



ASSEMBLÉE NATIONALE

12ème législature

Internet

Question écrite n° 74690

Texte de la question

M. Christian Vanneste souhaite attirer l'attention de M. le ministre d'État, ministre de l'intérieur et de l'aménagement du territoire, sur la lutte contre la cybercriminalité. En 1994, a été créée la brigade centrale de la répression de la cybercriminalité. En 2000, le ministère de l'intérieur a mis en place l'Office central de lutte contre la cybercriminalité liée aux technologies de l'information et de la communication (OCLCTIC). Le CLUSIF (Club de la sécurité des systèmes d'informations français) fait état d'une très forte augmentation des délits commis à seule fin d'enrichissement personnel en 2004. Il souhaiterait donc savoir quels sont les chiffres officiels que détient le ministère sur ces délits et quelles mesures sont mises en oeuvre par l'OCLCTIC afin de lutter contre la cybercriminalité.

Texte de la réponse

L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) centralise toutes les informations sur les infractions entrant dans son domaine de compétence et dispose ainsi d'un état de cette délinquance. Un important travail a par ailleurs été engagé afin de permettre dès 2006 une amélioration de l'enregistrement statistique de la cybercriminalité en favorisant l'enrichissement de la base nationale du système de traitement des infractions constatées. Plusieurs tendances se dessinent : d'une part, l'espace virtuel devient un nouveau territoire pour la criminalité organisée qui utilise parfaitement toutes les caractéristiques de l'environnement numérique (extraterritorialité, garanties renforcées de l'anonymat, manque d'harmonisation des législations,...). D'autre part, les délinquants s'attaquent aux TIC (intrusion dans les systèmes de traitement automatisés de données STAD - entrave, altération, destruction de données dans un STAD, diffusion de programmes informatiques permettant la fabrication de fausses cartes de paiement de type « yescard ») et utilisent les systèmes informatiques pour commettre des infractions « classiques ». C'est ainsi que l'escroquerie par utilisation de faux numéros de carte bancaire et la diffusion d'images pornographiques mettant en scène des mineurs génèrent également d'importants profits. Au cours de l'année 2004, les services de police et les unités de gendarmerie ont relevé 672 infractions liées aux TIC contre 1 224 en 2003, soit une baisse de 45 %. Cette forte diminution est due principalement à la chute des infractions relatives à la diffusion de programmes informatiques permettant la fabrication de fausses cartes de paiement type « yescard » (- 92 %, soit 64 faits en 2004 contre 792 en 2003). Toutefois, les autres infractions relatives aux TIC sont en augmentation : 285 faits en 2004 contre 254 en 2003 pour les atteintes aux STAD, les contrefaçons de logiciels et autres atteintes au code de la propriété intellectuelle enregistrent 268 faits en 2004 contre 139 faits en 2003 et les atteintes aux droits de la personne 54 faits en 2004 au lieu de 37 en 2003. Au cours de l'année 2004, les différents services de la police et de la gendarmerie nationales ont recensé une baisse de 26 % des infractions commises en utilisant les systèmes informatiques. Les escroqueries diverses par l'utilisation frauduleuse de numéros de cartes bancaires ont ainsi régressé de 93,71 %, soit 342 faits en 2004 contre 5 444 en 2003. En revanche, les escroqueries commises pour l'achat de biens ou de services ont vu leur nombre augmenter (+ 23,20 %, soit 6 287 faits en 2004 contre 5 103 en 2003), ainsi que les escroqueries commises pour la recharge de crédits dans le domaine de la téléphonie mobile (+ 10,44 %, soit 1 841 faits en 2004 contre 1 667 faits en

2003). À l'exception de ces deux dernières catégories, la forte diminution d'ensemble des infractions directement liées aux TIC ou dont la commission est facilitée ou liée à l'utilisation des technologies de l'information est à mettre au bénéfice des réponses techniques conjointes des établissements bancaires et des services répressifs ainsi qu'à une meilleure localisation des auteurs de ce type de délinquance. Ces améliorations sont aussi le fruit d'une politique soutenue de partenariat menée par l'OCLCTIC auprès de ses différents interlocuteurs (pouvoirs publics et secteur bancaire notamment). Plus particulièrement, en ce qui concerne les affaires de phishing (vol par internet des références de cartes de paiement ou d'identifiants d'accès aux compte bancaires en ligne), l'OCLCTIC et la fédération bancaire française ont élaboré un plan de sensibilisation et d'alerte en direction des établissements bancaires qui préconise la mise en place de mécanismes de contrôle permettant la détection rapide de virements frauduleux, en vue de leur blocage, ainsi que le recours à des mots de passe à usage unique pour l'accès aux comptes en ligne. L'office est également associé au forum Pouvoirs publics/industriels organisé par la direction centrale de la sécurité des systèmes d'information (DCSSI) du secrétariat général de la défense nationale (SGDN) dont l'objectif est de développer le partenariat en matière de sécurité des systèmes d'information. La mission de coordination et d'animation de la lutte contre la cybercriminalité imposera bien évidemment de développer le partenariat avec l'ensemble des acteurs publics ou privés concernés par le phénomène. Dans cette perspective, un regroupement commun des enquêteurs spécialisés dans la lutte contre la cybercriminalité appartenant à la police nationale et à la gendarmerie nationale est désormais organisé chaque année pendant quatre jours. La première convention internationale sur la cybercriminalité signée à Budapest le 23 novembre 2001 est entrée en vigueur le 1er juillet 2004. Par ailleurs, les pays du G5 ont engagé des discussions sur la rédaction d'une décision-cadre destinée à harmoniser les conditions de rétention des données de connexion dans l'ensemble de l'Union européenne. Au sein de la Commission européenne, l'OCLCTIC participe aux travaux du groupe « European fraud prevention expert group » qui a initié des sous-groupes spécialisés dans les domaines suivants : la protection des distributeurs automatiques de billets et terminaux de paiement, le phishing, la législation.

Données clés

Auteur : [M. Christian Vanneste](#)

Circonscription : Nord (10^e circonscription) - Union pour un Mouvement Populaire

Type de question : Question écrite

Numéro de la question : 74690

Rubrique : Télécommunications

Ministère interrogé : intérieur et aménagement du territoire

Ministère attributaire : intérieur et aménagement du territoire

Date(s) clé(s)

Question publiée le : 4 octobre 2005, page 9129

Réponse publiée le : 7 février 2006, page 1329