

La criminalité économique et financière à l'ère numérique | Le Net Expert Informatique



Les banques, les compagnies d'assurances, les sites gouvernementaux, les compagnies pétrolières et, maintenant, l'industrie aéronautique avec la cyberattaque de la compagnie polonaise LOT : le cybercrime cible des secteurs de plus en plus sensibles, sources de dégâts humains majeurs. Au-delà des pertes financières, c'est le cœur du système politique, économique et juridique qui est aujourd'hui menacé par ce fléau.

Que fait l'État, la justice, pour enrayer ces comportements ? Fabriquer des lois en série est-elle la solution face à l'existence de cyberparadis, d'une cyberéconomie souterraine de plus en plus puissante, et à la volatilité des preuves ? Le Point.fr a interrogé Myriam Quemener, magistrate, auteur d'un ouvrage de référence sur le sujet : La criminalité économique et financière à l'ère numérique.

Le Point.fr : « Certaines formes de cybercriminalité sont le fait de réseaux mafieux structurés issus de pays n'ayant pas de législation dédiée à ce phénomène », écrivez-vous. Le décalage entre les législations étatiques est-il surmontable et à quelle échéance ? Que font les autorités françaises en attendant une prise en charge globale et harmonisée de cette délinquance ?
Myriam Quemener : Les pays européens ont harmonisé leurs législations et la coopération internationale se renforce en permanence. La Convention de Budapest, seul traité relatif à la lutte contre la cybercriminalité, a déjà été signée par 46 pays, et d'autres États sont actuellement en négociation pour y adhérer. Pour ce qui concerne la France, notre pays dispose d'un arsenal ancien, en particulier la loi de 1988 dite « loi Goffrain » qui permet de réprimer les piratages informatiques et les cybermenaces. Cet arsenal s'est progressivement enrichi et perfectionné pour permettre le recours à des procédures adaptées à l'univers numérique. De nouvelles structures sont nées, comme l'Anssi, qui met en œuvre la stratégie gouvernementale en matière de cybersécurité, mais aussi une nouvelle sous-direction de lutte contre la cybercriminalité et un pôle numérique au parquet de Paris qui a vocation à s'étoffer. On a aussi créé le procureur de la République financier à compétence nationale exclusive en matière de délits boursiers et pour les affaires économiques et financières complexes qui sont aussi souvent à dimension internationale.

Quels sont les nouveaux moyens d'investigation des enquêteurs pour déjouer les attaques ?
Sur le plan procédural, le législateur a transposé le régime des interceptions téléphoniques à Internet. Il a aussi innové en prévoyant l'infiltration numérique, qui est une enquête sous pseudonyme. Elle permet à l'enquêteur d'utiliser un nom d'emprunt pour entrer plus facilement en contact avec le cyberdélinquant. Depuis la loi du 13 novembre 2014, l'enquête sous pseudonyme jusqu'alors utilisée en matière de pédopornographie et de contrefaçon s'applique à l'ensemble des procédures de criminalité organisée.

Les données personnelles sont considérées comme « l'or noir du XXI^e siècle ». La semaine dernière, une importante base de données américaine abritant les coordonnées, données de santé et autres informations personnelles d'environ 20 millions de fonctionnaires a été piratée. Quel usage les cyberdélinquants font-ils des données récupérées, et à quoi peut-on s'attendre dans les années qui viennent ?
Ils récupèrent ces données et les revendent sur les marchés noirs du Web (darknet) qui sont des réseaux parallèles aux réseaux ouverts du type Google. Cela permet par exemple de faire des achats sous de fausses identités ou d'obtenir des virements en se faisant passer pour une entreprise connue. Les données personnelles servent aussi à créer de faux profils, et tout cela se répercute sur l'e-réputation des entreprises. L'usurpation d'adresses IP (spoofing) qui permet de commettre des fraudes à la téléphonie mobile se développe aussi de manière considérable.

Quels sont les prochains défis de la criminalité astucieuse sur Internet ?
En cette période où le terrorisme frappe de façon dramatique, il est important de s'attaquer avec vigueur au financement du terrorisme, et cette lutte passe par une politique publique pragmatique et déterminée contre des phénomènes comme le cyberblanchiment ou les escroqueries aux faux ordres de virement. Il faut par ailleurs être attentif et vigilant face à des outils numériques comme le crowdfunding (financement participatif) ou les crédits à la consommation. Les sommes obtenues au travers de ces formes de prêt peuvent en effet servir à financer des activités illicites. Il en est de même du « trading haute fréquence » qui permet d'envoyer des ordres d'achat à une vitesse de l'ordre de la nanoseconde, grâce à des algorithmes superpuissants, permettant des manipulations de cours. Le courtage à haute fréquence a aussi ses dérivés : un courtier londonien a récemment été arrêté pour une manipulation sur le marché des contrats à terme électroniques aux États-Unis, qui avait contribué au mini-kraich de mai 2010 à Wall Street. Il faut aussi suivre avec attention le développement de ces fameuses « monnaies virtuelles » qui contournent le système bancaire et permettent d'échapper à tout contrôle étatique en raison de l'absence de traçabilité. Les objets connectés, qui favorisent l'usurpation de profils complets, et le cloud computing qui contient des données sensibles à valeur commerciale sont aussi des cibles potentielles de cyberattaques. D'autant que de nombreuses failles de sécurité existent et peuvent être exploitées par les cybercriminels.

Qu'est-ce qui dissuade vraiment les délinquants, qu'ils soient isolés ou membres d'organisations criminelles ?
La mise en place d'une stratégie globale au niveau des services de l'État est de nature à dissuader les cyberdélinquants, de même que les condamnations et démantèlements de réseaux de cybercriminels qui ne cessent d'augmenter grâce aux moyens d'investigation et à l'expertise de plus en plus pointue des enquêteurs dédiés.

Pensez-vous que l'Internet a démultiplié les risques, ou les a-t-il seulement déplacés ?
L'absence de confrontation physique auteur-victime, propre à Internet, facilite le passage à l'acte. Le système des rencontres virtuelles attire des personnes mal intentionnées qui peuvent plus facilement extorquer de l'argent, notamment via des sites de vente entre particuliers. Aujourd'hui, la cybercriminalité s'industrialise et s'organise sous forme de structures hiérarchisées allant de la main-d'œuvre de base qui récupère des données jusqu'aux têtes de réseau qui donnent les ordres.

Ces phénomènes sont-ils, comme le changement climatique, irréversibles ?
Je ne le pense pas, car, actuellement, il y a une mobilisation importante, du secteur tant public que privé, pour lutter contre ces phénomènes. Il est indispensable de multiplier les actions de formation pluridisciplinaire des acteurs publics et privés qui concourent à la lutte contre ces attaques. Cependant, il ne faut pas perdre de vue que ce type de délinquance lance un défi au temps judiciaire, c'est même une course contre la montre !
L'ouvrage en vente ici

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03941 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en cybercriminalité et en déclarations à la CNIL. Denis JACOPINI et le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plaît ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lepoint.fr/chroniqueurs-du-point/Laurence-neuer/cybercrime-un-defi-lance-au-temps-judiciaire-13-07-2015-1943938_56.php