ASSEMBLÉE NATIONALE

14ème législature

télécommunications

Question écrite n° 48555

Texte de la question

M. Marc Le Fur attire l'attention de M. le ministre de la défense sur les menaces numériques et la nécessité de développer la cyberdéfense. La cybercriminalité est un enjeu majeur pour les administrations, les entreprises et les citoyens, qui sont victimes de cyberattaques quotidiennes. La protection contre ces attaques visant à altérer, détruire ou exfiltrer des données est un véritable impératif. Ces menaces prennent aujourd'hui une nouvelle ampleur et posent de réelles questions en termes de sécurité nationale : tentative de pénétration de réseaux numériques à des fins d'espionnage tentatives de destruction des système d'information de l'État, des grands services publics et des entreprises. C'est pourquoi il lui demande de lui préciser les dispositifs destinés à être mis en oeuvre dans le cadre de la loi de programmation militaire et la politique de sécurité intérieure.

Texte de la réponse

Le chapitre IV de la loi no 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale a pour objet l'adaptation du droit national aux nécessités de la cybersécurité. En son sein, quatre volets peuvent être distingués. Le premier volet a permis de clarifier au sein de l'Etat les compétences en matière de cybersécurité. La loi a fondé en droit la compétence du Premier ministre en matière de définition de la politique nationale de défense et de sécurité des systèmes d'information. Cette disposition a été codifiée à l'article L.2321-1 du code de la défense. A ce titre, le Premier ministre coordonne l'action gouvernementale. Pour ce faire, il dispose de l'agence nationale de sécurité des systèmes d'information (ANSSI), service rattaché au secrétaire général de la défense et de la sécurité nationale. La loi confère à l'ANSSI la qualité d'autorité nationale de défense des systèmes d'information. La loi dote l'Etat du droit de procéder aux opérations techniques nécessaires afin de neutraliser les effets des attaques informatiques affectant gravement le potentiel de guerre, l'économie, la sécurité ou la capacité de survie de la Nation. De plus, l'Etat est autorisé à se doter des moyens nécessaires à l'accomplissement de ces opérations. Le deuxième volet concerne les opérateurs d'importance vitale. Il est apparu nécessaire d'améliorer la sécurité informatique des systèmes critiques de ces opérateurs. La loi confère au Premier ministre le pouvoir de fixer les règles de sécurité nécessaires à la protection des opérateurs d'importance vitale. Elle crée pour ces opérateurs une obligation de signalement des attaques informatiques dont ils sont victimes. L'Etat dispose désormais de la faculté d'intervenir sur les installations attaquées. Le troisième volet porte sur la capacité de l'Etat de prendre des mesures de lutte informatique défensive. Il autorise l'étude des programmes malveillants, dont la détention, l'exposition, l'offre, la location sont par ailleurs interdits, aux fins d'analyse et de recherche, dans le but de permettre la mise en œuvre de contre-mesures. Il permet d'obtenir des opérateurs de communication électronique l'identité des utilisateurs ou détenteurs d'équipements vulnérables, attaqués ou menacés, afin de les alerter. Enfin, le quatrième volet permet d'élargir le contrôle étatique à l'ensemble des équipements susceptibles de permettre des interceptions. De plus, dans son rapport annexé, la loi de programmation militaire a prévu un renforcement significatif des moyens humains et financiers consacrés à la cyberdéfense, au sein des armées, de la direction générale de l'armement et des services spécialisés. Par ailleurs, le Gouvernement a pris en compte la nécessité de soutenir le tissu industriel national

de ce secteur. Un rôle d'animateur de la filière industrielle a été confié à ANSSI. A ce titre, l'agence a conçu le plan « Cybersécurité » lancé le 12 septembre 2013 dans le cadre de la Nouvelle France Industrielle (NFI). Elle en a assuré l'animation, en soutien des acteurs publics et privés de la filière. De même, l'ANSSI est l'interlocuteur étatique des opérateurs d'importance vitale pour l'application des dispositions prévues par la loi de programmation militaire : définition des règles techniques susceptibles de renforcer la sécurité informatique de leurs systèmes d'information les plus sensibles ; mécanisme de déclaration des incidents informatiques ; cadre des contrôles techniques. Le décret no 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense fixe le cadre d'application des dispositions concernées. Les premiers arrêtés sectoriels devraient être publiés à la fin de l'année 2015. Parallèlement, l'ANSSI a préparé de concert avec le ministère de l'intérieur la mise en place d'un dispositif d'assistance aux victimes d'actes de malveillance. Annoncée par le Premier ministre le 18 juin 2015, la mise en place de ce dispositif a été intégrée à la stratégie nationale pour la sécurité du numérique présentée par le Premier ministre le 16 octobre 2015. Ce dispositif devrait voir le jour au cours de l'année 2016.

Données clés

Auteur : M. Marc Le Fur
Circonscription : Côtes-d'Armor (3e circonscription) - Les Républicains
Type de question : Question écrite
Numéro de la question : 48555
Rubrique : Défense
Ministère interrogé : Défense
Ministère attributaire : Premier ministre

Date(s) clée(s)

Question publiée au JO le : 4 février 2014, page 957
Réponse publiée au JO le : 26 janvier 2016, page 728