

Moyen d'enrichissement, lieu d'expression du pouvoir, des crimes et des conflits, Internet est désormais au service

# Cybercriminalité : fléau o



Par Solange Ghernaoui

Professeur ordinaire  
Département des systèmes d'information  
sgh@unil.ch

## Le cyberspace : nouvel écosystème

Avec un Internet omniprésent et incontournable, le cyberspace constitue désormais le prolongement technologique quasi naturel de notre environnement, c'est un écosystème régi par la loi du marché et les acteurs les plus forts. Ni pire ni meilleur, il reflète notre réalité sociale, économique, politique et criminelle. Désormais l'écosystème cybercriminel, indissociable de l'écosystème numérique, fait partie de notre société et nous impactent tous. Chaque équipement ou chaque entité accessible via Internet peut devenir une cible ou un vecteur de la cybercriminalité. Leur présence dans le cyberspace, comme celles des internautes, très visible notamment à travers des réseaux sociaux par exemple, justifient la présence des cybercriminels et leurs activités. Internet est un facteur de proximité criminelle, c'est une zone criminogène, une zone à risques. L'écosystème cybercriminel est, comme tout écosystème, vivant et dynamique, en permanente adaptation pour tirer partie des nouvelles opportunités, des nouvelles vulnérabilités, des nouveaux outils et vecteurs de la criminalité.

## Une criminalité facilitée

Les criminels ont bien compris comment exploiter les opportunités que leur offrent Internet pour être performants dans leurs activités classiques (trafics d'être humains, de drogue, chantage, extorsion, crime économique, blanchiment d'argent, etc. – vieux crimes avec de nouveaux moyens) et pour innover. Le mode de fonctionnement d'Internet, les failles technologiques, organisationnelles, humaines ou juridiques comme les problèmes de territorialité, d'entraide judiciaire internationale insuffisante ou le manque de moyens auxquels sont confrontées les instances de justice et de police pour poursuivre un crime transnational, profitent aux criminels. Internet leur offre une couche d'isolation protectrice, avec une relative impunité et une prise de risque minimale pour une profitabilité optimale.

## Des criminels rationnels et une économie parallèle

Les cybercriminels sont des acteurs rationnels et suivent la loi du marché, de l'offre et de la demande. Ils sont avant tout des criminels qui ont su extrapoler leurs activités, savoir-faire et modes d'action dans le cyberspace. Comme il existe, dans le

monde réel, des marchés noirs et une économie illicite, il en est de même dans le cyberspace. Les marchés noirs de la cybercriminalité fonctionnent sur la base économique des marchés classiques et ont pour seuls objectifs performances et rentabilité. Il s'agit de mar-

« Vieux crimes avec de nouveaux moyens »

chés noirs bien réels qui alimentent toute la chaîne des acteurs de la cybercriminalité. Ces marchés noirs s'appuient sur les outils de communication et de mise en relation de l'Internet. Ils utilisent les mêmes mécanismes, savoir-faire et outils que ceux liés notamment à la publicité en ligne et au e-commerce licites. Les marchés noirs de la cybercriminalité se trouvent à toutes les étapes de réalisation des cybercrimes, de leur préparation à leur monétisation. De plus, Internet contribue largement à la valorisation de leurs bénéfices.

L'équilibre de l'écosystème cybercriminel se maintient si dans le temps les acteurs obtiennent des gains financiers bien supérieurs aux risques encourus d'être poursuivis par les forces de police. Cela dépend des risques réels, qui peuvent être plus ou moins bien maîtrisés et contrôlés selon les stratégies criminelles développées, mais aussi de la perception de ces risques. Entre la maximisation des valeurs issues de la cybercriminalité, la rapidité des gains et les risques d'être pris, certains cybercriminels ont su développer une réelle intelligence économique dynamique et adaptative au service du crime. Quelles que soient les motivations des acteurs de la cybercriminalité, celle-ci engendre toujours des conséquences économiques non négligeables supportées par la société. Ses impacts sont directs et indirects avec des effets immédiats ou à long terme. La cybercriminalité porte atteinte aux individus, aux organisations et aux Etats, qu'elle fragilise et déstabilise.

## Bio

Professeure de l'Université de Lausanne, experte internationale, Solange Ghernaoui est directrice du *Swiss Cybersecurity Advisory and Research Group* ([www.scarg.org](http://www.scarg.org)) et du groupe de recherche en Science de la Complexité au sein de la faculté des HEC. Ancienne auditrice de l'Institut des hautes études de défense nationale, elle est l'auteur de très nombreux livres et publications scientifiques et de vulgarisation concernant la sécurité informatique, la cybercriminalité et la maîtrise des risques, dont « *Cyberpower: crime, conflict & security in cyberspace* » [EPFL Press, 2013], « *La cybercriminalité: le visible et l'invisible* » [Le Savoir suisse, 2009]. Chevalier de la Légion d'honneur, membre de l'Académie suisse des sciences techniques, elle fait partie des 300 personnalités les plus influentes de Suisse et des 20 femmes qui font la Suisse [Bilan 2011, 2012].

de tous les acteurs de la société, qu'ils soient individuels ou institutionnels, licites ou illicites, de bonne ou de mauvaise foi.

# u opportunité ?

Toutefois, l'ampleur des activités cybercriminelles, la nature des cybercriminels pouvant aller de monsieur et madame Tout le monde à des spécialistes de l'informatique ou de la grande criminalité organisée, en passant par des mercenaires à la solde des plus offrants, comme le champ d'action mondial des cybercriminels, contribuent à la difficulté de dresser un panorama définitif des acteurs de la cybercriminalité ou de quantifier à sa juste valeur les coûts que la cybercriminalité fait porter sur la société.

## Challenges de recherche et d'enseignement

Sur le plan de la recherche, appréhender efficacement la cybercriminalité nécessite plus que jamais de disposer de politiques de soutien à des recherches de nature interdisciplinaire qui favorisent notamment le décloisonnement traditionnel des champs disciplinaires au service de projets innovants dans la manière de penser la sécurité informatique et la protection des valeurs. Dans les conditions actuelles, c'est une belle reconnaissance des compétences de HEC Lausanne que d'avoir décroché le projet européen E-Crime, dont Interpol est également partenaire, relatif à l'impact économique de la cybercriminalité et aux mesures de lutte contre la cybercriminalité<sup>1</sup> (voir encadré).

La cybercriminalité commence à devenir un nouveau champ d'étude à part entière

qui reste à explorer de manière interdisciplinaire en croisant des savoirs issus notamment du droit, de la sécurité, de la sociologie, de l'anthropologie, de l'économie, des sciences politiques, des mathématiques, de l'informatique et des télécommunications. L'Unil est un précurseur dans ce domaine puisque c'est en 2001 que voit le jour, sur proposition des professeurs P. Margot, P. Moreillon et S. Ghernaoui, la Maîtrise universitaire en droit, criminalité et sécurité des technologies de l'information<sup>2</sup>, premier diplôme interfacultaire et interdisciplinaire de l'Université de Lausanne. Cette formation permet d'acquérir les compétences nécessaires à l'appréhension des problèmes d'ordre juridique, criminel, économique, politique, managérial et technologique liés à l'informatisation de notre société. Le professeur A. Villa, vice-doyen HEC, en est l'actuel directeur. Environ cinq cents étudiants suisses ou de nationalités étrangères ont bénéficié de cette formation innovante et unique en Suisse. Ils occupent pour la plupart des postes à responsabilités aux niveaux national et international.

<sup>1</sup> European Union's Seventh Framework Programme for Security - grant agreement n° 607775 <http://ecrime-project.eu/>

<sup>2</sup> Plus d'information sur [www.unil.ch/dcs](http://www.unil.ch/dcs)

« La cybercriminalité commence à devenir un nouveau champ d'étude à part entière »

Dossier spécial

INTERNET

L'équipe de Solange Ghernaoui partenaire du projet européen E-Crime

**ecrime**  
The Economic Impacts of Cyber Crime

Huit pays, dix partenaires dont Interpol, projet financé par la Communauté européenne de 2014 à 2017 pour étudier les impacts économiques de la cybercriminalité dans les secteurs non IT, évaluer les mesures existantes de lutte contre la cybercriminalité et proposer des éléments d'optimisation de la maîtrise de la cybercriminalité. (<http://ecrime-project.eu/>).



Frank Bertholet  
M 079 219 12 64  
f.bertholet@mengisdruck.ch

Imprimerie **mengis** Druck AG

[www.mengisdruck.ch](http://www.mengisdruck.ch) | [info@mengisdruck.ch](mailto:info@mengisdruck.ch)