Les armées françaises assument désormais la guerre de l'information

Elise Vincent

Le Monde, 22 octobre 2021

Le nouveau document de doctrine présenté mercredi indique que, dans le cadre d'opérations extérieures, il sera notamment possible de diffuser des contenus dans l'espace médiatique pouvant « induire en erreur » l'adversaire.

C'est un sujet périlleux sur lequel les armées souhaitaient se positionner depuis longtemps. Après en avoir plusieurs fois repoussé la date, le ministère des armées a finalement présenté, mercredi 20 octobre, sa nouvelle doctrine de lutte informatique d'influence (L2I), censée définir les contours des manœuvres militaires possibles dans l'espace médiatique, en particulier sur les *« médias sociaux »* lors d'opérations extérieures.

L'armée française a toujours mené des actions dans le champ informationnel, mais elle l'assume désormais haut et fort, comme d'autres puissances militaires. Tel était essentiellement le sens de la présentation organisée, mercredi, au siège de l'état-major des armées, à Paris. Et ce, un peu moins d'un an après que les armées se sont retrouvées épinglées par Facebook dans le cadre d'un rapport dévoilant pour la première fois que de faux profils se livraient à de la *« guerre informationnelle »* en Afrique.

A l'époque, ce rapport était sorti dans un contexte d'affrontement larvé entre Paris et Facebook lié à la naissance du Digital Service Act, un paquet de mesures européennes visant notamment à obtenir une plus grande transparence dans les algorithmes des réseaux sociaux. Les méthodes des militaires français avaient été mises au même niveau que les manipulations de l'information russes. Chose qu'avaient mal vécue les armées, considérant qu'elles avaient plutôt fait preuve d'inhibition jusque-là, s'interdisant notam-

ment les sujets électoraux, contrairement à la Russie.

« Induire en erreur » l'adversaire

Depuis, l'eau a coulé sous les ponts et les *« éléments publics »* de doctrine présentés, bien que sommaires, se veulent une façon de sortir de l'ornière. *« Le champ informationnel (…) est un lieu de compétition stratégique*, a justifié la ministre des armées, Florence Parly. *L'information fausse, manipulée ou subvertie, c'est une arme. »* Des propos immédiatement assortis d'une précaution importante aux yeux des armées : ces actions se font *« dans le strict respect »* de la charte des Nations unies et du droit international humanitaire (DIH). Une marge étroite, alors que le DIH n'est pas très bavard en matière de guerre informationnelle.

La nouvelle doctrine assume ainsi que les armées – au-delà de la simple veille numérique – pourront désormais avoir recours à de la diffusion de contenus pour *« induire en erreur »* l'adversaire. Elles pourront être amenées à *« dénoncer, contenir, affaiblir ou discréditer, y compris par la ruse, une attaque informationnelle »*. Avec leurs outils, elles seront également en mesure de *« promouvoir l'action des forces »*, de *« dénoncer les incohérences ou mensonges de l'adversaire »*, voire de *« convaincre les acteurs d'une crise d'agir dans le sens souhaité »*. Un exercice d'équilibre verbal, afin d'éviter les éventuelles accusations de manœuvres *« perfides »*, interdites, elles, sur le papier, par le droit international humanitaire.

Sur le plan organisationnel, c'est le commandement de la cyberdéfense (Comcyber), rattaché à l'état-major des armées, qui gardera la haute main sur les opérations de lutte informatique d'influence. Pour la production de contenus, il s'appuiera notamment sur le Centre interarmées des actions sur l'environnement (CIAE), basé à Lyon. Un centre très discret où, depuis 2012, les armées conçoivent en partie leurs *« opérations civilo-militaires »* et d'influence. Les effectifs du CIAE, comme ceux du Comcyber, sont amenés à fortement s'étoffer grâce aux crédits prévus dans le projet de loi de finances 2022.

Concernant les outils pour détecter les éventuelles manœuvres adverses de manipulation de l'information, ou pour diffuser les contenus produits, peu de détails ont été communiqués. Au ministère des armées, mercredi, on précisait juste qu'un certain nombre repose sur de simples logiciels libres, donc nécessitant peu de moyens financiers. Le ministère a aussi reconnu pouvoir être amené à s'appuyer sur le secteur privé pour acquérir des solutions techniques, *« mais*

pas pour lui commander des opérations d'influence ».

Maîtrise des algorithmes

En se lançant de façon plus décomplexée dans la lutte informationnelle, l'enjeu pour l'armée est toutefois, *in fine*, de gagner en influence, et que ses actions dans ce domaine atteignent une audience utile. Une bataille d'audience qui l'oblige à se frotter à une autre guerre, bien connue des médias traditionnels : celle de la maîtrise des algorithmes de référencement sur Internet et des outils de gestion particulièrement complexes des géants du numérique, comme Google Analytics. Pour cela, le ministère a admis chercher à recruter des spécialistes du marketing numérique dans les écoles de commerce.

Sur ce champ très sensible qu'est la lutte informatique d'influence, Paris assure avoir certaines *« lignes rouges »*. Comme ne pas avoir recours à des agents sous couverture disposant de carte de presse, un procédé courant dans de nombreux pays à des fins de renseignement. *« Il y a et il y aura toujours une forme d'asymétrie entre ce qu'on fait et ce que font nos adversaires. La Russie utilise ses médias. On ne fera pas ça »*, a-t-on assuré mercredi. La doctrine de L2I présentée se borne toutefois prudemment aux opérations conduites sous les ordres du Comcyber et de l'état-major des armées. Elle n'aborde pas les méthodes éventuellement utilisées par les services de renseignement français dans d'autres cadres.

Elle se veut aussi différente de la lutte contre les ingérences numériques étrangères dans les médias sur le territoire national, pilotée par l'agence Viginum. Cette dernière a été lancée le 15 octobre sous la tutelle du secrétariat général de la défense et de la sécurité nationale, rattaché au premier ministre.