ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 39124	De **M. François-Michel Lambert** (Libertés et Territoires - Bouches-du-Rhône)	**Question écrite**
Ministère interrogé > Transition numérique et communications électroniques	**Ministère attributaire** > Première ministre	
Rubrique >Internet	**Tête d'analyse** >Résilience des territoires - cybersécurité des infrastructures essentielles	**Analyse** > Résilience des territoires - cybersécurité des infrastructures essentielles.
Question publiée au JO le : **25/05/2021** Réponse publiée au JO le : **21/06/2022** page : **3362** Date de changement d'attribution : **17/05/2022**		

Texte de la question

M. François-Michel Lambert attire l'attention de M. le secrétaire d'État auprès des ministres de l'économie, des finances et de la relance, et de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques, sur la résilience des territoires du fait des risques pesant sur les infrastructures essentielles du pays face aux cyberattaques de plus en plus nombreuses. Le 7 mai 2021, les États-Unis ont subi une cyberattaque de grande ampleur sur leur plus grand oléoduc d'essence. La paralysie d'une partie conséquente de leur réseau de distribution d'essence a des conséquences sociales importantes, à travers l'augmentation du cours du pétrole et la crainte d'une pénurie de carburant dans certaines régions. Cette cyberattaque montre une fois de plus la vulnérabilité des infrastructures essentielles face aux attaques des *hackers*. À l'instar des États-Unis, la France a subi de nombreuses cyberattaques, 192 en 2020 selon l'ANSSI, notamment sur ses hôpitaux, particulièrement vulnérables en période de pandémie. Ces attaques se traduisent par un danger réel et concret pour les vies et les conditions de vie des citoyens. Les attaques sur les hôpitaux peuvent impacter l'accès au soin et plus généralement, celles sur les infrastructures essentielles françaises peuvent impacter un ensemble de besoins essentiels à la vie quotidienne. Concrètement, les Français pourraient voir leurs approvisionnements en eau, en électricité ou en carburant momentanément perturbés voire interrompus, ou voir leurs prix augmenter rapidement, accentuant les difficultés des plus fragiles. Si ces risques doivent être prévenus, il s'agit aussi de rendre le système économique et social français résilient face à ce type de menaces, territoire par territoire, par une meilleure connaissance de leurs faiblesses et de leurs expositions à certains risques particuliers liés à des infrastructures essentielles. Il lui demande en conséquence quelles dispositions structurelles entend mettre en œuvre le Gouvernement pour garantir une résilience des territoires face à ces diverses cybermenaces, et notamment en matière de préservation de la santé et du pouvoir d'achat des citoyens.

Texte de la réponse

La politique publique de renforcement de la cybersécurité a d'ores et déjà connu deux étapes : une étape de création à partir de 2009 et une étape centrée sur un travail de conviction et de partage de la vision de la menace depuis 2015. La XVIe législature sera le début d'une troisième étape, centrée sur un changement d'échelle des mesures de renforcement mises en œuvre. Au moins trois axes d'effort ont été identifiés. Le premier est la

sensibilisation qui, plus qu'un objectif, est un processus permanent. Cette sensibilisation vise au premier chef le grand public afin de généraliser les pratiques de cybersécurité et de protection des données sensibles. C'est pour répondre aux besoins du grand public que cybermalveillance.gouv.fr, groupement d'intérêt public, administre une plateforme d'assistance aux victimes au travers de laquelle l'ensemble des bonnes pratiques en matière numérique sont diffusées. Le deuxième axe est la prévention : l'ANSSI produit de nombreux guides et recommandations pour développer des systèmes d'information en toute sécurité. Des prestataires de services sont qualifiés par l'ANSSI et peuvent être mis à contribution pour installer des systèmes sécurisés. Le recours à de tels systèmes doit être amplifié. C'est déjà le cas dans le cadre de la commande publique avec des clauses de sécurité de systèmes d'information type établies par la direction des achats de l'État (DAE) et l'ANSSI. Le troisième axe est la réaction aux incidents. La capacité de réponse à incidents continue de s'améliorer avec la création de Cyber Security Incident Response Teams (CSIRT) régionaux ou sectoriels. Le recours au pouvoir de sanctions de la CNIL est également un outil efficace pour inciter l'ensemble des acteurs à améliorer leur cybersécurité. Enfin, l'accent mis sur la réponse pénale à la cybercriminalité, passant préalablement par l'action des services enquêteurs, est utile pour mettre fin au sentiment d'impunité de certains cybercriminels. Par ailleurs, le renforcement de la cybersécurité et la limitation des risques touchant les particuliers et les entreprises constitue également une priorité européenne. Ainsi, la Commission européenne a publié le 16 décembre 2020 une ambitieuse proposition d'évolution de la directive Network and Information System (NIS). Le texte a pour objectif d'harmoniser les exigences de cybersécurité entre les États membres et de définir des mécanismes de coopération pour mieux gérer les risques de cybersécurité. La proposition prévoit également une extension du champ de la régulation, fixant les critères pour qualifier les « opérateurs de services essentiels », auparavant laissés à la main des États. S'ajoutent aux domaines actuellement régulés (banques, marchés financiers, énergie, transports, santé, eau potable et réseaux télécoms) de nouveaux secteurs tels que la gestion des déchets, les services postaux, ou encore les fournisseurs d'accès à internet (FAI) et les datacenters. Le périmètre d'application de la directive se voit donc étendu à la majorité des opérateurs de chaque secteur d'activité, faisant ainsi passer le nombre d'opérateurs supervisés de quelques centaines à plusieurs milliers. La proposition vise également à renforcer la cybersécurité des entités dans leur globalité, en prenant notamment en compte la chaîne de sous-traitance et non plus seulement la sécurisation des systèmes d'information supportant des services essentiels (SIE). Les autorités françaises souscrivent pleinement à l'ambition européenne. La transposition de la future directive élèvera sensiblement le niveau de cybersécurité des opérateurs français. De surcroît, un travail exploratoire est en cours afin de déterminer les dispositions législatives utiles à un renforcement des pouvoirs de l'État dans l'encadrement de la cybersécurité. A l'issue, le Gouvernement déterminera l'étendue des mesures législatives à soumettre au Parlement.