	Projet de loi		
	Programmation militaire pour les années 2024 à 2030 (PROCÉDURE ACCÉLÉRÉE)	N°	32 rect. bis
Direction de la Séance	(n°S 667, 666, 654, 646)		**2 juin 2026**

a m e n d e m e n t	**C**	**Favorable**
présenté par	**G**	

M. CADIC, Mme BILLON, M. COURTIAL, Mme DEVÉSA, MM. DHERSIN, DUFFOURG, HAYE et MENONVILLE et Mmes PATRU, PERROT, ROMAGNY et SAINT-PÉ

Article 1er
RAPPORT ANNEXÉ

Alinéa 9

Compléter cet alinéa par deux phrases ainsi rédigées :

La France se dote d'une capacité de cyberdissuasion graduée et attribuable contre les acteurs étatiques conduisant des cyberattaques persistantes contre ses intérêts, ses infrastructures critiques et ses représentants. En cas de guerre hybride menaçant le territoire national, la continuité des activités essentielles à la vie de la Nation et la protection de la population, les armées conduisent les actions de luttes informatiques défensive (LID), offensive (LIO) et d'influence (L2I) en étroite coordination avec le Secrétariat général de la défense et de la sécurité nationale.

Objet

Le présent amendement vise à consacrer dans la loi de programmation militaire une doctrine de cyber-riposte active et proportionnée. Il traduit dans le rapport annexé l'orientation défendue par le rapport sénatorial « Pour une coordination de la cyberdéfense plus offensive dans la LPM 2024-2030 », co-rédigé par MM. Cadic et Vallet.

Face à la multiplication des attaques persistantes de niveau étatique — notamment celles attribuées au groupe APT31 (République populaire de Chine), ayant notamment visé des parlementaires français —, il est nécessaire que la France affirme explicitement sa volonté de disposer d'une capacité de riposte crédible, graduée et attribuable. Cette posture constitue à la fois un élément de dissuasion et un signal adressé aux partenaires de l'Alliance atlantique et de l'Union européenne quant à la pleine participation française à la cyberdéfense collective.

La formulation retenue est conforme aux orientations de la Revue nationale stratégique de 2022 et à la doctrine cyber offensive rendue publique par le ministère des Armées en 2019. Elle ne préjuge pas des modalités opérationnelles, qui relèvent du domaine classifié.