GRAND CONSEIL **Q 4182**
de la République et canton de Genève

Signataire : Diane Barbier-Mueller

Date de dépôt : 25 novembre 2026

Question écrite

Cyberattaques : nos infrastructures essentielles peuvent-elles fonctionner sans internet ?

En octobre et novembre 2026, plusieurs vagues de cyberattaques ont touché les installations frigorifiques de centaines de supermarchés européens[1]. En exploitant des vulnérabilités de systèmes de contrôle connectés à internet, des pirates sont parvenus à modifier à distance les températures des réfrigérateurs et congélateurs, parfois jusqu'à 50 °C, provoquant la destruction de marchandises et des interruptions d'activité.

Ces attaques ont également touché la Suisse, comme l'a confirmé l'Office fédéral de la cybersécurité (OFCS) dans une alerte publiée le 10 novembre 2026[2]. Celui-ci souligne que les risques ne concernent pas uniquement les commerces alimentaires, mais également les pharmacies, les laboratoires et les établissements de santé.

Ces événements mettent en lumière une vulnérabilité préoccupante : la dépendance croissante d'équipements physiques essentiels à des systèmes informatiques connectés à internet.

Cette dépendance constitue un risque en cas de panne généralisée d'internet ou d'interruption majeure des réseaux de télécommunication, qu'elle résulte d'une défaillance technique, d'un incident affectant les infrastructures ou d'une cyberattaque.

---

1 Article d'Euronews : https://fr.euronews.com/2026/11/02/cyberattaque-vise-les-systemes-de-refrigeration-de-supermarches-en-europe

2 Alerte de l'Office fédéral de la cybersécurité : https://www.bacs.admin.ch/fr/warnung-kuehlanlagen-fr

Si la numérisation permet d'améliorer l'efficacité et la supervision des installations, elle ne devrait pas compromettre leur capacité à fonctionner de manière autonome en cas de cyberattaque ou de panne généralisée des réseaux.

Cette problématique concerne particulièrement les infrastructures dont dépend directement la sécurité de la population : les Hôpitaux universitaires de Genève (HUG), les établissements de soins, les installations de distribution d'eau et d'énergie, mais également les équipements frigorifiques nécessaires à l'approvisionnement alimentaire et à la conservation de médicaments.

Le Grand Conseil s'est déjà penché sur les enjeux de cybersécurité, notamment dans le cadre de la motion M 2922 et de la stratégie cantonale présentée en réponse par le Conseil d'Etat. Toutefois, la question de la capacité des équipements physiques essentiels à poursuivre leur fonctionnement lorsqu'ils sont déconnectés d'internet mérite d'être examinée plus spécifiquement.

Je prie donc le Conseil d'Etat de répondre aux questions suivantes :

- ***Les équipements essentiels au fonctionnement des infrastructures publiques genevoises, notamment des HUG, des établissements de soins et des installations d'approvisionnement en eau et en énergie, peuvent-ils continuer à assurer leurs fonctions critiques en cas de déconnexion d'internet ou d'isolement de leurs réseaux informatiques ?***
- ***Lorsque cette autonomie n'est pas garantie, quelles mesures sont prévues pour garantir la continuité de ces fonctions en cas de cyberattaque ?***
- ***Des tests sont-ils régulièrement effectués pour vérifier que les équipements essentiels des infrastructures publiques peuvent continuer à fonctionner de manière autonome en cas de déconnexion d'internet ou d'isolement de leurs réseaux informatiques ?***
- ***Quelles mesures le Conseil d'Etat a-t-il prises ou entend-il prendre pour sensibiliser les exploitants privés d'infrastructures essentielles, notamment les supermarchés, les pharmacies et les entreprises de stockage alimentaire, aux risques liés aux équipements connectés et à la nécessité de garantir leur fonctionnement en cas de déconnexion ?***

Je remercie d'avance le Conseil d'Etat de ses réponses.