ASSEMBLÉE NATIONALE

13ème législature

Internet

Question écrite n° 114310

Texte de la question

M. André Wojciechowski attire l'attention de M. le secrétaire d'État auprès du ministre de la défense et des anciens combattants sur le manque de sensibilisation évident en ce qui concerne la sécurité des systèmes informatiques. Lors de son audition par la commission de la défense nationales et des forces armées, le directeur général de l'agence nationale de la sécurité des systèmes informatiques a souligné l'importance de mettre en place un ensemble de règles simples visant à mieux assurer la sécurité informatique. Prenant en considération que les cybermenaces sont en constante augmentation, il semble opportun, comme le font déjà certains pays comme la Suisse, de sensibiliser l'opinion publique sur ce phénomène. Il lui demande s'il n'entend pas mettre en place rapidement, une campagne d'information visant à sensibiliser les acteurs de la vie économique, les entreprises, les administrations et l'ensemble de nos concitoyens afin de prévenir les cybermenaces et inculquer quelques règles de base indispensables à une meilleure gestion d'internet.

Texte de la réponse

Le Gouvernement a pleinement pris la mesure de l'importance du développement d'une stratégie nationale de défense et de sécurité adaptée aux menaces qui pèsent sur les systèmes informatiques français. Le Livre blanc sur la défense et la sécurité nationale, publié en juin 2008, indiquait à ce titre que « dans les 15 ans à venir, la multiplication des tentatives d'attaques menées par des acteurs non étatiques, pirates informatiques, activistes ou organisations criminelles, est une certitude ». Face à ce constat, le Gouvernement a engagé, dès 2009, un renfort significatif des capacités nationales en matière de cyberdéfense par la création : - de l'agence nationale de la sécurité des systèmes d'information (ANSSI), comme autorité nationale en matière de cyberdéfense ; - d'observatoires zonaux de la sécurité des systèmes d'information (OzSSI) dans chacune des sept zones de défense métropolitaines. L'ANSSI, service à compétence nationale rattaché au secrétariat général de la défense et de la sécurité nationalle (SGDSN), a pour mission d'organiser la réponse et de décider des premières mesures urgentes à mettre en oeuvre en cas d'attaque informatique majeure contre la Nation, notamment au sein des administrations et des opérateurs de communications électroniques. Les OzSSI, observatoires créés sous l'égide de la direction de la planification de sécurité nationale du ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration, animent un réseau d'entraide et de partage des bonnes pratiques en matière de sécurité des systèmes informatiques. Ils contribuent à relayer l'action de l'État depuis l'échelon central, l'ANSSI, vers l'ensemble des acteurs locaux concernés (services déconcentrés de l'État, collectivités territoriales, organismes chargés d'une mission de service public, PME, opérateurs privés...) en s'assurant de la bonne utilisation des aides et des moyens mis à leur disposition. En janvier 2011, l'ANSSI a rendu publique la Stratégie française de cyberdéfense. Ce document développe quatre objectifs stratégiques permettant à tous les citoyens de comprendre les enjeux et la portée de l'action gouvernementale dans la réalisation des ambitions du Livre blanc : - faire de la France une puissance mondiale de cyberdéfense et appartenir au premier cercle des nations majeures dans ce domaine, tout en conservant son autonomie ; - garantir la liberté de décision de la France par la protection de l'information de souveraineté. Cet objectif vise à assurer la confidentialité des échanges informatiques entre les autorités gouvernementales à l'aide d'outils dédiés (tels les chiffreurs

informatiques) ; - renforcer la cybersécurité des infrastructures vitales nationales afin de contrer les attaques visant à entraîner des conséquences humaines ou économiques graves ; - assurer la sécurité du cyberespace en sensibilisant les entreprises et les particuliers à la notion d'« hygiène informatique » par l'adoption de bonnes pratiques adaptées à l'usage quotidien des outils informatiques. Afin de répondre à ces objectifs, le Gouvernement a décidé, dès le mois de mai 2011, de mettre en oeuvre un plan interministériel de cybersécurité visant à coordonner les capacités de protection des systèmes d'information de chaque ministère. Cette homogénéisation technique a été confiée à l'ANSSI. Parallèlement, le Gouvernement va créer un groupe d'intervention rapide destiné à traiter, dans les meilleurs délais, les attaques informatiques les plus graves. Il permettra de soutenir les organismes publics et les opérateurs les plus sensibles (tels que les sociétés de transport ou les hôpitaux) dès lors qu'ils auront été l'objet d'une attaque informatique susceptible de présenter un danger pour la sécurité de leur activité, de menacer l'intégrité de leur patrimoine informationnel, de déséquilibrer le fonctionnement économique du pays, ou de porter atteinte à la vie quotidienne des Français. A l'heure actuelle, dans l'hypothèse d'une attaque informatique de grande ampleur, des mesures de sécurité des systèmes d'information sont intégrées au plan Vigipirate. Ce volet informatique du plan se traduit par une surveillance accrue des réseaux. Un plan de réaction aux cyberattaques a également été élaboré : il s'agit du plan Piranet, auquel participent tous les acteurs concernés par la cybersécurité. En 2010, le SGDSN et l'ANSSI ont organisé un premier exercice pour tester ce plan d'action et évaluer les répercussions d'une cyberattaque sur la société, les PME et l'État. Concernant les actions spécifiquement menées par le ministère de la défense et des anciens combattants, outre sa participation au fonctionnement des OzSSI, le ministère accompagne les entreprises nationales de l'industrie de défense et d'armement dans leur protection contre les menaces informatiques. De plus, il impose dans les contrats qu'il passe, notamment par la direction générale de l'armement, des exigences qui contribuent à renforcer la résilience des industriels contre ces menaces. Par ailleurs, le ministère sensibilise tous ses personnels à la sécurité des systèmes d'information et insère dans ses formations, y compris celles ouvertes au monde civil comme l'institut des hautes études de la défense nationale (IHEDN), des séances consacrées à la cyberdéfense. Enfin, concernant les sanctions prononcées à l'encontre des cybercriminels, le ministère de la défense et des anciens combattants n'a plus autorité dans le traitement judiciaire des délits depuis la réorganisation des forces de l'ordre qui a placé, le 1er janvier 2009, la gendarmerie nationale sous la tutelle du ministère de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration.

Données clés

Auteur : M. André Wojciechowski
Circonscription : Moselle (7e circonscription) - Union pour un Mouvement Populaire
Type de question : Question écrite
Numéro de la question : 114310
Rubrique : Télécommunications
Ministère interrogé : Défense et anciens combattants (secrétariat d'État)
Ministère attributaire : Défense et anciens combattants

Date(s) clée(s)

Question publiée le : 12 juillet 2011, page 7510
Réponse publiée le : 21 février 2012, page 1560