ASSEMBLÉE NATIONALE

16ème législature

Interrogations sur les VBMR face aux cyberattaques.

Question écrite n° 17096

Texte de la question

Mme Gisèle Lelouis attire l'attention de M. le ministre des armées sur les failles concernant les véhicules blindés multi-rôles (VBMR). Depuis la parution du Livre blanc sur la défense et la sécurité nationale en 2013 et dans le cadre du programme Scorpion visant à moderniser l'armement terrestre, la France remplace ses nombreux véhicules de l'avant blindés (VAB) au profit du VBMR. Ce remplacement, sans réelle augmentation des effectifs blindés, posait déjà la question d'une dispersion des modèles pour l'industrie quand la France n'en avait autrefois qu'un, évitant un « cauchemar logistique », alors qu'il est connu que la haute intensité se joue aussi sur la masse (car il faut du nombre pour contrôler une zone, ce qu'une armée d'échantillons, même la plus sophistiquée, ne peut faire) avec des modèles « bon marché » rapides à produire, d'excellentes capacités tout-terrains etc., même si l'indispensable capacité de projection « des gabarits SNCF » est assurée. Ces derniers véhicules blindés multi-rôles, incarnés par les Griffon et les Serval sont de véritables laboratoires technologiques, avec de grandes capacités, démontrant le savoir-faire de l'industrie française. Coutant donc le double d'un VAB, ils sont en train de devenir la colonne vertébrale de l'armée de terre française, malgré certains retards de livraison. Sur les 1872 VBMR Griffon prévus en 2019 pour l'horizon 2030, 575 ont bien été livrés en 2024 et 208 VBMR-L Serval sur 978. Ces blindés assurent ainsi les fonctions de protections balistiques, le transport, la communication et l'observation sur le terrain. Cependant, au cours de l'entraînement interarmées de cyberdéfense (DEFNET) organisé du 18 au 29 mars 2024, un militaire est parvenu à mettre en panne un véhicule blindé multi-rôle Griffon. En effet, à l'aide d'un télémètre développé par l'armée, le militaire est parvenu à perturber le système informatique du véhicule le forçant à freiner et le mettant momentanément hors de combat. Plus encore, les dégâts causés au véhicule par l'appareil peuvent compromettre le réseau de communication. L'impact de cet incident ne doit pas être négligé. En effet, le véhicule blindé multi-rôle Griffon se décline en plusieurs modèles. Il joue donc des rôles clefs dans de nombreux secteurs tels que le transport de troupes (Griffon VTT), l'observation de l'artillerie (Griffon VOA), le commandement (Griffon VPC) et les opérations médicales (Griffon SAN) etc. La mise hors combat de ces véhicules à la suite d'une cyberattaque en fait une cible facile pour l'adversaire et la compromission du réseau de communication qui en découle fragilise grandement l'intégrité de tout le réseau de communication de l'armée française. Cet évènement met également en lumière la portée informationnelle de telles attaques. En effet, la diffusion d'image des véhicules immobilisés à la suite de cyberattaque au sein de l'espace médiatique peut saper la confiance que portent les Français, y compris militaires, dans l'efficacité de l'armée. Ainsi, l'armée française doit être en mesure de répondre à ces éventuelles diffusions et pallier sa vulnérabilité actuelle aux cyberattaques tactiques. On peut également questionner la portée globale de cette vulnérabilité aux cyberattaques. Celle-ci, concerne-t-elle tous les types de véhicules blindés multi-rôles ? L'EBRC Jaguar dont 60 exemplaires ont été réceptionnés sur les 300 prévus pour 2030 présente-t-il la même vulnérabilité au cyber ? Ce dernier présentait déjà un défaut avec sa tourelle T40, qui héberge deux missiles MMP sous blindage, dans un lanceur rétractable, avec deux autres munitions disponibles en soute, obligeant l'un des trois membres d'équipage ayant perdu à la courte paille, de s'exposer pour recharger, la menace cyber lui ajoutant un possible nouveau défaut. La stratégie politico-industrielle du tout technologique nécessite une adaptabilité et des ajustements nécessaires, malheureusement coûteux pour maintenir une opérabilité efficace des armées. Ainsi, dans la mesure où cette vulnérabilité s'étendrait à l'ensemble des modèles VBMR ou véhicules blindés reliés au réseau, cet évènement pose la question de la

vulnérabilité et de la place des systèmes informatiques au sein des forces armées. La protection et l'intégrité de ces systèmes sont une nécessité absolue pour assurer le bon fonctionnement de l'armée de terre. Alors, doit-on revoir la place et l'importance des systèmes informatiques au sein des véhicules blindés, ou renforcer la sécurisation des systèmes informatiques de ceux-ci ? Si c'est le cas, Mme la députée demande à M. le ministre ce qu'il compte faire pour pallier la vulnérabilité des systèmes informatiques des VBMR face aux éventuelles cyberattaques, afin d'assurer l'efficacité de l'armée française. Par ailleurs, certaines questions se posent sur les blindés « remplacés » par les VBMR, à savoir les VAB. M. le ministre a annoncé l'envoi à l'étranger de « centaines de blindés » français d'occasion. Elle lui demande s'il ne serait pas aussi judicieux d'en garder en stock pour « faire masse », pallier d'éventuelles défaillances des VBMR, voire d'en équiper les unités élémentaires de réserve de l'armée de terre au vu des projets de croissance.

Données clés

Auteur : Mme Gisèle Lelouis
Circonscription : Bouches-du-Rhône (3e circonscription) - Rassemblement National
Type de question : Question écrite
Numéro de la question : 17096
Rubrique : Défense
Ministère interrogé : Armées
Ministère attributaire : Armées

Date(s) clée(s)

Question publiée au JO le : 16 avril 2024, page 2903
Question retirée le : 11 juin 2024 (Fin de mandat)