



ASSEMBLÉE NATIONALE

17ème législature

Cybersécurité dans l'éducation nationale et l'enseignement supérieur

Question écrite n° 14457

Texte de la question

M. Anthony Boulogne interpelle Mme la ministre déléguée auprès du ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique, chargée de l'intelligence artificielle et du numérique, sur la montée des cybermenaces pesant sur les établissements scolaires et de l'enseignement supérieur et les moyens publics mis en œuvre pour renforcer la sécurité informatique de ces entités. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié mercredi 11 mars 2026 le Panorama de la cybermenace de l'année 2025. 1366 incidents de sécurité (événements découlant d'actions menées par des acteurs malveillants sur un système d'information) ont été portés à la connaissance de l'ANSSI, soit un nombre équivalent à 2024 mais en nette progression par rapport aux années précédentes (1 112 en 2023 et 831 en 2022). La croissance des incidents de sécurité traités par l'ANSSI démontre bien une montée de la cybermenace dans le pays. Sur les 1 366 incidents portés à la connaissance de l'ANSSI, 34 % concernent le secteur de l'éducation et de la recherche. 128 compromissions par rançongiciel ont été enregistrées, une menace qualifiée d'importante par l'institution. Si les acteurs économiques sont les principales victimes de ce type d'attaques, les écoles françaises sont désormais ciblées. Ainsi selon l'ANSSI : « les établissements scolaires, notamment d'enseignement primaire et secondaire, ont été particulièrement touchés en 2025. Ces incidents ont pu avoir des impacts conséquents et visibles sur ces structures, forçant parfois la mise en œuvre d'un mode de fonctionnement dégradé pendant plusieurs semaines, avec notamment des difficultés d'accès à des ressources internes aux établissements ». Les établissements relevant de l'enseignement supérieur ne sont pas épargnés par les cybermenaces : diffusion de campagnes d'hameçonnage après la compromission de comptes de messagerie du personnel ou d'étudiants ; mise à l'arrêt de sites internet appartenant à des entités du secteur de l'éducation ou modification des contenus hébergés au sein de ces sites. Les acteurs cybercriminels agissent, dans ces cas-là, par pur opportunisme en s'engouffrant dans des failles de sécurité informatique. Certains incidents peuvent provoquer l'interruption totale du système d'information de l'établissement pris pour cible. L'ANSSI relève également le ciblage d'entités hébergeant des activités sensibles, citant notamment « la compromission de ressources d'intérêt appartenant à un institut de recherche français ». L'intérêt des attaquants est clair : cibler des acteurs français de la recherche, à des fins d'espionnage ou de pré-positionnement dans les systèmes informatiques en vue d'une attaque ultérieure. Le développement des capacités d'action des attaquants, notamment *via* l'intelligence artificielle, risque d'accroître la vulnérabilité d'entités dont le niveau de sécurité informatique laisse à désirer, notamment les petites structures scolaires disposant de moyens limités en la matière. S'agissant des établissements d'enseignement supérieur et accueillant des activités de recherche, la menace d'espionnage et de captation d'informations stratégiques (par exemple : touchant des activités liées à la BITD) va continuer de se développer du fait des logiques agressives des compétiteurs. L'État ne peut pas rester immobile face à une telle situation. M. le député demande donc à Mme la ministre de lui détailler quelles mesures l'État compte mettre en œuvre pour renforcer la sécurité informatique des établissements scolaires et mieux protéger les établissements de l'enseignement supérieur et les instituts de recherche, particulièrement vulnérables aux tentatives d'espionnage. M. le député insiste sur la nécessité de renforcer, de manière globale, la résilience des entités publiques et privées face à la recrudescence des cyberattaques et l'exacerbation des menaces émanant des compétiteurs stratégiques. Il souhaite connaître ses intentions à ce sujet.

Données clés

Auteur : [M. Anthony Boulogne](#)

Circonscription : Meurthe-et-Moselle (6^e circonscription) - Rassemblement National

Type de question : Question écrite

Numéro de la question : 14457

Rubrique : Enseignement

Ministère interrogé : [Intelligence artificielle et numérique](#)

Ministère attributaire : [Premier ministre](#)

Date(s) clé(s)

Question publiée au JO le : [21 avril 2026](#), page 3303