ASSEMBLÉE NATIONALE

9 mai 2023

PROGRAMMATION MILITAIRE 2024-2030 - (N° 1033)

Adopté

AMENDEMENT

N º DN918

présenté par
M. Jacques, rapporteur et M. Gassilloud

ARTICLE 2

RAPPORT ANNEXÉ

Compléter la troisième phrase de l’alinéa 51 par les mots :

« , en coordination avec les autres services de l’État concernés ».

EXPOSÉ SOMMAIRE

La Revue nationale stratégique (RNS) de 2022 a érigé, à juste titre, l’influence au rang des priorités du ministère des Armées en en faisant une fonction stratégique à part entière. Le projet de loi de programmation militaire pour les années 2024 à 2030, qui décline les objectifs fixés dans la RNS, réaffirme l’ambition du ministère en matière de lutte informatique d’influence en renforçant la dotation des armées pour leur permettre, jusqu’aux niveaux opératif et tactique, de faire face aux attaques informationnelles qu’elles subissent. Plus généralement, le projet de loi de programmation militaire pour les années 2024 à 2030 consacre 4 milliards d’euros au domaine de la cyberdéfense sur la période de la programmation, dont relèvent les financements consacrés à la lutte informatique d’influence, contre 1,6 milliard d’euros dans la loi de programmation militaire pour les années 2019 à 2025 sur la période de la programmation, soit une hausse très substantielle de 150 %.

Mais en sus des moyens budgétaires, il convient de porter une attention toute particulière à l’impératif de coordination dans la conduite d’une politique dès lors que celle-ci est partagée entre différentes entités au sein d’un même ministère, et *a fortiori* si celle-ci est partagée entre différents ministères. En ce qui le concerne, le commandement de la cyberdéfense (COMCYBER), qui dépend du chef d’état-major des armées (CEMA), est en charge de la lutte informatique d’influence au profit des armées. Il n’est toutefois pas porteur de la fonction « influence » au niveau du CEMA. Il ne s’occupe en effet que du volet cyber de la politique ministérielle d’influence, tandis que la cellule « anticipation stratégique et orientations » (ASO), rattachée au CEMA, structure ladite politique à l’échelle de l’état-major des armées (EMA). Par ailleurs, le COMCYBER et l’EMA travaillent également avec les trois armées et les services de renseignement du secteur de la défense dans ce cadre.

Or, pour être efficace, la politique d'influence nécessite une approche globale et interministérielle. L'ensemble des armées, directions et services du ministère des Armées en charge de l'influence devront en effet travailler avec l'ensemble des services de l'État chargés de la politique d'influence, parmi lesquels, entre autres, la Direction générale de la sécurité intérieure (DGSI), Viginum ou encore le ministère de l'Europe et des Affaires étrangères. L'importance de la coordination de l'ensemble des acteurs a d'ailleurs été rappelée par le Secrétaire général de la défense et de la sécurité nationale lors de son audition devant la commission de la Défense nationale et des forces armées le jeudi 6 avril 2023.

Par conséquent, cet amendement vise à inscrire cet objectif de coordination de l'effort du ministère des Armées en matière de lutte informatique d'influence avec l'ensemble des services de l'État concernés par la politique d'influence dans le rapport annexé du projet de loi.