



ASSEMBLÉE NATIONALE

17ème législature

Sécurité des radios tactiques : chaîne d'approvisionnement et cyber-sabotage

Question écrite n° 12912

Texte de la question

M. Marc Chavent interroge Mme la ministre des armées et des anciens combattants sur l'acquisition de 14 000 radios individuelles pour les combattants débarqués et 1 000 radios véhicules, équipements critiques pour le commandement, la géolocalisation et l'échange de données tactiques. Plusieurs conflits récents ont montré que les équipements de communication peuvent devenir des vecteurs directs de vulnérabilité opérationnelle : radios et pagers piégés ou compromis à la source utilisés par le Hezbollah, interception et injection de faux ordres sur des réseaux radios tactiques en Ukraine, exploitation de *firmwares* modifiés ou de fonctions dormantes sur des équipements livrés intacts mais dégradés en situation réelle, ou utilisation d'interfaces secondaires (Bluetooth, ports de maintenance) comme points d'entrée lors d'exercices OTAN de type RED TEAM. Ces exemples démontrent que la menace ne se limite plus au simple brouillage ou à l'écoute, mais inclut désormais des attaques combinant sabotage industriel, compromission logicielle et interception/manipulation des flux tactiques, incluant des scénarios de type *man-in-the-middle*. Dans ce contexte, il lui demande quelles garanties sont exigées pour sécuriser l'intégrité de la chaîne d'approvisionnement, des composants électroniques et du *firmware*, contre toute altération volontaire ou mécanisme de sabotage à déclenchement différé ; quelles méthodes d'audit et de tests logiciels permettent de détecter toute manipulation subtile du comportement des radios en conditions opérationnelles, y compris des attaques de type *man-in-the-middle* ; comment les interfaces IP, Bluetooth et protocoles radio tactiques sont protégées contre les interceptions, injections ou altérations de flux par des acteurs hostiles et quelles mesures empêchent toute exploitation hostile de la géolocalisation amie et des métadonnées de communication. Il lui demande également si elle peut confirmer que l'ensemble de ces mesures garantit la résilience opérationnelle et la sécurité tactique des forces françaises, même face à des attaques d'un nouveau genre combinant sabotage industriel, compromission logicielle et manipulation des flux radio.

Données clés

Auteur : [M. Marc Chavent](#)

Circonscription : Ain (5^e circonscription) - Union des droites pour la République

Type de question : Question écrite

Numéro de la question : 12912

Rubrique : Défense

Ministère interrogé : [Armées et anciens combattants](#)

Ministère attributaire : [Armées et anciens combattants](#)

Date(s) clé(s)

Question publiée au JO le : [17 février 2026](#), page 1305