ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 1712	De **M. Michaël Taverne** (Rassemblement National - Nord)	**Question écrite**

Ministère interrogé > Intérieur et outre-mer	**Ministère attributaire** > Intérieur et outre-mer

Rubrique >collectivités territoriales	**Tête d'analyse** >Insuffisances de la cybersécurité des communes rurales et de taille moyenne	**Analyse** > Insuffisances de la cybersécurité des communes rurales et de taille moyenne.

Question publiée au JO le : **04/10/2022**
Réponse publiée au JO le : **24/01/2023** page : **678**

Texte de la question

M. Michaël Taverne attire l'attention de M. le ministre de l'intérieur et des outre-mer sur la problématique des lacunes en matière de cybersécurité dans les communes rurales et de taille moyenne. En effet, ainsi que l'a révélé une enquête menée en 2021 par le site *cybermalveillance.gouv.fr* auprès des municipalités de communes de moins de 3 500 habitants, les enjeux de cybersécurité sont peu identifiés, peu considérés et donc peu anticipés puisque 65 % des collectivités interrogées estiment que le risque numérique est faible, voire inexistant, ou ne savent pas l'évaluer. Alors que la sécurité des systèmes d'informations est un enjeu majeur pour les organismes publics, qu'ils relèvent de l'État ou des collectivités locales, il apparaît nécessaire de mieux organiser la formation des élus locaux mais aussi des agents territoriaux, notamment dans les communes rurales et de taille moyenne qui ne disposent que de peu de moyens, notamment en matière de capital humain, pour faire face à ces problématiques qui pourtant pourraient entraîner une paralysie totale de leur fonctionnement en cas de cyber-attaque ou de panne généralisée. Il demande donc au Gouvernement quelles actions sont envisagées afin de répondre à ce besoin des collectivités.

Texte de la réponse

Bien que les collectivités territoriales sont responsables de la sécurisation de leurs propres systèmes d'information, le ministère de l'Intérieur et des Outre-mer est pleinement conscient des situations parfois précaires et des multiples attaques cyber que ces dernières subissent. Pour cette raison, le secrétaire général du ministère a, par circulaire en date du 20 avril 2022, rappelé aux préfets de région et de département la nécessité de structurer l'action publique territoriale en leur assignant un rôle de coordination des différents acteurs locaux : délégué régional de l'ANSSI, conseils régionaux par le biais des CIRT régionaux (centres de conseils et de soutien vis-à-vis des collectivités locales et des TPE/PME en cas de de cyberattaque, dotés chacun d'un million d'euros du plan France Relance). Les préfets de région et de département réalisent cette action de coordination dans le but de structurer la politique de sensibilisation et de prévenir et de gérer une éventuelle crise déclenchée par une attaque numérique qui aura des impacts sur la vie économique et sociale. La DGSI, la DGPN et la DGGN assurent pour leur part une mission de sensibilisation à la cybermenace en organisant des sessions d'information aux bénéfices de nombreux élus locaux, collecitivités et PME. Même si cela ne relève pas du périmètre du ministère de l'Intérieur et des Outre-mer, une partie des 136 millions d'euros, spécialement fléchée sur la cybersécurité dans le cadre du plan France Relance, est dédiée au renforcement des capacités de cyberdéfense des territoires. Selon l'agence nationale de la sécurité des systèmes d'information (ANSSI), « le volet cybersécurité de France Relance […] cible en priorité certains secteurs et

entités parmi les plus critiques, dont la cybersécurité nécessite un renforcement urgent et soutenu. Il accorde ainsi une importance particulière aux collectivités territoriales et aux organismes au service du citoyen, en particulier dans le domaine social, de la santé, de la formation et de l'information ». L'ANSSI pourra bien évidement rendre compte de son action globale sur le sujet.