ASSEMBLÉE NATIONALE

14ème législature

terrorisme

Question écrite n° 78011

Texte de la question

M. Jacques Cresta attire l'attention de M. le ministre de l'intérieur sur la cyber attaque terroriste dont a été victime le groupe TV5 Monde le mercredi 8 avril à 22 heures. Cette attaque informatique est l'œuvre du groupe CyberCalifat qui avait pour ambition d'utiliser les canaux de ce média pour promouvoir au travers de films son idéologie. Ce n'est pas leur première attaque cyber terroriste, puisque le centre de contrôle de l'armée américaine et Newsweek avaient déjà fait l'objet d'attaque ces derniers mois. Mais cette fois l'attaque est exceptionnelle tant par son importance, sa complexité que par son symbole. Son symbole car TV5 Monde est la chaîne francophone diffusée partout dans le monde, elle est la voix internationale de la culture française. Son importance et sa complexité puisque l'on pensait que ce type d'attaque ne pouvait être que le seul fait d'un État et pas d'un groupe terroriste car cela nécessite des moyens humains, techniques et technologiques importants. Une nouvelle fois après les attentats de janvier 2015 ce sont les symboles de notre République, la liberté d'expression, qui sont attaqués par les extrémistes. Le président de la République a annoncé 200 postes supplémentaires pour nos services de renseignement, afin de renforcer notre cyberdéfense. Le projet de loi sur le renseignement donnera à nos services plus de moyens d'actions, dans le respect de la liberté des Français. Il souhaite connaître les mesures que comptent prendre le Gouvernement pour identifier les auteurs de cette cyberattaque et éviter que de telles attaques ne se reproduisent.

Texte de la réponse

TV5 MONDE a subi le 8 avril 2015 une attaque informatique sans précédent sur un groupe de médias français. Le secrétaire général de la défense et de la sécurité nationale a été alerté par la victime le soir-même et a dépêché sur place, le lendemain matin, une équipe de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), agence qui lui est rattachée. Alors que l'ANSSI intervient en général auprès d'administrations sensibles ou d'opérateurs d'importance vitale qui n'ont pas vocation à communiquer largement et ne souhaitent pas se présenter comme vulnérables, l'exposition naturelle de la victime a conduit à une médiatisation très rapide de l'affaire et le SGDSN a publié dans la matinée un communiqué de presse. Dans le même temps, les équipes techniques de la chaîne et de l'ANSSI ont conduit les premières analyses en préservant les traces, les enregistrements et toutes les données dont l'exploitation pourrait permettre de comprendre le mode opératoire de ce piratage. Les attaquants ont pris simultanément le contrôle de la diffusion de la chaîne, de ses comptes twitter et facebook, de son site Internet et de son réseau interne. Outre les effets visibles par le grand public, l'attaque a touché certains équipements majeurs du réseau (effacement du microcode d'équipements, opération qui s'apparente à une destruction logique) et l'ensemble du réseau interne était contrôlé par les attaquants. Il s'agit du premier cas rendu public de cybersabotage sur le sol français. Si les attaquants n'ont visé qu'une partie des machines du réseau interne à la chaîne, ils avaient mis en place, au sein même de ce réseau, des moyens leur permettant de le détruire intégralement. L'importance de l'affaire a donné lieu à une réunion de ministres le 9 avril en présence des directeurs de grands groupes de médias nationaux et à plusieurs interventions officielles dans la presse condamnant l'agression. Grâce aux données recueillies, l'ANSSI a pu élaborer des recommandations particulières, adaptées au monde des médias, et les a diffusées

aux professionnels du secteur. Dès le dépôt d'une plainte, une enquête a été entamée par le ministère de l'intérieur afin d'identifier les coupables. Cette enquête est encore en cours. Dans les mois qui ont précédé, l'ANSSI était intervenue dans plusieurs affaires de cyberattaques contre des médias. En janvier, après les attentats, LE MONDE a été victime de hameçonnage et des messages haineux ont été publiés depuis son compte Twitter officiel. Des attaques sporadiques ont visé à saturer son accès à Internet. Sollicitée, l'ANSSI a apporté son expertise et renouvelé les recommandations générales qu'elle avait adressées de façon préventive à ses contacts dans les groupes de médias au lendemain des attentats. Le 20 janvier, FRANCE 3 REGIONS et 1ERE OUTRE-MER ont été piratées. Le lendemain, des sites Internet de FRANCE 3 REGIONS ont été défigurés. Des données ont été exfiltrées et publiées sur Internet. L'ANSSI est intervenue sur place et FRANCE TELEVISIONS a mis à jour son système de publication. Avec le développement de la cybermenace, l'ANSSI intervient dans un cadre élargi. Une posture nationale ambitieuse de cybersécurité et de cyberdéfense, fixée dans un comité de pilotage placé sous l'autorité de la Présidence de la République, avait été traduite en une stratégie nationale publiée en 2011. Point focal de l'organisation de l'Etat dans le domaine, l'ANSSI se consacrait alors essentiellement à la protection des systèmes d'information des administrations sensibles. Avec le livre blanc sur la défense et la sécurité nationale et les dispositions de l'article 22 de la loi de programmation militaire du 18 décembre 2013, le périmètre de responsabilité de l'ANSSI s'est étendu aux opérateurs d'importance vitale. La question du champ d'intervention de l'ANSSI se pose à nouveau alors que des acteurs essentiels au fonctionnement de la démocratie, sans pourtant avoir la qualité d'opérateurs d'importance vitale, sont pris pour cible par des cyberattaquants. Plus généralement, de nombreux industriels, dont le poids économique, l'empreinte sociale ou l'excellence en matière d'innovation font des acteurs majeurs de la croissance française, sans pour autant être qualifiés d'importance vitale, sont soumis à un pillage informatique méthodique. L'Etat ne peut pas être absent de ces domaines essentiels qui comprennent, au-delà des administrations elles-mêmes et des opérateurs d'importance vitale, les plateformes nécessaires au débat démocratique et pluraliste ainsi que les acteurs économiques essentiels à la compétitivité et à la croissance. Le Premier ministre a présenté le 16 octobre 2015 la nouvelle « stratégie nationale pour la sécurité du numérique », issue d'un travail interministériel, qui fixe cinq objectifs stratégiques relatifs à la défense des intérêts fondamentaux de la France et au traitement de crise informatique majeure, à la confiance numérique et à la protection des données des Français, à la sensibilisation et à la formation, à l'environnement des entreprises du numérique, à la souveraineté numérique européenne et à la stabilité du cyberespace.

Données clés

Auteur : M. Jacques Cresta
Circonscription : Pyrénées-Orientales (1re circonscription) - Socialiste, écologiste et républicain
Type de question : Question écrite
Numéro de la question : 78011
Rubrique : Ordre public
Ministère interrogé : Intérieur
Ministère attributaire : Premier ministre

Date(s) clée(s)

Question publiée au JO le : 14 avril 2015, page 2799
Réponse publiée au JO le : 23 février 2016, page 1562