



ASSEMBLÉE NATIONALE

14ème législature

Internet

Question écrite n° 61515

Texte de la question

M. Arnaud Robinet attire l'attention de Mme la secrétaire d'État, auprès du ministre de l'économie, du redressement productif et du numérique, chargée du numérique, sur la multiplication des cyberattaques sur le territoire français. On estime en effet à 150 000 le nombre de virus en circulation dans le cyberspace et à 148 000 le nombre d'ordinateurs dont la sécurité est compromise chaque jour. La Commission européenne avait annoncé un plan de cybersécurité au niveau communautaire pour protéger l'Internet ouvert et les libertés en ligne, le 7 février 2013. Ce plan établit cinq objectifs : augmenter la cyberrésilience ; lutter contre la cybercriminalité ; développer une politique et des moyens de cyberdéfense ; développer les ressources industrielles et technologiques en matière de cybersécurité ; instaurer une politique internationale cohérente de l'Union européenne en matière de cybersécurité. Il s'agit plus largement de favoriser la croissance économique en renforçant la confiance du public dans le commerce électronique et l'utilisation d'Internet. Cette stratégie globale devait être relayée au niveau national, chaque État membre devant disposer désormais d'une stratégie nationale, d'une autorité compétente, d'un *Computer Emergency Response Team* (CERT) et d'un plan de coopération national pour définir les rôles et responsabilités en cas d'incident. Ce plan prévoyait également l'instauration d'un mécanisme de coopération entre les États membres et la Commission pour diffuser des messages d'alerte rapides sur les risques et incidents « au moyen d'une infrastructure sécurisée, pour collaborer et organiser des examens par les pairs ». Il lui demande ainsi de bien vouloir lui préciser les moyens de mise en action de cette stratégie européenne sur le plan national.

Texte de la réponse

Service du Premier ministre à compétence nationale rattaché au secrétaire général de la défense et de la sécurité nationale, l'agence nationale de la sécurité des systèmes d'information (ANSSI) assure depuis 2009 la mission de sécurité des systèmes d'information et, à ce titre, celle de défense de ces systèmes. Autorité nationale en matière de sécurité des systèmes d'information, l'ANSSI a une mission de protection qui comporte plusieurs aspects : la sensibilisation des différents publics aux menaces présentes dans le cyberspace et aux moyens de s'en protéger, et la prévention contre les cyberattaques pour garantir effectivement la sécurité des systèmes d'information des administrations et des opérateurs essentiels au bon fonctionnement de la Nation. Autorité de défense des systèmes d'information, l'ANSSI a une mission de réaction aux attaques et d'appui à la reprise de l'activité normale des systèmes d'information. Elle est chargée, sous l'autorité du Premier ministre, de piloter la réponse de l'État en cas d'attaques informatiques et d'assurer la défense des systèmes de l'État et des entreprises nécessaires au bon fonctionnement de la Nation. Depuis 2012, le Gouvernement soutient le développement de l'ANSSI pour l'accomplissement de ses missions dont le caractère essentiel a été souligné dans le Livre blanc sur la défense et la sécurité nationale publié en avril 2013. Les attaques informatiques sont désormais considérées comme une des menaces majeures auxquelles notre pays doit faire face. En 2014, l'ANSSI a engagé un travail interministériel d'élaboration d'une nouvelle stratégie nationale de cybersécurité. Le Premier ministre a présenté le 16 octobre la « stratégie nationale pour la sécurité du numérique » qui sera déclinée au sein de chaque département ministériel. Compte tenu des enjeux liés à la cybersécurité, le

gouvernement a veillé au renforcement de l'ANSSI. L'agence, qui comptait une centaine d'agents lors de sa création en 2009, sera ainsi forte de 600 agents à l'horizon 2017. A côté d'autres départements ministériels, le ministère de l'intérieur travaille en lien étroit avec l'ANSSI, tant lors du traitement des attaques informatiques, notamment celles concernant les opérateurs d'importance vitale, que dans le domaine de la prévention. Dans ce cadre et selon son mandat, la direction générale de la sécurité intérieure (DGSi) recueille du renseignement, participe à l'évaluation de la menace et à l'identification de ses acteurs. Saisie des enquêtes judiciaires relatives aux attaques informatiques visant les opérateurs d'importance vitale ou les administrations, la DGSi a également un rôle de prévention des risques potentiels, ainsi qu'une mission de sensibilisation aux risques numériques auprès des organismes publics et privés. Au ministère de l'intérieur, une sous-direction de la lutte contre la cybercriminalité a été créée au sein de la direction centrale de la police judiciaire (DCPJ) et un préfet chargé de la lutte contre les cybermenaces a été désigné afin de coordonner l'action du ministère en matière de lutte contre la cybercriminalité. En 2015, le ministère de l'intérieur et l'ANSSI ont engagé une réflexion sur les missions du dispositif d'assistance aux victimes d'actes de cybermalveillance annoncé dans la stratégie numérique du Gouvernement.

Données clés

Auteur : [M. Arnaud Robinet](#)

Circonscription : Marne (1^{re} circonscription) - Les Républicains

Type de question : Question écrite

Numéro de la question : 61515

Rubrique : Télécommunications

Ministère interrogé : Numérique

Ministère attributaire : Premier ministre

Date(s) clé(s)

Question publiée au JO le : [22 juillet 2014](#), page 6150

Réponse publiée au JO le : [17 novembre 2015](#), page 8302