



16ème législature

Question N° : 10948	De Mme Nathalie Da Conceicao Carvalho (Rassemblement National - Essonne)	Question écrite
Ministère interrogé > Première ministre		Ministère attributaire > Première ministre
Rubrique > ministères et secrétariats d'État	Tête d'analyse > Renforcement de la cybersécurité	Analyse > Renforcement de la cybersécurité.
Question publiée au JO le : 22/08/2023 Réponse publiée au JO le : 31/10/2023 page : 9681		

Texte de la question

Mme Nathalie Da Conceicao Carvalho appelle l'attention de Mme la Première ministre sur l'ambition annoncée de la France dans sa loi de programmation militaire de renforcer la cybersécurité et d'améliorer la résilience des entreprises et organismes publics sensibles. En consacrant 413,3 milliards d'euros aux armées dont 10 milliards d'euros pour les investissements technologiques, la France souhaite rattraper son retard dans le contexte géopolitique que l'on connaît. Cependant, cette loi ne permet pas d'appréhender clairement comment les enjeux liés à la protection cyber seront traités par les autres ministères de l'État. Les exemples récents sur les hôpitaux paralysés plusieurs jours montrent que l'exposition est forte dans ces établissements et que le manque de moyens représente un risque sur la continuité des soins d'urgences. Aussi, elle lui demande si le Gouvernement peut fournir le détail des budgets alloués à chaque ministère en vue de renforcer leurs capacités de protection des systèmes d'informations et quels sont les objectifs spécifiques visés par ces investissements dans les autres ministères en matière de cybersécurité.

Texte de la réponse

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. A ce titre, l'ANSSI coordonne l'ensemble de la gouvernance de l'Etat en matière de lutte informatique défensive et de politique publique de cybersécurité. Dans ce cadre, elle assure un service de veille, de détection, d'alerte et de réponse aux attaques informatiques constituant une menace pour la sécurité nationale. Les dispositions législatives adoptées dans la loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, traitant de la sécurité des systèmes d'information, complètent des mesures de la précédente loi de programmation militaire qui avait doté l'ANSSI de nouvelles capacités en matière de lutte contre les cybermenaces portant atteinte à la sécurité nationale. Les articles 64 à 67 de la loi de programmation militaire, codifiés au sein du code de la défense, ont pour objectif de renforcer les capacités d'analyse de la menace et de détection des attaques informatiques. Leur mise en œuvre permettra d'améliorer la connaissance des modes opératoires des cyberattaquants, nécessaire à la détection d'anomalies affectant les systèmes importants pour le fonctionnement de l'Etat et pour la vie courante de nos concitoyens, parmi lesquels ceux des principaux établissements hospitaliers. En effet, l'ANSSI surveille les attaques ciblant les systèmes d'information d'intérêt. Elle assure à cet effet un service de supervision au profit des administrations et organismes propriétaires de ces systèmes d'information. De plus, la loi de programmation autorise désormais l'ANSSI, en cas de menace susceptible de porter atteinte à la sécurité nationale, d'enjoindre à un fournisseur de système de résolution de noms



de domaine de bloquer, suspendre ou rediriger des noms de domaine. Ces mesures viennent compléter les dispositifs de sécurité des systèmes d'information des ministères et organismes. Les principaux centres hospitaliers en bénéficieront. L'élévation du niveau de sécurité des systèmes d'information de l'Etat dépend également du renforcement des capacités propres aux ministères et des moyens financiers qui y sont consentis. Dans le cadre du plan d'investissement France Relance, l'ANSSI a piloté des dispositifs de renforcement de la sécurité des systèmes d'information de l'Etat. Outre l'ambition d'élever substantiellement le niveau de sécurité numérique de l'Etat et des services publics, le volet cybersécurité du plan de relance a permis de donner l'impulsion nécessaire à l'investissement durable des bénéficiaires dans la mise en sécurité de leurs systèmes d'information. Le ministère de la santé en a particulièrement bénéficié. S'agissant de préciser les volumes budgétaires consacrés à la cybersécurité, il est à signaler que le plan Francerelance a investi 176 millions d'euros sur la période 2021-2022. En revanche, il n'est pas possible d'isoler les seules dépenses annuelles de sécurité des systèmes d'information des ministères. En effet, elles sont considérées comme partie intégrante des budgets consacrés aux systèmes d'information et à la transformation numérique des ministères.