CYBERSÉCURITÉ

SOLANGE GHERNAOUTI
Professeure, directrice du Swiss Cybersecurity Advisory & Research Group, HEC – Unil (www.scarg.org)

Le chemin se trace en marchant

La perpétuité pour le créateur de la plateforme électronique «Silkroad» de mise en relation et de vente en ligne entre vendeurs de tout ce qui est illicite et acheteurs. Plaque tournante du monde criminel, ce site du marché noir, ouvert en 2011 et fermé par le FBI deux ans plus tard, est une véritable entreprise criminelle pour effectuer des trafics en tout genre (drogue, piratage informatique, faux papier, tueur à gage, blanchiment d'argent). Cette place de marché mondial a su tirer parti du numérique, des techniques d'anonymisation et de l'usage du Bitcoin pour être performante. Son fondateur Ross Ulbricht, qui se fait appeler Dread Pirate Roberts – le terrible pirate Roberts – comme le héro au masque noir du roman fantastique de l'Américain William Goldman paru en 1973 «The Princess Bride», aurait amassé une fortune de 18 millions de dollars et inspiré la concurrence.

Le signal lancé par les autorités américaines est clair, ce n'est pas parce qu'Internet permet de tout faire, qu'il faut tout faire et laisser faire. Avec cette affaire, le sentiment d'impunité que pouvaient ressentir les criminels est mis à mal et la capacité de faire du crime un moyen comme un autre pour s'enrichir est ébranlée, la perpétuité c'est long…

Peu de temps avant ce procès aux Etats-Unis, nous apprenions que le Ministère public de la Confédération ne traitait que deux plaintes sur 240 liées à des cybercrimes. C'est très peu et cela reflète la pénurie de moyens accordés à la lutte contre la cybercriminalité, mais aussi la difficulté et la complexité de ce type d'enquête. Cela alimente un cercle vicieux, les victimes ne déposent pas plaintes convaincues de l'inutilité de la démarche. Dans la mesure où il n'y pas de plaintes, il est difficile de justifier du besoin d'accorder plus de ressources à la lutte contre la cybercriminalité…

Nous ne devons pas nous habituer aux cybernuisances et considérer qu'elles font partie de notre quotidien, ni que le système de justice et police ne peut réaliser sa mission première du fait d'un Internet mondialisé. Etre victime de pickpockets sur Internet ou dans la rue est traumatisant à plus d'un titre, c'est une violence réelle, physique, émotionnelle et économique aux impacts directs (plus d'argent) et indirects (trauma, peur...) importants. De plus cela contribue à enrichir les acteurs criminels au détriment de la société. Car l'argent volé appauvrit la victime, qu'elle soit une personne ou une entreprise commerciale, et ne permet pas de contribuer au développement économique ou au bien-être de proches, mais il alimente les réseaux criminels pour leur donner plus de pouvoir et de puissance de nuisance.

Un des défis les plus importants de la lutte contre la cybercriminalité est l'efficacité de la collaboration et de l'entraide judiciaire internationale, ce qui suppose qu'au niveau national ces questions soient aussi résolues et que les cantons disposent des ressources nécessaires. Pour pallier la distribution de moyens, qui sont encore insuffisants dans tous les cantons, et les problèmes de coordination inhérents, disposer en Suisse d'un centre spécialisé, correctement dimensionné et organisé, permettrait de monter en puissance et de gagner en efficacité dans la lutte contre la cybercriminalité.

La prévention c'est bien mais insuffisant, nul n'est à l'abri d'un clic de trop, d'une escroquerie bien montée ou de l'attractivité de certaines offres commerciales qui semblent tout à fait licites mais qui en réalité sont le fait de criminels, comme la vente en ligne de produits contrefaits par exemple.

Avec les informations récoltées sur les victimes potentielles notamment sur les réseaux sociaux ou les techniques d'usurpation d'identité, les criminels sont très efficaces pour leurrer leurs proies d'autant plus qu'ils maîtrisent l'art de la communication et de la manipulation ou encore les techniques de marketing et de e-commerce.

De plus, aucune entité est totalement immune aux intrusions informatiques et au vol de données. Il suffit pour s'en convaincre de rappeler l'intrusion dans les systèmes de l'Office Personnal Management ayant conduit au vol de données concernant quatre millions d'employés fédéraux aux Etats-Unis annoncé au début du mois de juin 2015 (http://www.opm.gov/news/latest-news/announcements/Information About the Recent Cybersecurity Incident).

Le même terme anglais «power» signifie puissance et pouvoir, donnons le pouvoir et la puissance à nos acteurs de la lutte contre la cybercriminalité d'effectuer leur tâche car désormais, chaque système connecté, chaque internaute est une proie potentielle, augmenter le niveau de vigilance et de sensibilisation et le niveau de protection des infrastructures est fondamental, mais il existera toujours des victimes qu'il faudra secourir si nous ne voulons pas vivre dans une société du chacun pour soi et laisser monter en puissance et en pouvoir les acteurs criminels. ■