ASSEMBLÉE NATIONALE

17ème législature

Sabotage à bas coût de l'électronique militaire : quelle résilience ?

Question écrite n° 11901

Texte de la question

M. Marc Chavent interroge Mme la ministre des armées et des anciens combattants sur la manière dont les conflits récents ont mis en évidence l'émergence de modes d'action militaires reposant sur le sabotage ciblé à très bas coût, visant non plus uniquement les équipements de communication, mais plus largement l'ensemble de l'électronique critique sur laquelle repose aujourd'hui la conduite des opérations militaires. Des opérations documentées ont montré qu'il était possible, par la compromission d'équipements électroniques apparemment secondaires (capteurs, systèmes de navigation, composants embarqués, dispositifs de contrôle ou de maintenance) de provoquer des effets militaires disproportionnés : dysfonctionnements simultanés, perte de confiance dans les systèmes, ralentissement de la chaîne décisionnelle et désorganisation ponctuelle mais critique des forces engagées. Dans un contexte où les forces françaises s'appuient de manière croissante sur des systèmes numérisés, interconnectés et largement automatisés, du combattant débarqué aux plateformes majeures, en passant par la logistique, la maintenance, les munitions et les systèmes de commandement, la question de la résilience ne se limite plus aux seules communications. Elle concerne désormais la sécurité et la robustesse de l'ensemble de l'écosystème électronique militaire et dual, souvent issu de chaînes d'approvisionnement mondialisées et complexes. Alors que la vitesse de décision est devenue un facteur déterminant (celui qui décide en quelques secondes l'emportant sur celui qui décide en quelques minutes), une altération, même temporaire, de la fiabilité des systèmes électroniques pourrait suffire à créer un avantage décisif pour un adversaire, sans confrontation directe. Dès lors, il souhaite savoir si le Gouvernement estime que la France est aujourd'hui suffisamment préparée à faire face à des actions de sabotage ciblé portant sur l'ensemble de son électronique militaire et dual, au-delà des seuls équipements de communication, et quelles mesures concrètes sont mises en œuvre ou envisagées pour garantir la sécurité, la traçabilité et la résilience des chaînes technologiques critiques, afin d'éviter qu'une vulnérabilité de ce type ne puisse, à faible coût, désorganiser son appareil de défense ou ralentir sa capacité de réaction en cas de crise majeure.

Texte de la réponse

Le ministère des armées et des anciens combattants est conscient des vulnérabilités pouvant entraîner la compromission d'équipements électroniques, qu'il s'agisse de systèmes de navigation, de contrôle ou de maintenance, et provoquer des dysfonctionnements simultanés et une désorganisation ponctuelle mais critique des forces engagées. Le ministère est particulièrement sensible à la protection des entités participant aux programmes d'armement. Plusieurs dispositifs sont mis en œuvre afin de protéger ces entités des risques de sabotage physique ou numérique. Ils portent notamment sur la sécurité des activités d'importance vitale et la protection du secret de la défense nationale et concernent les grands maîtres d'œuvre, l'industrie de façon plus générale ainsi que les sociétés détenant des informations et des supports classifiés. Une attention spécifique est portée sur les PME et ETI, qui peuvent bénéficier du dispositif subventionné Diag Cybersécurité mis en place par BPIFrance avec le soutien de la direction générale de l'armement : en 2025, 80 contrats de diagnostic ont été signés. En particulier, les systèmes d'information employés pour l'exécution des marchés d'armement sont soumis à une démarche d'homologation. Celle-ci repose sur une analyse globale des risques, prenant en compte tous les éléments essentiels au fonctionnement et à la sécurité du système. Afin de mieux sécuriser le tissu industriel, composé entre autres de petites et moyennes entreprises, sur lequel reposent les chaînes de

sous-traitance des programmes d'armement, la direction générale de l'armement produit un référentiel de maturité cyber et un référentiel de sûreté physique.

Données clés

Auteur : M. Marc Chavent
Circonscription : Ain (5e circonscription) - Union des droites pour la République
Type de question : Question écrite
Numéro de la question : 11901
Rubrique : Défense
Ministère interrogé : Armées et anciens combattants
Ministère attributaire : Armées et anciens combattants

Date(s) clée(s)

Question publiée au JO le : 23 décembre 2025, page 10429
Réponse publiée au JO le : 12 mai 2026, page 4131