ASSEMBLÉE NATIONALE

14ème législature

Internet

Question écrite n° 35998

Texte de la question

Mme Geneviève Gaillard attire l'attention de M. le ministre de l'intérieur sur la recrudescence massive de la cybercriminalité d'implantation ivoirienne ciblant nos concitoyens. Elle souligne que nul ne semble à l'abri de ces tentatives d'escroqueries et mentionne que les adresses électroniques de l'assemblée nationale en font régulièrement l'objet, ce qui témoigne de la généralisation et du sentiment d'impunité total de ces délinquants, qui n'hésitent pas pour mener à bien leurs arnaques à contrefaire des entêtes des autorités françaises, administrations fiscales, organismes consulaires. Ces escrocs que l'on appelle communément « brouteurs » en Côte d'Ivoire maîtrisent bien les outils informatique, sont spécialistes de la retouche d'images et utilisent également des flux-vidéos préenregistrés sur leur webcam. La liste des méfaits est grande : arnaques aux sentiments, les escrocs créent de faux comptes sur des sites de rencontre, l'hameçonnage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. Les victimes sont destinataires d'un email d'un de leurs contacts réels leur apprenant qu'il est en voyage d'affaire à Abidjan et qu'il s'est fait agressé sur la route de l'aéroport se faisant voler tous ses papiers, ou qu'il a eu un accident de voiture et se trouve à l'hôpital sur le point de se faire opérer, et qu'il a besoin d'argent d'urgence par mandat. Les arnaques « à l'héritage », les escrocs diffusent un message électronique proposant de mirobolantes commissions, en échange de l'utilisation d'un compte bancaire pour effectuer des virements d'un montant très élevé. L'objectif des escrocs consiste soit à obtenir le numéro de comptes bancaires et un exemplaire de la signature de leur titulaire pour donner de faux ordres de virement à leur banque, soit à leur faire payer de prétendus « frais de dossier » préalables, qui se succèderont alors en cascade. Les arnaques à la loterie, ici les escrocs diffusent des messages électroniques avisant que leur cible a gagné le gros lot d'une loterie, généralement par tirage au sort parmi des adresses électroniques. L'objectif consiste soit à demander le paiement de frais de dossier et de transport des gains vers la France, soit à faire venir » l'heureux gagnant » pour retirer son gain à Abidjan et à lui voler tout ce qu'il a emporté à son arrivée en Côte d'Ivoire. Elle veut encore citer les arnaques à la commande de matériel et promesse de paiement par carte de crédit ou virement bancaire, les détournements de courrier à destination des banques, les arnaques à la voiture d'occasion sur site de vente entre particuliers, les arnaques au dédommagement des victimes d'abus de confiance, la liste n'étant encore pas exhaustive. Le comble étant consommé quand certains fraudeurs après avoir escroqué une première fois leur victime n'hésitent pas à se faire passer pour un organisme de lutte contre la cybercriminalité dans le but d'arnaquer leur victime une deuxième fois ! Elle dénonce une situation devenue insupportable et qui semble laisser nos concitoyens à leur propre sort, sans que l'État déploie les moyens à la hauteur de l'intensité atteinte par cette criminalité impunie. À l'heure actuelle, une plateforme de lutte contre la cybercriminalité existe en Côte d'Ivoire, elle souhaite connaître le niveau de collaboration avec le cyber police française, et souhaite être informée sur les effectifs et moyens de notre cyber police, et enfin savoir quelles mesures urgentes et efficaces le Gouvernement compte prendre pour protéger la population de cette cybercriminalité ivoirienne et pour accompagner les victimes de ces escroqueries.

Texte de la réponse

La sécurité de l'espace numérique constitue pour la société (acteurs économiques, particuliers...) et pour l'Etat un enjeu majeur alors que le développement d'Internet et des systèmes d'information offre de nouvelles occasions à une criminalité, souvent internationale, qui sait tirer profit des structures de l'environnement numérique (anonymisation, etc.). Comme d'autres acteurs publics et privés, les forces de sécurité de l'Etat consacrent d'importants moyens, humains et techniques, à la lutte contre la cybercriminalité sous toutes ses formes. Au sein du ministère de l'intérieur, cette mission incombe à titre principal à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de la direction centrale de la police judiciaire. Composé de policiers et de gendarmes, cet office central anime et coordonne l'action des services centraux et territoriaux de la police judiciaire, conduit des actes d'enquête et des travaux techniques d'investigation en appui de nombreux services, aussi bien de police et de gendarmerie que d'autres administrations (direction générale des douanes et droits indirects, etc.). La collaboration est particulièrement développée avec la gendarmerie nationale, dont le service technique de recherches judiciaires et de documentation est doté d'une division de lutte contre la cybercriminalité. La gendarmerie dispose aussi d'une expertise judiciaire avec son département informatique et électronique de l'institut de recherche criminelle de la gendarmerie nationale, à l'instar du service central de l'informatique et des technologies de la sous-direction de la police technique et scientifique de la direction centrale de la police judiciaire. Une plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) a été mise en place en 2009 pour gérer le site www. internet-signalement. gouv. fr, qui offre des conseils de prévention et permet aux internautes et aux professionnels de signaler, de manière simple, tout contenu illicite sur Internet. En 2012, la plate-forme, composée de policiers et de gendarmes et placée au sein de l'OCLCTIC, a reçu près de 120 000 signalements (et plus de 80 000 au premier semestre 2013), dont plusieurs milliers ont été transmis pour enquête aux services répressifs français et à Interpol. Une plate-forme téléphonique d'information et de prévention du public sur toutes les formes d'escroqueries existe également. Appelée « Info escroqueries » et composée de policiers et de gendarmes, elle a reçu plus de 42 000 appels en 2012 (et près de 19 000 appels au premier semestre 2013). L'OCLCTIC dispose aussi d'un groupe d'enquête mixte police-gendarmerie spécialisé dans la répression des principales infractions de cybercriminalité (fraude aux cartes de paiement pour les ventes à distance, fausses annonces, escroqueries à la nigériane, à la fausse loterie...) et notamment dans l'identification des réseaux criminels. L'action de la police et de la gendarmerie nationales s'appuie sur un réseau de plus de 600 enquêteurs spécialisés dans le numérique. Une vigilance particulière s'exerce à l'égard des opérations frauduleuses affectant les transactions par carte de paiement. L'OCLCTIC a renforcé son partenariat avec la fédération bancaire française et le groupement d'intérêt économique des cartes bancaires afin d'améliorer l'échange d'informations opérationnelles et techniques. Sur le plan juridique, la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure a doté les services de sécurité de moyens accrus (captation à distance des données issues de communications électroniques dans la lutte contre la criminalité organisée, création d'une incrimination pénale d'usurpation d'identité sur Internet...). La cybercriminalité étant essentiellement un phénomène transnational, les coopérations bilatérales avec les pays « sources » sont renforcées et la coopération opérationnelle internationale se développe dans le cadre de diverses enceintes européennes et internationales (Union européenne, Conseil de l'Europe, G8, Interpol...). La France est adhérente à la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001. Elle participe au réseau d'alerte G8 dit « 24/7 », qui permet la mise en relation directe des services d'enquête pour répondre aux demandes urgentes de gel de données numériques. L'Union européenne s'est pour sa part dotée en janvier dernier d'un Centre européen de lutte contre la cybercriminalité (EC3), placé auprès d'Europol, qui va renforcer les capacités des Etats membres. Deux autres projets européens sont en cours : un projet de directive sur la sécurité des systèmes d'information et un projet, dit « 2 Centre », qui vise à développer dans les principaux pays de l'Union un réseau de centres d'excellence dédiés à la formation et à la recherche en matière de cybercriminalité. Sur le plan de la coopération bilatérale avec les pays « sources », l'OCLCTIC participe depuis plusieurs années à des actions de formation au bénéfice de pays d'Afrique francophone (Sénégal, Côte d'Ivoire, Bénin, Togo, Burkina Faso), d'où sont commises la plupart des escroqueries sur Internet. Consciente des enjeux liés à la cybercriminalité, la Côte d'Ivoire a renforcé sa législation et mis en place une direction de l'informatique et des traces technologiques qui comprend, outre des services spécialisés chargés des infrastructures de télécommunications et pouvant apporter une assistance technique aux services répressifs et à la justice, une plate-forme de lutte contre la cybercriminalité qui gère les signalements transmis par les victimes, ivoiriennes ou étrangères, par exemple françaises. Cette plate-forme dispose d'un profil Facebook accessible à

tous et diffusant des conseils et des avis de recherche d'escrocs identifiés. En avril 2013, l'OCLCTIC a dispensé une formation spécialisée au profit de 18 enquêteurs ivoiriens. La coopération avec les Etats francophones d'Afrique devrait se poursuivre en 2014 avec le projet développé par le sous-groupe « High Tech Crime » du G8, qui gère les points de contact « 24/7 ». Il s'agit de dispenser une formation à destination de ces pays pour les aider à créer un point de contact ou à optimiser le fonctionnement de celui dont ils disposent déjà. Par ailleurs, le Gouvernement a engagé une adaptation du dispositif de lutte contre la cybercriminalité, qui passe notamment par une connaissance accrue du phénomène. A la suite du séminaire gouvernemental sur le numérique du 28 février dernier, il a été décidé de mettre en place un groupe de travail interministériel (Justice/Economie et Finances/ Intérieur/ Economie numérique) chargé d'élaborer une stratégie globale de lutte contre la cybercriminalité, prenant en compte la dimension internationale et européenne du phénomène, et portant notamment sur le développement des dispositifs d'aide aux victimes et de sensibilisation des publics. Ce groupe de travail a commencé à se réunir en juillet 2013 et devrait rendre son rapport d'ici à la fin de l'année.

Données clés

Auteur : Mme Geneviève Gaillard
Circonscription : Deux-Sèvres (1re circonscription) - Socialiste, écologiste et républicain
Type de question : Question écrite
Numéro de la question : 35998
Rubrique : Télécommunications
Ministère interrogé : Intérieur
Ministère attributaire : Intérieur

Date(s) clée(s)

Question publiée au JO le : 13 août 2013, page 8604
Réponse publiée au JO le : 19 novembre 2013, page 12119