# ASSEMBLÉE NATIONALE

15ème législature

## Clarification de la prévention contre les cybermenaces

Question écrite n° 34715

### Texte de la question

M. Sébastien Chenu interroge M. le ministre de l'intérieur sur la multiplication des cyberattaques sur le territoire. Dans la nuit du 24 au 25 novembre 2020, la mairie d'Aulnoye-Aymeries, commune du Nord, a été pris pour cible d'une cyberattaque, laquelle lui aura dérobé plusieurs fichiers. Contre le rendu de ces fichiers, les pirates ont réclamé rançon le lendemain ; celle-ci s'élevait à 150 000 euros. Les attaques dématérialisées ne sont pas chose nouvelle. Depuis le premier confinement, les vagues d'attaques se sont démultipliées ; d'après les statistiques récoltées par Orange cyberdéfense, leur progression se comprendrait à la hauteur de 25 % depuis le commencement de la pandémie en France. Elles ont touché aussi bien les particuliers, les entreprises que les services publics. Néanmoins, il existe une véritable incertitude généralisée quant aux moyens de protection et aux procédures de réponse face à de telles atteintes à l'intégrité numérique des personnes physiques ou morales. Cette expansion de la cybercriminalité tend à questionner l'efficacité pratique des rapports de lutte contre la cybermenace, qui pourtant sont légion depuis le début du quinquennat. La priorité n'est donc pas uniquement à la sensibilisation et au soutien de politiques industrielle de la sécurité numérique. Il est essentiel de systématiser des codes de procédure complets et clairs pour l'ensemble des acteurs de l'économie nationale, quels que soient leur taille, leur secteur ou leur ancrage dans le territoire. Étant donné la rapidité d'une bonne défense contre une cyberattaque, un tel code offrirait à tout acteur la possibilité de se défendre efficacement. D'autre part, il est plus que nécessaire de prévoir des mesures concrètes de prévention. Si la sensibilisation des acteurs ayant accès à des postes de travail individuel revêt une part fondamentale, il reste qu'imputer la responsabilité de première riposte à un individu exerçant son emploi n'est pas un cadre propice à l'épanouissement des travailleurs sur leur lieu de travail. La prospective de l'accroissement statistique des cyberattaques sur le territoire national requiert donc un plan de prévention macroéconomique, telle que la déconnexion systématique durant les heures de hors-activité des réseaux d'ordinateurs, des disques externes et autres terminaux reliés, si cet arrêt ne pose aucun risque. Enfin, la dernière clarification devrait être portée sur la pénalité imposée aux cybercriminels récidivistes. Il est notamment important de réfléchir à la qualité du système pénal international pour ce qui concerne les commanditaires des cyberattaques, ainsi que celle des brigades de traçage des cybercriminels issus du territoire national. Réciproquement, étant donné la prolifération de ce type de crime, il serait important d'augmenter le coût des pénalités encourues afin de renforcer le caractère dissuasif de la loi. Il lui demande ainsi s'il envisage un protocole que chaque acteur économique peut avoir à disposition, à l'image des plans d'urgence de la MEAE, pour expliciter des pratiques de prévention et de défense autonome, tout en renforçant le code pénal sur la cybercriminalité *via* le durcissement des peines dès la première récidive.

### Données clés

**Auteur :** M. Sébastien Chenu
**Circonscription :** Nord (19e circonscription) - Non inscrit
**Type de question :** Question écrite
**Numéro de la question :** 34715
**Rubrique :** Internet
**Ministère interrogé :** Intérieur

Version web : https://www.assemblee-nationale.fr/dyn/15/questions/QANR5L15QE34715

**Ministère attributaire :** Intérieur

## Date(s) clée(s)

**Question publiée au JO le :** 8 décembre 2020, page 8886
**Question retirée le :** 21 juin 2022 (Fin de mandat)