ASSEMBLÉE NATIONALE

15ème législature

Effets économiques de la LPM sur la filière « cyber »

Question écrite n° 23658

Texte de la question

M. Christophe Blanchet interroge Mme la ministre des armées sur les retours sur investissements de la loi de programmation militaire 2019-2025 (LPM) dans le secteur « cyber ». La LPM votée en 2018 a permis des avancées conséquentes en matière de « cyber » sécurité et d'action « cyber » de manière plus générale. Les capacités des armées en matière de prévention, de détection et d'attribution des cyberattaques devaient se voir renforcées par la création de 1 500 postes sur la période 2019-2025. L'objectif était de porter à 4 000 personnes la force « cyber » de la République française. Alors que l'année 2019 s'achève bientôt, il souhaite savoir si les crédits attribués au titre de la LPM ont été utilisés dans la poursuite de cet objectif. De plus, il lui demande si la valorisation des problématiques « cyber » au sein de la LPM 2019-2025 a permis, à ce jour, de soutenir l'expertise au sein de la filière.

Texte de la réponse

La revue stratégique de défense et de sécurité d'octobre 2017, puis la revue stratégique cyber de février 2018, témoignent des ambitions françaises en matière de cyberdéfense. En pratique, pour le ministère des armées, la loi relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense (LPM 2019-2025) en traduit les ambitions. Elle prévoit notamment de renforcer l'action du commandement de la cyberdéfense (COMCYBER), créé en 2017 et placé sous l'autorité du chef d'état-major des armées. Le COMCYBER assure le commandement, la conduite et la cohérence de l'ensemble des actions et des capacités en matière de cyberdéfense dans trois domaines essentiels : la prévention, la détection et l'attribution. Si la LPM 2014-2019 avait consenti un effort financier important, environ un milliard d'euros, pour le développement du domaine cyber, l'effort prévu au cours de la LPM 2019-2025 est supérieur, avec une dotation de 1,6 milliard d'euros. Il permet d'une part, de répondre aux besoins en investissement (équipements et infrastructure) et en fonctionnement (formations, exercices, déplacements…), d'autre part, d'augmenter les effectifs de 1 123 cyber-combattants jusqu'en 2025. Les objectifs de recrutement prévus pour 2019 sont à cet égard remplis. Grâce à cet effort ambitieux, le ministère des armées dispose d'un modèle cyber complet, qui pourra garantir en 2025 une posture permanente de cyberdéfense sur l'ensemble de sa surface numérique attaquable, appuyée sur l'hypervision opérationnelle de l'ensemble des systèmes d'information et des moyens. Pour y parvenir, la stratégie capacitaire repose sur deux piliers : l'atteinte des objectifs de recrutement et l'adaptation du modèle d'acquisition aux besoins cyber, en particulier par le développement de moyens agiles de captation de l'innovation. L'action du COMCYBER s'appuie également sur la réorientation de la réserve de cyberdéfense, dont le projet « Réserve 2019 » prévoit de consolider la montée en puissance des effectifs et de favoriser les recrutements. Ces actions s'inscrivent dans un cadre en évolution permanente, dont les travaux ont donné lieu à des publications récentes : - La politique ministérielle de Lutte informatique défensive (LID), publiée en janvier 2019, et complétée plus récemment d'une stratégie d'innovation et de développement capacitaire LID. Adressée aux acteurs des programmes d'armement et aux industriels de Défense, cette dernière décrit les orientations et les cinq chantiers prioritaires de développement dans ce domaine capacitaire : la « donnée », l'automatisation des tâches récurrentes, l'interopérabilité, l'innovation et l'interconnexion ; - Une doctrine de lutte

informatique offensive (LIO), qui vise à faire partager les grands principes d'emploi et de strict encadrement, notamment juridique, de cette composante opérationnelle militaire, dont la vocation est d'accompagner l'engagement des armées dans le cyberespace ; - Un White paper sur le droit international appliqué aux opérations dans le cyberespace. Fruit des travaux menés conjointement par le COMCYBER, la direction des affaires juridiques et la direction générale des relations internationales et stratégiques, ce document a été transmis à la rentrée 2019 à toutes les ambassades de France et représentations diplomatiques. Enfin, le COMCYBER développe des coopérations internationales à vocation opérationnelle, afin de consolider ses capacités d'anticipation et d'action dans le cyberespace, par un renforcement du partage d'informations sur les incidents et la lutte informatique défensive. En outre, il contribue activement aux travaux au sein de l'Organisation du traité de l'Atlantique Nord et de l'Union européenne.

Données clés

Auteur : M. Christophe Blanchet
Circonscription : Calvados (4e circonscription) - La République en Marche
Type de question : Question écrite
Numéro de la question : 23658
Rubrique : Défense
Ministère interrogé : Armées
Ministère attributaire : Armées

Date(s) clée(s)

Question publiée au JO le : 15 octobre 2019, page 8610
Réponse publiée au JO le : 7 janvier 2020, page 69