# ASSEMBLÉE NATIONALE

13ème législature

## Internet

Question écrite n° 96133

### Texte de la question

M. Jean-Claude Fruteau attire l'attention de M. le ministre d'État, ministre de la défense et des anciens combattants, sur les risques, pour la sécurité nationale, de la multiplication des « cyberattaques » contre les sites Internet de l'ensemble des institutions publiques en général et contre les réseaux sensibles de la défense nationale en particulier. Depuis quelques années, les attaques menées sur Internet ne se résument plus seulement à des actes crapuleux (fraudes à la carte bancaire, « *phishing* »...). Elles menacent directement la sécurité des États : en 2007 en Estonie, et en 2008 en Géorgie, les sites Internet des principales institutions publiques avaient été piratés lors de périodes de grande tension. Plus récemment, en 2009, un réseau informatique a lancé une attaque, de manière concertée, contre les systèmes informatiques de gouvernements et d'organisations privées dans 103 pays dans l'objectif d'extraire des documents hautement sensibles. Au-delà du vol de données, ces attaques peuvent avoir pour objet la paralysie des systèmes de communications dans le but de provoquer une déstabilisation économique. Selon le forum économique mondial, une panne majeure des infrastructures d'information (réseaux téléphoniques, fibre optique, réseaux d'ordinateurs...) pourrait avoir un coût global de 250 milliards de dollars. La probabilité d'une telle panne dans les dix ans serait de 10 % à 20 %. Face aux enjeux en présence, il souhaite connaître les moyens mis en oeuvre pour, d'une part, lutter contre ce phénomène et, d'autre part, protéger les réseaux et les informations sensibles de la défense nationale.

### Texte de la réponse

La montée en puissance des menaces informatiques est très préoccupante dans la mesure où elle représente un sérieux danger pour l'ensemble des systèmes d'information, tant publics que privés. Le Livre blanc sur la défense et la sécurité nationale a d'ailleurs parfaitement identifié cette menace en faisant de la lutte contre les attaques informatiques une priorité majeure des dispositifs de sécurité nationale. Conformément aux orientations définies par le Livre blanc, une Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n° 2009-834 du 7 juillet 2009 pour permettre à la France de se doter d'une véritable capacité de défense de ses systèmes d'information. Relevant du Premier ministre et placée sous la tutelle du secrétaire général de la défense et de la sécurité nationale, l'ANSSI a notamment pour missions : de détecter les attaques informatiques et de réagir rapidement, grâce à un centre opérationnel renforcé de cyberdéfense, chargé de la surveillance permanente des réseaux les plus sensibles de l'administration et de la mise en oeuvre de mécanismes de défense adaptés ; de prévenir la menace en contribuant au développement d'une offre de produits et de services de confiance pour les administrations et les acteurs économiques ; de jouer un rôle permanent de conseil et de soutien aux administrations et aux opérateurs d'importance vitale ; d'informer régulièrement les entreprises et le grand public sur les menaces et les moyens de s'en protéger, en développant une politique de communication et de sensibilisation active ; d'entretenir des liens étroits avec ses homologues étrangers, une coopération internationale étant indispensable compte tenu de l'absence de frontières dans l'espace numérique. Pour décliner sur l'ensemble du territoire national les mesures destinées à améliorer la sécurité des systèmes d'information (SSI), le Livre blanc a prévu la création d'un observatoire zonal de la sécurité des systèmes d'information (OZSSI) au sein de chaque zone de défense. Placés sous l'autorité des

préfets de zone, ces observatoires sont notamment chargés d'une mission de soutien en formation et en conseil aux administrations locales, d'animation d'un réseau largement ouvert à l'ensemble des acteurs concernés (échelons déconcentrés de l'État, collectivités territoriales, organismes ayant une mission de service public, entreprises et opérateurs privés...) et de remontée des signaux précurseurs d'incidents. Le ministère de la défense et des anciens combattants gère un nombre considérable de systèmes d'information couvrant trois domaines : les systèmes d'information opérationnels et de communication liés à l'emploi des forces, les systèmes d'information scientifiques et techniques, et les systèmes d'information, d'administration et de gestion. La direction générale des systèmes d'information et de communication (DGSIC) du ministère de la défense et des anciens combattants, créée en mai 2006, assure le pilotage central de l'ensemble de ces systèmes, pour lesquels elle définit une politique commune. Elle définit notamment les orientations générales en matière de sécurité des systèmes et en contrôle l'application. La protection contre les attaques informatiques au sein du ministère de la défense et des anciens combattants repose sur une cyberdéfense active alliant prévention et réaction. S'agissant des mesures de prévention sur les réseaux et les informations sensibles de la défense nationale, le ministère applique une séparation stricte entre les réseaux publics et les réseaux classifiés. Par ailleurs, le ministère a opté pour un décloisonnement maîtrisé de ses réseaux internes et l'interconnexion des réseaux non classifiés avec l'Internet est assurée par des points d'accès surveillés, sécurisés, contrôlés et dotés de filtres particuliers. La prévention s'inscrit également dans la conception des systèmes puis dans leur exploitation. Ainsi, dès la phase projet, la sécurité est intégrée dans l'architecture des systèmes dont le niveau de sécurité est formellement validé puis se prolonge lors de leur mise en exploitation par : la sensibilisation des agents du ministère de la défense et des anciens combattants sur la vulnérabilité du réseau Internet et l'interdiction de tout échange ou traitement d'information sensible par le réseau Internet ; l'installation des correctifs de sécurité sur les systèmes d'exploitation et les suites logicielles de bureautique, et la mise à jour des logiciels de protection : antivirus, antispam, pare-feu, etc. ; la surveillance et l'analyse en temps réel, par les administrateurs des systèmes d'information, des anomalies relevées par les dispositifs de sécurité informatique et, a posteriori, par l'examen des journaux d'événements. Pour autant, face à la multiplication des attaques de toute nature et à l'interconnexion croissante des réseaux, ces mesures, dites « statiques », sont complétées par un dispositif de défense active et dans la profondeur des réseaux, en voie d'amélioration. À ce titre, le ministère a engagé une importante réorganisation de ses infrastructures de communication et d'hébergement des applications, ainsi que de son schéma de gestion de crise informatique, en cohérence avec l'organisation interministérielle générale mise en place par l'ANSSI. Plusieurs opérations majeures telles que la rénovation des infrastructures de transport, la rationalisation des serveurs et la réduction du parc des applications concourent à cette réorganisation. En matière de ressources humaines, le ministère de la défense et des anciens combattants veille par ailleurs avec une particulière attention à conforter et à développer les compétences permettant de prévenir et de parer les nouveaux risques et menaces. En termes d'organisation, une instruction ministérielle du 30 novembre 2008 portant code de bon usage des systèmes d'information et de communication du ministère de la défense précise l'utilisation attendue par le ministère de ses systèmes d'information, les dispositions spécifiques à l'usage de certains médias, les attributions particulières des acteurs de la SSI et les moyens de contrôle mis en oeuvre. Par ailleurs, les agents du ministère de la défense et des anciens combattants sont périodiquement sensibilisés aux risques informatiques par la mise en ligne d'informations pertinentes sur l'Intranet du ministère et dans le cadre de séances de formation dispensées par les officiers de sécurité des systèmes d'information des organismes de la défense. Ces mesures de prévention sont évaluées régulièrement au travers d'audits, de contrôles et d'inspections menés par des équipes spécialisées du ministère de la défense et des anciens combattants. Pour ce qui concerne les mesures permettant d'agir en réaction à une éventuelle attaque, l'instruction ministérielle du 26 septembre 2008 relative à la mise en oeuvre de la lutte informatique défensive au sein du ministère de la défense a mis en place une organisation permanente de veille, alerte et réponse (OPVAR). Disposant d'une connaissance et d'une vision de l'ensemble des réseaux, l'OPVAR a pour mission de prévenir et d'anticiper les crises et de détecter les activités hostiles (veille), d'analyser, de hiérarchiser et de notifier tout événement présentant un risque (alerte), ainsi que de déterminer et de conduire les actions défensives correspondantes (réponse). Ces processus de détection et de gestion des incidents s'appuient sur : un centre d'analyse de lutte informatique défensive (CALID), qui assure la fonction de veille et réalise le volet technique des fonctions d'analyse et de réponse ; un centre opérationnel, qui décide des réponses appropriées en fonction des éléments techniques fournis par le CALID et des priorités liées aux missions. L'OPVAR entretient des liens étroits avec le centre opérationnel de l'ANSSI, ainsi que sur le plan

international avec son entité homologue de l'Organisation du traité de l'Atlantique nord (OTAN).

## Données clés

**Auteur :** M. Jean-Claude Fruteau
**Circonscription :** Réunion (5e circonscription) - Socialiste, radical, citoyen et divers gauche
**Type de question :** Question écrite
**Numéro de la question :** 96133
**Rubrique :** Télécommunications
**Ministère interrogé :** Défense et anciens combattants
**Ministère attributaire :** Défense et anciens combattants

## Date(s) clée(s)

**Question publiée le :** 14 décembre 2010, page 13434
**Réponse publiée le :** 8 mars 2011, page 2274