

Chronique de Jawad Kerdoudi, président de l'IMRI: « La cybercriminalité, migration du crime réel vers le virtuel »

✕	Chronique de Jawad Kerdoudi, président de l'IMRI: « La cybercriminalité, migration du crime réel vers le virtuel »
---	---

Comme chaque semaine, l'Institut Marocain des Relations Internationales (IMRI) publie une chronique sur l'actualité. Cette semaine, son président Jawad Kerdoudi s'est intéressé à « La cybercriminalité, migration du crime réel vers le virtuel ».

La récente attaque aux Etats-Unis des systèmes informatiques de Sony Pictures relance le problème de la cybercriminalité. Celle-ci est définie comme l'ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la communication. Ces infractions concernent plusieurs secteurs tels que le « carding » qui porte sur le piratage des cartes bancaires, le « skimming » criminalité qui s'attaque aux automates, le « phishing » qui est une pêche des informations bancaires et commerciales, et enfin les escroqueries sur internet de toutes sortes qui englobent la xénophobie, la pedopornographie, l'incitation à l'usage des stupéfiants, le proxénétisme, le terrorisme, et le piratage téléphonique au préjudice des opérateurs.

Ce phénomène prend de plus en plus d'ampleur avec le développement d'internet qui est certes un moyen formidable de communication, mais également un instrument puissant de pouvoir et de guerre. Selon le Computer Crime Research Center, seuls 12% des cybercrimes étaient connus par la police et la justice en 2004. Plusieurs scandales ont défrayé la chronique, dont celui de la NSA en 2013 provoqué par Edward Snowden. Le coût global des cyberattaques a été estimé à 300 milliards d'euros pour les entreprises en 2013. Les Etats-Unis perdent entre 17,5 à 87,5 milliards d'euros par an, et 556 millions de personnes dans le monde ont été victimes de cybercriminalité. Cette situation risque d'empirer du fait du développement extraordinaire des investissements dans le secteur technologique numérique tels que ADSL, L4G, WIFI, Cloud. Le phénomène risque de s'amplifier également par la dématérialisation des processus, le développement du e-commerce et du e-learning, la croissance des paiements en ligne, l'augmentation des utilisateurs du Web qui a enregistré un taux de croissance de 46% entre 2012 et 2013. Le haut lieu mondial de la cybercriminalité pour la création de logiciels malveillants est la Chine, suivie par la Russie, les Etats-Unis, le Brésil et le Royaume-Uni. Pour les machines détournées la première place appartient aux Etats-Unis, suivie par la Chine, la Corée du Sud, l'Allemagne et la France. Enfin par les crimes relatifs aux arnaques sur internet, la palme revient à l'Afrique en particulier la Côte d'Ivoire et le Nigeria.

MINIMISER LES CONSÉQUENCES DE L'ATTAQUE

Pour se protéger contre la cybercriminalité, il est clair que le risque zéro n'existe pas. Il faut faire en sorte que si elle arrive, les conséquences de l'attaque soient minimales. Il faut pour cela renforcer les moyens matériels et humains, procéder à une modification de la législation, développer une culture de l'informatique, et associer le secteur privé à la lutte contre ce fléau. Il faut également privilégier l'approche préventive, c'est-à-dire qu'il faut augmenter les difficultés des attaques en diminuant les profits potentiels. Cela signifie le renforcement de la robustesse des infrastructures informatiques et de télécommunications. Il faut enfin s'appuyer sur des structures de veille et d'alerte telles que le CERT/CC américain. La coopération internationale est indispensable, car les pays qui ne sont pas dotés de lois contre la cybercriminalité sont des paradis numériques, où les cybercriminels peuvent lancer des attaques informatiques ou héberger des sites illicites en toute impunité. Elle a déjà commencé par la Convention de Budapest du 23 Novembre 2001 sur la cybercriminalité qui a le mérite de régler les problèmes de compétence et d'entraide entre Etats, et de les obliger à conserver certaines données pour permettre la traçabilité de l'information. Elle énumère plusieurs infractions (accès illégal, interception illégale, atteinte à l'intégrité des données et des systèmes) pour lesquelles chaque pays doit avoir un volontaire politique et une coopération efficace de leurs services de justice et de police. Cette coopération internationale pose le problème de la gouvernance d'internet sur le plan mondial. Certains s'interrogent sur la pertinence d'une réglementation, d'autres demandent qu'elle soit déclarée comme un bien commun, et placée sous le contrôle de l'ONU ou d'un organisme intergouvernemental autonome.

QU'EN EST-IL DE CETTE QUESTION DE LA CYBERCRIMINALITÉ POUR LE MAROC ?

D'après Microsoft, le Maroc est 3,5 fois plus vulnérable aux logiciels malveillants que la moyenne mondiale. Le Maroc présente des failles touchant l'administration et les infrastructures qui constituent des menaces pour la sécurité nationale publique et économique. Preuve en est le piratage à partir du mois d'Octobre 2014 de documents confidentiels marocains relatifs à la diplomatie, au Sahara, et aux services de l'appareil de l'Etat. Le cybercriminel se fait appeler Chris Coleman, sévit sur un compte Twitter et n'a pas caché son objectif de nuire au Maroc. Une lecture officielle de ce cybercrime a été présentée le 11 Décembre 2014 devant la Chambre des Conseillers accusant les services spécialisés algériens d'avoir monté et accompagné cette opération. Dès lors, il faut que la cybercriminalité soit un chantier prioritaire pour le gouvernement, et passe du stade défensif à celui offensif. D'où la nécessité de créer une structure civile placée à un haut niveau, et qui aura par vocation la centralisation des informations et la coordination entre les services civils et militaires. Elle doit disposer également d'un centre de documentation chargé recueillir les statistiques spécifiques en vue de les analyser. Elle devra jouer un rôle opérationnel, signaler les contenus illicites sur internet, et apporter une assistance technique au profit du secteur public et privé. Elle sera également chargée de la formation et de la sensibilisation, et assurera les relations avec les Agences internationales chargées de lutter contre la cybercriminalité.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source :

http://www.aufait.ma/2014/12/23/chronique-de-jawad-kerdoudi-president-de-limri-la-cybercriminalite-migration-du-crime-reel-vers-le-virtuel_635947
par Jawad Kerdoudi, président de l'IMRI