

## QUESTIONS OUVERTES

# Comment lutter contre la cybercriminalité ?

*Les infractions et crimes commis via Internet sont légion. Pour juguler cette cybercriminalité, les protections techniques sont loin de suffire. Une coopération internationale et la mobilisation de tous les acteurs, du citoyen à l'État, sont requises.*

Solange GHERNAOUTI-HÉLIE

La criminalité classique étend son emprise par une large gamme de forfaits commis à travers le réseau Internet : escroqueries, fraudes, extorsions, abus, espionnages, vandalismes, conflits, harcèlements, etc. – termes auxquels on peut accoler désormais le préfixe *cyber*. La cybercriminalité recouvre ainsi toute activité illégale ou irrégulière réalisée à travers le cyberspace. Par extension, elle intègre toute forme de malveillance électronique effectuée au moyen de l'informatique et des télécommunications (téléphonie, cartes à puce,...). Cette nouvelle forme de criminalité, dont l'ampleur est considérable mais encore mal chiffrée, appelle la société et les gouvernements à réagir. Comment ? Avant de proposer quelques réponses, précisons le contexte et les enjeux de la cybercriminalité.

Les technologies de l'information et de la communication sont devenues des cibles de la malveillance (vol d'ordinateurs ou de données, prise en otage de ressources informatiques...) ou des moyens pour commettre des actions illicites (chantage, détournement, blanchiment d'argent...). Le réseau Internet facilite des délits classiques, notamment ceux relevant de la criminalité économique, et donne lieu à de nouvelles formes de délits (fraude informatique, piratage de logiciels...). La dématérialisation des services et des transactions, les outils de mise en relation et de communication, la capacité d'agir à distance et sous de fausses identités ou des identités usurpées, de passer par un grand nombre d'intermédiaires techniques (serveurs, four-

nisseurs d'accès, etc.) et de pays différents : tout cela autorise des formes d'organisation, d'échanges et d'activités criminelles très profitables au regard de l'investissement nécessaire et du risque encouru.

Par ailleurs, dans le cyberspace, tout le monde peut communiquer avec n'importe qui, n'importe quand, n'importe où. Les utilisateurs – enfants, personnes âgées ou autres personnes sans histoires – y côtoient virtuellement des acteurs malveillants de

tions ou les États. Elles sont la cible de cybermenaces sur leur disponibilité, leur intégrité ou leur confidentialité. Elles peuvent également être utilisées pour manipuler l'opinion (endoctrinement, diffusion de rumeurs...), pour l'espionnage, pour la surveillance et le contrôle social, ou encore pour déstabiliser une économie, voire un État. Le réseau Internet est certes un fabuleux outil de communication, mais il constitue aussi un instrument de pouvoir et une arme de guerre !



**LES GUICHETS AUTOMATIQUES BANCAIRES** font aussi partie des cibles d'attaques réalisées via Internet, pour récupérer des données bancaires confidentielles.

toutes sortes [pédophiles, terroristes, criminels, délinquants, escrocs professionnels, etc.]. Internet est dès lors un espace où le risque informatique d'origine criminelle est structurel, omniprésent et permanent.

Au-delà de leur intérêt pour les individus, les infrastructures informatiques et de télécommunication sont aussi d'importantes ressources stratégiques pour les organisa-

## Un phénomène difficile à chiffrer

Il faut aussi avoir conscience que la cybercriminalité se développe dans un contexte global de guerre économique permanente, de recherche de profit immédiat, de crise financière internationale, d'injustice sociale, de risques écologiques, sans vision à long terme ni parfois de gouvernance. Par ailleurs, sur Internet, tout s'achète et tout se vend, y compris la découverte de vulnérabilités des systèmes informatiques, les outils d'attaques informatiques, les données personnelles, les identités et identifiants, etc. Enfin, la loi qui s'impose sur Internet est celle des acteurs les plus forts, tel l'empire *Google*. Comment, dans ce contexte compliqué et mêlant des aspects très divers, lutter contre la cybercriminalité ?

Pour répondre à cette question, il est d'abord nécessaire de s'interroger sur la gouvernance d'Internet, sur la dépendance vis-à-vis d'Internet, vis-à-vis des fournisseurs de solutions et de services, y compris ceux

de sécurité. Il faut aussi connaître les acteurs de la cybercriminalité ainsi que l'ampleur du phénomène. Tous ces éléments ne sont pas aisés à cerner. Qui contrôle Internet ? Qui contrôle la sécurité informatique, ceux qui en ont besoin ou ceux qui vendent des solutions ? Qui sont les cybercriminels ? Comment quantifier l'espionnage électronique ? Comment savoir si nos données ont été volées alors qu'elles sont justes copiées et qu'elles existent toujours ? Comment identifier un harcèlement, une campagne de désinformation et manipulation d'opinion, et évaluer leur impact ? Comment estimer le produit du blanchiment d'argent *via* Internet ? Comment apprécier les effets en cascade, les impacts directs et indirects consécutifs à une interruption de service informatique ?

On ne sait pas répondre précisément à toutes ces questions. Pourquoi ? Beaucoup de délits ne sont pas dénoncés, pour diverses raisons (inutilité de la démarche, crainte d'une publicité négative, etc.). De plus, il existe très peu d'études sur les victimes de cybercrimes. Et le nombre d'incidents rapportés aux instances de justice et police, ainsi que le nombre de cas faisant l'objet de sanctions juridiques, ne suffisent pas à apprécier la réalité de la cybercriminalité. Le chiffre noir de la cybercriminalité est considérable, même s'il est mal connu (il représente le nombre de crimes inconnus des services de police, dans la mesure où aucune plainte n'a été déposée, et indique donc l'écart entre la malveillance connue et la malveillance bien réelle).

Certes, des rapports sur les sinistres informatiques sont régulièrement publiés par diverses institutions, par exemple l'*Internet Crime Complaint Center* (IC3, Centre des plaintes contre les crimes sur Internet) aux États-Unis. Mais seuls quelques faits et tendances peuvent en émerger et ces rapports ne reflètent qu'une partie visible de l'iceberg de la cybercriminalité. Selon l'organisation non gouvernementale *Computer Crime Research Center*, en 2004, seuls 12 pour cent des cybercrimes étaient connus des instances de justice et de police. En 2009, selon cette même source, le nombre de plaintes déposées au niveau international serait de l'ordre de 20 pour cent.



© Shutterstock/Photosan, Renana Inga

Comme la plupart des sinistres ne sont pas déclarés et que l'information disponible est très incomplète, on ne peut estimer correctement le phénomène cybercriminel. C'est là un véritable obstacle à la mise en place de moyens de lutte financiers, organisationnels et humains. Par ailleurs, les études quantitatives ne sont pas toutes fiables. Ainsi, celles qui émanent des acteurs du marché de la sécurité informatique peuvent indiquer des tendances, mais elles peuvent aussi constituer un outil de marketing destiné à vendre des solutions et des conseils en matière de sécurité informatique. La méfiance est donc de rigueur : les études sont parfois biaisées en fonction de l'intérêt des parties prenantes. L'insécurité fait peur et la peur peut être un formidable levier commercial...

Ce bref aperçu permet de comprendre l'étendue et la complexité du problème de la lutte contre la cybercriminalité. Ce combat dépend d'une volonté politique et devrait se fonder sur une approche globale, au service d'une vision partagée de la sécurité publique, pour une protection efficace des citoyens, des nations et des valeurs

**LES CRIMES ET DÉLITS** commis dans le cyberspace peuvent viser des individus, mais aussi des organisations, des entreprises et même des États.

## L'AUTEUR



Solange GHERNAOUTI-HÉLIE, experte internationale en sécurité du numérique, est professeur à l'École des hautes études commerciales (HEC) de l'Université de Lausanne, en Suisse.

fondamentales des sociétés démocratiques (notamment la protection des données personnelles et la protection des personnes à l'égard du traitement automatisé des données à caractère personnel). Et tous les acteurs, tous les fournisseurs de services et intermédiaires techniques, doivent assumer leur part de responsabilité dans ce combat global et collectif.

## Quelles armes pour lutter ?

L'un des enjeux majeurs de la lutte contre la cybercriminalité est celui de développer une culture de l'informatique et pas seulement celle de la sécurité, trop souvent fondée sur la peur : il ne suffit pas de sensibiliser la population aux dangers du réseau Internet et aux précautions élémentaires, les citoyens doivent aussi comprendre les fondements et l'organisation du système qu'ils utilisent.

Une lutte efficace contre la cybercriminalité exige aussi une approche préventive, afin de réduire les possibilités de commettre des forfaits sur le cyberspace. En d'autres termes, il s'agit d'augmenter la difficulté des attaques et les risques pris par leurs auteurs, tout en diminuant les profits qu'ils peuvent espérer. Cela signifie renforcer la robustesse

des infrastructures informatiques et de télécommunication à l'aide de mesures de sécurité techniques, procédurales et managériales cohérentes, et mettre en place un système juridique et policier efficace. Ainsi, outre une volonté politique, la lutte contre la cybercriminalité suppose des moyens juridiques, organisationnels, procéduraux, techniques et humains, ainsi que des partenariats entre les secteurs public et privé.

Une coopération internationale est par ailleurs indispensable. Les pays qui ne sont pas dotés de lois contre la cybercriminalité sont des paradis numériques, où les criminels peuvent lancer des attaques informatiques ou héberger des contenus illicites en toute impunité. La différence des approches légales nationales constitue un frein à la lutte contre la cybercriminalité, transnationale par nature. Non seulement un cadre légal applicable au niveau national doit exister, mais il doit aussi être compatible avec celui des autres États ; c'est ce qu'a très bien souligné la Convention sur la cybercriminalité du Conseil de l'Europe, établie à Budapest en novembre 2001.

Au-delà de l'harmonisation des cadres légaux, les États doivent traduire leur volonté politique par une coopération efficace de leurs services de justice et de police. Cela

suppose des structures organisationnelles, des procédures et des personnes compétentes pour faciliter une réelle coopération internationale, comme c'est le cas avec les actions menées par Interpol et Europol contre la criminalité.

À l'instar de la lutte contre le réchauffement climatique, la lutte contre la cybercriminalité fait l'objet de sommets et de débats politiques. Le Sommet mondial sur la société de l'information, tenu à Genève en 2003 et à Tunis en 2005, a notamment contribué à identifier la nécessité d'une gouvernance de l'Internet plus internationale, plus « onusienne », et la nécessité d'un Internet plus fiable et plus accessible à l'ensemble de la planète.

Des dispositions mondiales ont alors été prises pour développer la cybersécurité et lutter contre la cybercriminalité. Ainsi, l'Union internationale des télécommunications, via son programme *Global Cybersecurity Agenda* lancé en 2007, a publié un rapport stratégique qui fait référence, et elle a contribué à créer en 2009 le Centre IMPACT (*International Multilateral Partnership Against Cyber Threats*) de lutte contre les cybermenaces, installé en Malaisie. Par ailleurs, en 2008, l'OTAN a décidé de créer en Estonie un centre de formation à la défense contre les attaques cybernétiques sur Internet. Bien qu'il soit



impossible de lister toutes les institutions concernées par la maîtrise de la sécurité informatique et la lutte contre la cybercriminalité, citons toutefois l'ENISA (*European Network and Information Security Agency*, l'Agence européenne de sécurité de l'information et des réseaux), ou encore l'OCDE (Organisation de coopération et de développement économiques) qui proposent des activités, événements, publications et directives dans ces domaines.

## Y a-t-il une réelle volonté politique ?

Toutefois, toutes les recommandations ou structures ne peuvent se substituer à une réelle volonté politique ou à la mobilisation des acteurs publics et privés. Dégager des moyens nécessaires à la réalisation d'une stratégie de lutte bien définie, clairement traduite par des politiques de sécurité réalisables, ne se limite pas à financer des mesures techniques de sécurité (comme celle du contrôle d'accès). En effet, afin que les infractions puissent être dénoncées et analysées, et leurs auteurs identifiés et poursuivis, il faut mettre en place une organisation efficace des acteurs concernés (services de justice, police, gendarmerie, renseignement, protection civile), spécifier des procédures adaptées et régler les problèmes de compétences territoriales. Cela reste à faire.

En France, parmi les acteurs institutionnels impliqués dans la lutte opérationnelle contre la cybercriminalité, retenons surtout l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de la Direction centrale de la police judiciaire. Cet office collabore notamment avec la Direction centrale du renseignement intérieur, la Direction générale de la sécurité extérieure, la Direction de la protection et de la sécurité de la défense, Interpol et Europol ; il est également le point de contact national pour les pays ayant ratifié la Convention sur la cybercriminalité. Par ailleurs, pour certaines enquêtes, dont celles nécessitant la récupération ou l'analyse de données informatiques, divers services de police, de la gendarmerie nationale ou des douanes



par exemple, sont amenés à collaborer. Il convient aussi de mentionner la création, en juillet 2009, de l'Agence nationale de sécurité des systèmes d'information (ANSSI), de compétence nationale, rattachée au secrétaire général de la Défense.

Précisons enfin que la prévention des cybercrimes s'appuie sur des structures de veille et d'alerte, telles que le CERT/CC américain (*Computer Emergency Response Team/Coordination Center*). Ces organisations ont un rôle clef d'anticipation, par la détection de signaux faibles qui préfigurent les attaques d'envergure. Elles sont également actives dans la diffusion des découvertes de nouvelles vulnérabilités, des solutions de sécurité, de recommandations pratiques ou connaissances en matières de gestion de risques et de crises.

La synergie et la convergence du crime mafieux, du crime économique et du cybercrime, ainsi que le rapprochement des mondes terroriste et criminel, constituent des menaces sur la sécurité des nations, des organisations publiques ou privées, et des individus. La réaction à ces menaces doit prendre plusieurs formes et être transnationale. Prise de conscience internationale, sujet de débats politiques et juridiques, mais aussi sujet d'études techniques, sociologiques et économiques, la cybercriminalité ne peut être combattue qu'en portant les efforts sur tous ces différents axes. Il s'agit d'un défi à relever rapidement, tout en respectant les droits de l'homme et les valeurs démocratiques de nos sociétés. ■

**LES LOCAUX D'IMPACT** à Cyberjaya, en Malaisie. IMPACT (*International Multilateral Partnership Against Cyber Threats*) est le premier partenariat global et international contre les cybermenaces. Cette plate-forme est le siège opérationnel du programme *Global Cybersecurity Agenda* lancé en 2007 par l'Union internationale des télécommunications, dont 191 États sont membres.

## ✓ BIBLIOGRAPHIE

S. Ghernaouti-Hélie,  
**La cybercriminalité : le visible et l'invisible**,  
Presses Polytechniques  
et Universitaires Romandes, 2009.

J.-Y. Marion et M. Kaczmarek,  
**Boulevard du cybercrime**,  
dans *Dossier Pour la Science* n°66,  
« L'ère d'Internet », janvier-mars 2010.

**Convention sur la cybercriminalité du Conseil de l'Europe :**  
<http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm>

**Global Cybersecurity Agenda :**  
<http://www.itu.int/osg/csd/cybersecurity/gca/index.html>

Centre IMPACT :  
<http://www.impact-alliance.org/>

ENISA (Agence européenne de sécurité de l'information et des réseaux) :  
<http://enisa.europa.eu/>

ANSSI (Agence nationale de sécurité des systèmes d'information) :  
<http://www.ssi.gouv.fr>