ASSEMBLÉE NATIONALE

14ème legislature

Question N° : 33795	De **M. Lionel Tardy** (Union pour un Mouvement Populaire - Haute-Savoie)	**Question écrite**

Ministère interrogé > Défense	**Ministère attributaire** > Défense

Rubrique >télécommunications	**Tête d'analyse** >protection	**Analyse** > données classifiées.

Question publiée au JO le : **23/07/2013**
Réponse publiée au JO le : **08/10/2013** page : **10583**

Texte de la question

M. Lionel Tardy attire l'attention de M. le ministre de la défense sur le scandale provoqué par le programme de surveillance électronique mis en place par le gouvernement des États-unis et connu sous le nom de Prism. Il souhaite savoir si une évaluation a été menée sur l'impact de ce programme pour l'État français et en particulier pour les services dépendants de son ministère. Il souhaite également connaître les initiatives qui ont été prises ou seront prises afin de limiter l'impact négatif de tels programmes, et préserver ainsi les informations classifiées et empêcher l'interception de données intéressant la sécurité nationale.

Texte de la réponse

Le ministère de la défense est responsable de la sécurité et de la protection de ses systèmes d'information et procède à ce titre, en toutes circonstances, à une évaluation des risques préalablement à leur mise en service. S'agissant plus particulièrement des systèmes d'information traitant des données classifiées, la réglementation élaborée par le secrétariat général de la défense et de la sécurité nationale impose l'adoption de mesures de sécurité dont la finalité est de protéger les informations de tout type de menaces et notamment d'une éventuelle tentative de captation d'origine étrangère. Le ministère de la défense conçoit en conséquence ses propres outils de sécurisation, utilisant des mécanismes de cryptographie conçus en liaison avec l'agence nationale de la sécurité des systèmes d'information (ANSSI) et ses principaux partenaires industriels. Ces équipements sont utilisés en métropole et sur les différents théâtres d'opérations extérieurs afin de protéger les communications du ministère ayant pour objet la transmission d'informations classifiées. Le ministre dispose en outre de l'expertise de la direction de la protection et de la sécurité de la défense, dont l'une des missions consiste à contrôler l'application des règles tendant à préserver la confidentialité des données classifiées. Par ailleurs, il est à noter que le ministère de la défense protège également ses réseaux moins sensibles au moyen d'équipements fiables, habituellement validés par l'ANSSI. Enfin, il est rappelé que le Livre blanc sur la défense et la sécurité nationale publié le 29 avril dernier décrit la vulnérabilité croissante de l'État et de la société face à des attaques informatiques de plus en plus dangereuses : tentatives de pénétration de réseaux à des fins d'espionnage, prise de contrôle à distance, paralysie voire risque de destruction d'infrastructures d'importance vitale, de systèmes d'armes et de capacités militaires stratégiques. Dans ce contexte, le projet de loi relatif à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, qui sera prochainement examiné par le Parlement, vise à adapter le droit aux nouveaux défis de la cyberdéfense et à renforcer les moyens mis en oeuvre sous l'autorité du Premier ministre pour assurer la sécurité des systèmes d'information stratégique. Il prévoit de plus un effort marqué dans le développement des capacités de cyberdéfense militaires (mise en place d'un dispositif de cyberdéfense militaire étroitement intégrée aux forces et en relation avec le domaine du renseignement, accroissement des moyens

humains consacrés à la cyberdéfense, important effort financier en faveur des services spécialisés du ministère de la défense).