ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 17445	De **Mme Alexandra Martin (Alpes-Maritimes)** (Les Républicains - Alpes-Maritimes)	**Question écrite**
Ministère interrogé > Intérieur et outre-mer	**Ministère attributaire** > Intérieur et outre-mer	
Rubrique >établissements de santé	**Tête d'analyse** >Cyberattaques perpétrées à l'encontre des établissements hospitaliers	**Analyse** > Cyberattaques perpétrées à l'encontre des établissements hospitaliers.
Question publiée au JO le : **30/04/2024** Question retirée le : **11/06/2024** (fin de mandat)		

Texte de la question

Mme Alexandra Martin (Alpes-Maritimes) appelle l'attention de M. le ministre de l'intérieur et des outre-mer sur les cyberattaques perpétrées à l'encontre des établissements hospitaliers. Le mardi 16 avril 2024, le centre hospitalier Simone Veil de Cannes a été la cible d'une cyberattaque paralysant son activité. En conséquence, il a été décidé le report des consultations et des opérations non urgentes, n'entraînant pas de perte de chance. Près d'un tiers de l'activité opératoire a été déprogrammée. La direction de l'établissement de santé a, en effet, pris la décision d'activer une cellule de crise en lien avec l'agence régionale de santé de PACA, laquelle prévoit un cyberconfinement général privant l'hôpital de ses accès informatiques. Les professionnels de l'hôpital appliquent dès lors les procédures dites dégradées et ont donc recours à des kits papiers, lesquels allongent de manière considérable les procédures et retardent les rendus d'examens. Il s'agit de la première cyberattaque d'ampleur à laquelle le centre hospitalier Simone Veil de Cannes a été confronté. Sa préparation et les derniers exercices anti-cyberattaques ont permis la réactivité de l'hôpital face à l'évènement. Il n'en demeure pas moins que son activité a été fortement perturbée par l'attaque. Si à ce stade, aucune rançon ni de vol de données n'ont été encore identifiés, les questions demeurent quant aux motivations des agresseurs. De manière préventive, l'hôpital a procédé à une pré-déclaration auprès de la CNIL. La direction de l'hôpital craint en effet le piratage de données subi en février 2024 par l'hôpital d'Armentières. À la suite d'une attaque semblable à celle perpétrée contre l'hôpital de Cannes, les dossiers médicaux de plus de 950 000 patients ont été diffusés sur le *dark web*. Les assaillants numériques ont exigé une rançon pour restaurer l'accès aux données de l'établissement de soins. En représailles de son refus - comme la loi le prévoit -, les criminels ont publié plus de 18 Go de données confidentielles, incluant des adresses, des numéros de téléphone, des antécédents médicaux, des photos, des documents des patients de l'hôpital depuis 2014. Les attaques de ce type contre les établissements publics sont de plus en plus fréquentes. Elles entraînent des perturbations importantes pour les services de santé et mettent en péril la confidentialité des données et informations médicales des patients. Pourtant, des moyens de prévention et de sécurisation des logiciels existent. Une tentative de cyberattaque contre les hôpitaux niçois a récemment été déjouée, grâce à des pare-feux. Il s'agit de dispositifs de sécurité qui protègent les ordinateurs connectés à un réseau des tentatives d'intrusion qui pourraient en provenir. Seulement, ces dispositifs représentent un coût certain pour des établissements dont la première mission est d'assurer des soins. Aussi, elle lui demande comment le Gouvernement entend protéger les centres hospitaliers de ces attaques en ligne et s'il envisage d'allouer des moyens pour leur permettre de s'équiper en matériels de protection informatique.