Forum International Cybercriminalité - Intervention de Michèle Alliot-Marie

- Informatique - Sécurité Informatique -

Date de mise en ligne : mercredi 25 mars 2009

Spyworld Actu

Intervention de Michèle ALLIOT-MARIE, Ministre de l'Intérieur, de l'Outre-Mer et des Collectivités Territoriales - Forum International Cybercriminalité - Mardi 24 mars 2009 - Lille

Mesdames, Messieurs,

La cybercriminalité d'aujourd'hui se distingue de celle d'hier d'abord par son étendue.

Criminels et délinquants ont compris qu'ils pouvaient, grâce au monde virtuel, reproduire et amplifier ce qu'ils faisaient dans le monde réel.

C'est vrai des atteintes à la vie privée, devenues un nouvel enjeu avec la multiplication des réseaux sociaux sur Internet.

C'est vrai des escroqueries en ligne ou des attaques racistes et antisémites.

C'est vrai de la pédophilie et de la pédopornographie, qui vise des enfants et des adolescents de tous âges.

C'est vrai de l'espionnage industriel. Au cours des trois dernières années, près de 500 agressions économiques d'origine informatique ont été relevées par nos services. C'est vrai du terrorisme, qui utilise Internet pour répandre sa propagande, diffuser des modes d'emploi d'explosifs ou pirater des sites stratégiques.

Le seul point commun aux formes diverses de la cybercriminalité est l'usage du réseau.

Pour lutter contre la délinquance et la criminalité sur le terrain réel, nous disposons d'une gamme d'outils diversifiés et éprouvés.

Pour relever le défi de la cybercriminalité, il nous faut des moyens adaptés (I), dans le cadre d'une approche globale de la lutte contre la cybercriminalité (II).

Ma priorité a été de renforcer nos capacités d'action contre la cybercriminalité

J'ai pris l'an dernier un certain nombre d'engagements devant vous. Je les ai tenus.

Améliorer la formation des enquêteurs d'abord, en quantité et en qualité.

J'ai décidé le doublement en trois ans du nombre de cyberenquêteurs de la police et de la gendarmerie.

En créant la certification d'Investigateur en Cybercriminalité, j'ai amélioré le niveau de formation des cyberenquêteurs au sein de l'Office de Lutte contre la Criminalité liée aux Technologies de l'Information.

Le titre d'Investigateur en Cybercriminalité correspond à une certification de niveau bac+3 et bac+4. Il sanctionnera une formation de 4 semaines au sein de l'Office tout en valorisant l'expérience acquise dans des fonctions exercées sur le terrain pendant 3 années minimum.

Les enquêteurs formés par la police ont atteint le nombre de 200 à la fin de l'année 2008. Ils seront 300 à la fin de l'année 2009.

Parallèlement, le nombre de NTECH, formés par la gendarmerie en partenariat avec l'université, atteindra 214 fin 2009. En complément de ce dispositif, des "correspondants NTECH" au sein des brigades seront formés par la gendarmerie nationale.

Des instruments nouveaux ont été mis en place.

- Une plate-forme nationale de signalement des sites et contenus illicites sur Internet est hébergée par l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information.

Jusqu'alors, le signalement automatique n'était possible que pour les sites à caractère pédopornographiques. Depuis janvier dernier, elle donne aux internautes les moyens de signaler automatiquement toute forme de malversation constatée sur Internet.

Près de 450 000 connexions ont été enregistrées depuis le début de l'année. Plus de 12 500 signalements ont été effectués.

- Pour mieux cibler les investigations, j'ai créé un groupe dédié aux escroqueries sur Internet au sein de l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication de la police judiciaire.

Ce groupe permet, grâce à l'expertise de policiers et de gendarmes, de centraliser les informations relatives aux escroqueries, facilite les recoupements entre différentes plaintes recueillies sur l'ensemble du territoire national.

Pour aller au-delà de ces premiers résultats, il faut modifier la législation.

J'ai donc fait inscrire dans le projet de LOPPSI des mesures visant à renforcer notre action. La CNIL a été saisie pour ce qui la concerne, et Conseil d'Etat pour l'ensemble du projet de loi.

L'usurpation d'identité sur Internet sera mieux sanctionnée.

Usurper l'identité d'autrui par courrier est interdit par la loi. Ce n'est pas le cas pour l'usurpation d'identité sur Internet. Et pourtant, la diffusion sur Internet est plus large que celle que peut connaître le courrier.

Le blocage des contenus à caractère pédopornographique par les fournisseurs d'accès à Internet est prévu dans le projet de loi.

Il n'est pas tolérable que des sites hébergés à l'étranger puissent diffuser de tels contenus sur Internet. J'ai donc mené la concertation avec les fournisseurs d'accès pour que soit inscrit dans la loi le principe du blocage de ces

sites et contenus.

La possibilité de captation de données numériques à distance permettra aux enquêteurs, par exemple, de saisir en temps réel des données au moment où elles s'affichent sur l'écran d'un pédophile ou d'un terroriste.

Mesdames, Messieurs,

Renforcer nos moyens humains, matériels et juridiques est un préalable et une nécessité. Ce n'est pas suffisant.

Une approche globale est indispensable à la lutte contre la cybercriminalité.

Une approche fondée sur la coopération internationale.

Contre une menace qui ignore les frontières, nous ne pouvons pas agir seuls. Je veux encourager le dialogue, les échanges et les actions communes avec nos partenaires extérieurs.

L'existence même de ce Forum International Cybercriminalité s'inscrit dans cette perspective. Je tiens à en féliciter les organisateurs.

Le guide méthodologique sur les bonnes pratiques face à la cybercriminalité est le résultat concret d'une coopération entre les cyber-enquêteurs français et belge. Je m'en félicite et je salue la présence ici de Stéphane De Clerk ministre belge de la justice.

A l'échelle de l'Union Européenne, j'ai fait adopter par le conseil des ministres de l'Union la création d'une plateforme européenne de signalement des infractions relevées sur Internet.

Financée par la Commission européenne, hébergée par Europol, elle sera mise en place cette année et fonctionnera à partir de dispositifs de signalement nationaux.

J'entends également poursuivre notre coopération bilatérale avec dans ce domaine.

Ainsi, lors de ma récente visite aux Etats-Unis, j'ai obtenu que nous travaillions à la connexion de cette future plate-forme avec la plate-forme américaine.

Les contacts avec mon homologue lors du sommet franco-russe ouvrent aussi des perspectives.

Une approche globale, c'est aussi une approche qui associe l'ensemble des acteurs de la chaîne de sécurité.

Cela suppose des structures de dialogue pour favoriser les échanges.

- J'ai créé un Conseil de sécurité économique au sein du ministère de l'Intérieur parce que nous devons mieux travailler ensemble à l'identification des menaces. En son sein, un groupe dédié à l'insécurité économique nous fait avancer la réflexion dans ce domaine.

Un Conseil national du numérique, chargé de la concertation avec l'ensemble des acteurs du numérique, sera mis en place par le gouvernement dans le cadre du plan France numérique 2012.

J'ai souhaité qu'y figure un groupe chargé des questions de sécurité, associant tous les acteurs de l'Internet, y compris les utilisateurs. Criminologues, juristes, fournisseurs d'accès à Internet, chefs d'entreprises pourront y travailler ensemble.

Au-delà des structures, c'est un nouvel état d'esprit que j'entends créer en renforçant le partenariat avec les entreprises.

La protection des entreprises contre l'ingérence et l'espionnage industriel est un enjeu de sécurité nationale.

C'est particulièrement vrai à l'heure de la crise économique et financière.

Protéger les entreprises, c'est protéger notre tissu économique, et donc nos emplois.

Voilà pourquoi j'appelle chacun à la vigilance et à une politique volontariste d'intelligence économique, défensive pour lutter contre les ingérences étrangères, active pour appuyer les secteurs sensibles ou stratégiques.

J'incite à prendre en compte tous les pôles d'excellence de notre patrimoine économique, industriel et scientifique : qui pourrait ainsi penser que 2/3 des situations avérées d'ingérence économique recensées depuis deux ans concernent la filière agro-industrielle ?

C'est forte de ces convictions qu'à l'été dernier, j'ai demandé à chaque préfet de région d'élaborer un plan triennal d'intelligence économique dans leur région. Ces plans, que je viens d'approuver, représentent une démarche cohérente au profit des entreprises comme des structures de recherche et, tout particulièrement des pôles de compétitivité.

J'attends maintenant que les préfets de région fassent vivre ces plans, en étroite liaison avec tous les services concernés de l'Etat et, au premier chef, les services de la DCRI.

Les entreprises sont un enjeu de la lutte contre la cybercriminalité. Elles doivent en devenir des acteurs à part entière.

La crise économique aggrave les risques de la compétition internationale.

Plus que jamais, l'intelligence économique est une arme indispensable pour faire face aux prédateurs et pour donner aux acteurs de la vie économique les munitions nécessaires.

Mon objectif est donc de donner force et visibilité au secteur de l'intelligence économique.

Cette volonté politique reconnaît l'importance de la recherche d'informations stratégiques.

Cette volonté politique implique également, il faut le répéter, une évolution de certaines méthodes utilisées dans l'univers de l'intelligence économique.

C'est pour cela que j'ai introduit deux orientations dans la LOPPSI.

D'abord, soumettre les sociétés et leurs dirigeants à une procédure d'agrément.

Dans cette procédure, l'avis d'une commission consultative nationale sera sollicité. Cette commission associera naturellement les acteurs professionnels. C'est la garantie de décisions objectives, conscientes des réalités économiques, loin des réflexes et des routines de l'administration française.

Ensuite, pour éviter certaines pratiques, je veux aussi réduire les risques de trafics d'influence.

Le projet de loi proposera donc un délai de 3 ans avant que les fonctionnaires civils et militaires ayant exercé dans un service de renseignements ne puissent exercer d'acticités privées.

Je sais que ces propositions suscitent de nombreux commentaires. Les uns les considèrent comme insuffisantes, les autres comme excessives. Je laisse à chacun le soin de trouver une cohérence dans ces critiques.

Moi, ce qui m'intéresse, je le rappelle, c'est de donner à l'intelligence économique la place qui doit être la sienne. Une place d'importance, vous l'avez compris, ce qui suppose que le secteur dispose d'entreprises ambitieuses et fortes !

Mesdames, Messieurs,

Ministre de l'Intérieur, en charge de la protection des Français, je refuse de laisser nos concitoyens et nos entreprises sans défense face à une menace protéiforme, internationalisée et de plus en plus sophistiquée.

Internet est un formidable espace de libertés.

En luttant contre la cybercriminalité, je veux faire d'Internet ce qu'il n'aurait jamais dû cesser d'être : un espace d'échanges, de diversité et de dialogue d'échelle mondiale.

Je vous remercie.

Post-scriptum :

http://www.interieur.gouv.fr/misill...