ASSEMBLÉE NATIONALE

4 mai 2023

PROGRAMMATION MILITAIRE 2024-2030 - (N° 1033)

Adopté

AMENDEMENT

N º DN501 (Rect)

présenté par
M. Saintoul, Mme Abomangoli, M. Alexandre, M. Amard, Mme Amiot, Mme Amrani, M. Arenas, Mme Autain, M. Bernalicis, M. Bex, M. Bilongo, M. Bompard, M. Boumertit, M. Boyard, M. Caron, M. Carrière, M. Chauche, Mme Chikirou, M. Clouet, M. Coquerel, M. Corbière, M. Coulomme, Mme Couturier, M. Davi, M. Delogu, Mme Dufour, Mme Erodi, Mme Etienne, M. Fernandes, Mme Ferrer, Mme Fiat, M. Gaillard, Mme Garrido, Mme Guetté, M. Guiraud, Mme Hignet, Mme Keke, M. Kerbrat, M. Lachaud, M. Laisney, M. Le Gall, Mme Leboucher, Mme Leduc, M. Legavre, Mme Legrain, Mme Lepvraud, M. Léaument, Mme Pascale Martin, Mme Élisa Martin, M. Martinet, M. Mathieu, M. Maudet, Mme Maximi, Mme Manon Meunier, M. Nilor, Mme Obono, Mme Oziol, Mme Panot, M. Pilato, M. Piquemal, M. Portes, M. Prud'homme, M. Quatennens, M. Ratenon, M. Rome, M. Ruffin, M. Sala, Mme Simonnet, Mme Soudais, Mme Stambach-Terrenoir, Mme Taurinya, M. Tavel, Mme Trouvé, M. Vannier et M. Walter

---

ARTICLE 2

RAPPORT ANNEXÉ

Compléter le rapport annexé par l’alinéa suivant :

« Dans un délai de deux ans à compter de la promulgation de la présente loi, le Gouvernement remet au Parlement un rapport sur les évolutions de la menace cyber et la capacité de résilience du ministère des armées. Ce rapport fera l’objet d’un examen par la commission de la défense nationale et des forces armées. »

EXPOSÉ SOMMAIRE

Par cet amendement, le groupe LFI-NUPES souhaite mettre l’accent sur les évolutions de la menace cyber, et sur la faible capacité de résilience et d’adaptation de l’État français dans son traitement. En effet, les nouveaux modes de conflictualité, et particulièrement ceux liés à l’émergence du cyber, souffrent d’un sous-investissement chronique et d’un manque de planification de moyen et long terme.

La sophistication toujours plus grande des attaques cyber et le développement d’armements spatiaux permettant d’infliger des dommages insoutenables ou impossibles à attribuer à une

puissance ennemie pourrait mettre la France face au fait accompli d'une attaque sans être en mesure d'y riposter. Il pourrait également exister à terme des vulnérabilités dans le domaine informatique et des communications.

Ces ruptures technologiques appellent un effort diplomatique particulier de la France pour adapter sa politique de formation, de recrutement et de montée en compétence. Les espaces de stockage des données sensibles sont aujourd'hui insuffisants, de même que le financement dédié au renforcement du capital technique et opérationnel dans le domaine du cyber. Les évolutions de la menace cyber doivent forcer la Nation à développer une « culture du cyber », envers la population qu'il convient de sensibiliser aux dangers, qu'auprès des autorités publiques, des acteurs économiques, et territoriaux et des collectivités, en renforçant la sensibilisation et la prévention pour leur permettre de diffuser une culture et une prise de conscience du risque cyber.

Le cyber étant par nature un espace mouvant, protéiforme et en recomposition permanente, il suppose une adaptation constante de la part de l'ensemble des acteurs afin d'augmenter la résilience globale de la société, de renforcer ses capacités d'anticipation de la menace, de défense et de riposte, de résiliation et de promotion d'un certain nombre de valeurs au niveau international.