers superviseurs et/ou analystes, commandés par un officier, lequel a un rôle de conseiller auprès du commandement.

Pour s’acquitter de ses tâches, un tel détachement utilise plusieurs outils, dont le MTLID-T [Moyen technique de lutte informatique défensive dans sa version tactique], développé par Airbus. « Un lot tactique est composé de caissons techniques modulaires et aérotransportables, pouvant être déployés en quelques jours sur un système d’information n’importe où dans le monde », explique Transmetteurs.

Ce dernier n’a pas livré de détails sur l’activité de la 807e CT au Levant. En revanche, elle a souligné que le centre de supervision affecté à la force Barkhane est « capable de détecter au plus vite les incidents ou indices d’agressions cybernétiques à travers toute la bande sahélo-saharienne, depuis les grandes emprises militaires telles que Niamey, jusqu’aux plus isolées comme Gossi ou Faya-Largeau » et qu’il fournit « également la capacité de réaction cyberdéfense du théâtre. » Au total, il a à veiller sur un réseau informatique de 2.000 ordinateurs.

Et, visiblement, les experts de la 807e CT n’ont guère le temps de s’ennuyer.

« Chaque jour, sur les 100 millions d’évènements de sécurité collectés, environ 150 alertes sont générées puis traitées. Chaque année plus de 600 contre-mesures sont prises pour corriger ces
incidents qui peuvent aller d’une attaque collatérale de cybercriminalité à une tentative d’exfiltration de données vers Internet ou encore la perte de tout ou partie des services d’un
système d’information », indique le magazine.

Et, récemment, poursuit-il, « dix attaques majeures ont pu être identifiées et stoppées à temps », soit une « attaque tous les dix jours en moyenne, avec un impact sur les réseaux informatiques et par extension sur les opérations en cours. »

Le magazine n’en a pas dit davantage sur ces attaques « majeures », encore moins sur les motivations de ceux qui les ont lancées.

Cela étant, en juin 2019, lors [d’une audition](http://videos.senat.fr/video.1230400_5d120453ab6cc.ce-souverainete-numerique?timecode=7915000) menée par la commission d’enquête sénatoriale sur la souveraineté numérique, le général Olivier Bonnet de Paillerets, alors « patron » du commandement de la cyberdéfense [COMCYBER] avait relativisé le risque d’attaque « complexe » contre les réseaux de Barkhane.

« Aujourd’hui, les menaces et le nombre des attaquants augmentent, mais la capacité d’attaques complexes appartient encore aux États. Les investissements en organisation, doctrine d’emploi, recrutement d’experts, nécessitent une cohérence qui n’existe que dans certains États. Cela nous donne tout de même un avantage comparatif dans une guerre même dissymétrique », avait expliqué l’officier. « l n’existe aujourd’hui aucun ennemi potentiel, à part l’Iran, voire la Russie [mais nous ne sommes pas confrontés à eux], qui puisse menacer nos réseaux et notre capacité à agir dans un espace numérisé », avait ensuite précisé le général François Lecointre, le chef d’état-major des armées [CEMA]. Qu’en est-il actuellement?

Photo : armée de Terre