PSC INFO

4 | 2016

Dossier
Cybercriminalité

Chère lectrice, cher lecteur,


PSC

L'énergie qu'il faut déployer pour pratiquer le vol et et le mensonge sur Internet, pour y simuler des sentiments ou pour y déverser sa haine, semble sans limites.

Les propos tenus par Stéphane Koch dans notre interview m'ont fait prendre une nouvelle fois conscience que l'éducation est l'une des clés pour prévenir efficacement la criminalité sur Internet. Détenir une compétence médiatique est décisif pour savoir comment se protéger, ne pas croire tout ce qu'on voit ou ce qu'on lit, et pour comprendre comment fonctionnent les dispositifs de communication numériques. Cette protection passe par l'amélioration du niveau de connaissances des utilisatrices et des utilisateurs.

La police municipale de Zurich a engagé un dialogue soutenu avec la population, en se servant systématiquement des médias sociaux. Depuis quelque temps, la population peut suivre le travail policier des deux iCoPs Jean Patrick et Eleni Moschos, en se servant des média sociaux. Tous les deux sont en contact étroit avec des jeunes et des jeunes adultes de Zurich et environs, et se font ainsi l'écho de la population, qui souhaite davantage de transparence et de confiance.

Nos meilleurs vœux pour
la nouvelle année 2017.

Martin Boess
Directeur PSC

Situation actuelle et tendances de la cybercriminalité

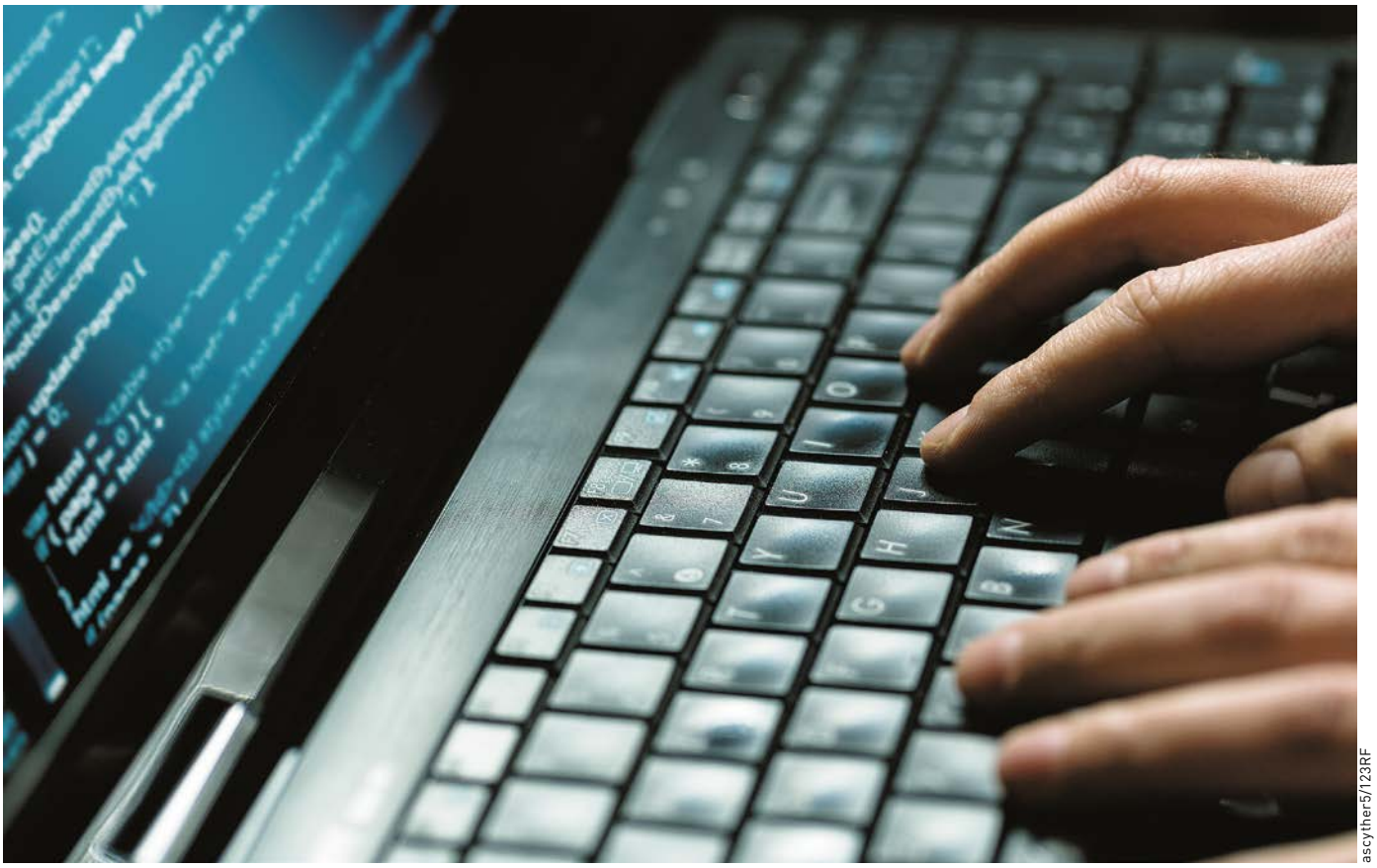
Interview de Stéphane Koch

Monsieur,
Sur votre site www.intelligentzia.ch, vous résumez vos services de la façon suivante : « Conseil & formation en intelligence économique et gestion stratégique de l'information, stratégies numériques et réseaux sociaux, sécurité de l'information ». Les éléments de votre formation sont également impressionnants et se rapportent tous aux médias numériques sous les aspects les plus divers. Vous êtes donc pour nous l'interlocuteur idéal pour une interview visant à présenter à nos lecteurs la thématique « Criminalité sur et via Internet », mettant bien sûr l'accent sur les mesures de prévention de la criminalité et les poursuites pénales.
Mais tout d'abord une question générale en introduction :

Quelle est la différence entre la criminalité « normale » et la cybercriminalité, et comment le Web a-t-il modifié la criminalité ?
La différence se situe principalement au niveau de la dématérialisation de notre société. Dès lors, la cybercriminalité représente globalement une continuité ou une adaptation des formes de criminalité que l'on trouve dans le monde physique. Nombre d'actions criminelles qui se déroulent par le biais de l'utilisation des TIC (technologies de l'information et de la communication), respectivement d'internet, ont une base ancrée dans le monde physique (que ce soit au niveau de l'utilisation d'un serveur, ou d'un ordinateur ou encore d'un périphérique mobile), donc en relation avec un potentiel « for juridique » (base légale liée à l'emplacement d'un serveur/ordinateur dans le monde physique). Les principales différences résident dans l'asymétrie entre le peu de moyens nécessaires pour mettre en œuvre une action cybercriminelle et l'impact important que celle-ci peut avoir, tant au niveau financier que par rapport au nombre de personnes ou d'entreprises qui peuvent être touchées par une action unique. Une autre forme d'asymétrie se situe au niveau de la lutte contre les actions cybercriminelles, même si l'organisation et la diffusion de ces actions (fraude en ligne, cyberattaque, cyberextorsion, etc.) demandent peu de moyens aux cybercriminels. Ce que les autorités concernées vont devoir entreprendre pour lutter contre ces formes de cybercriminalité va – à l'inverse – demander énormément de ressources, que ça soit au niveau humain, en temps, ou au niveau technique. De plus, c'est aussi extrêmement contraignant au niveau de la justice. Les lieux physiques entre l'organisation et la mise en œuvre d'une action cybercriminelle, ainsi que ceux liés à l'emplacement des victimes de cette action ne sont pas nécessairement les mêmes et peuvent être répartis dans différentes zones géographiques du monde qui ne bénéficieront


DR

Stéphane Koch, conseiller et formateur en communication et stratégie numérique, spécialiste de la sécurité de l'information, spécialiste de réputation numérique et réseaux sociaux.



ascyther5/123RF

« La cybercriminalité adapte des formes de criminalité que l'on trouve dans le monde réel. »

pas nécessairement d'accords d'entraide judiciaire. Un autre changement majeur est qu'aujourd'hui les cybercriminels peuvent toucher leurs victimes potentielles chez elles, sans pour autant avoir à fracturer leurs appartements. Et il en va de même pour les entreprises. Le cybercriminel n'est qu'à un clic de souris de sa victime. Et dans le cas de fraude en ligne, les dommages causés peuvent facilement dépasser la valeur des biens qui se trouveraient physiquement dans un domicile donné. Dans un cas de sextorsion, par exemple, la victime pourrait ressentir un traumatisme psychologique identique à celui d'une agression physique, sans pour autant avoir directement été physiquement agressée. De plus, paradoxalement et en opposition aux sciences forensiques classiques, domaine dans lequel l'évolution des technologies a facilité l'investigation (recherche de traces, utilisation de l'ADN, reconstitution et numérisation en 3D des scènes de crime, par exemple), l'évolution du domaine des TIC a compliqué d'autant l'investigation numérique. Des cybercriminels chevronnés sont tout à fait capable de modifier, d'altérer, voire d'effacer des traces numériques. Et si on prend en compte que chaque ordinateur impliqué dans une activité cybercriminelle peut représenter une scène de crime en tant que tel, et qu'un certain nombre d'ordinateurs concernés par « cette activité » appartiendront à des particuliers innocents (leurs ordinateurs mal protégés, ou infectés, ayant été utilisés à l'insu de leurs propriétaires), on prend alors toute la mesure de la complexité de l'investigation numérique. Donc, oui, le web a fondamentalement modifié la criminalité, d'autant plus que les gens n'ont pas été formés à détecter le pendant « cybernétique » des formes de la criminalité classique, alors que « l'intervention » de la police, elle, est devenue beaucoup plus compliquée.

Quels sont, d'après votre estimation, les principaux secteurs de délits sur Internet, ou plus précisément, quels sont selon vous les délits basés sur Internet qui entraînent les plus grands dommages dans notre pays ?

Il n'est pas facile de répondre, car tous les délits ne sont pas signalés, que ça soit au niveau des individus ou celui des entreprises. Parfois on hésite à signaler que l'on a été victime d'une fraude en ligne, d'un chantage, ou d'un vol de données. Mais actuellement les tentatives de phishing visant à injecter un ransomware dans les ordinateurs des particuliers et des entreprises semblent occuper la première place du podium (90% des attaques par phishing contiennent un logiciel de rançon). Europol a d'ailleurs annoncé que ces logiciels de rançon sont considérés comme une menace prioritaire au niveau européen. Les « fraudes au président » occupent aussi une place importante par rapport au montant des

wk1003mike/Shutterstock.com

« 90% des attaques par phishing contiennent un logiciel de rançon. »

fonds détournés. D'autres types de fraudes, aussi basées sur l'usurpation d'identité et l'ingénierie sociale, sont fortement présentes sur les réseaux sociaux. A ce titre, l'usurpation d'identité n'étant pas, en tant que telle un délit pénal, ça facilite le travail des cybercriminels.

Y a-t-il des délits qui touchent plus particulièrement la Suisse et si oui, comment peut-on l'expliquer ?

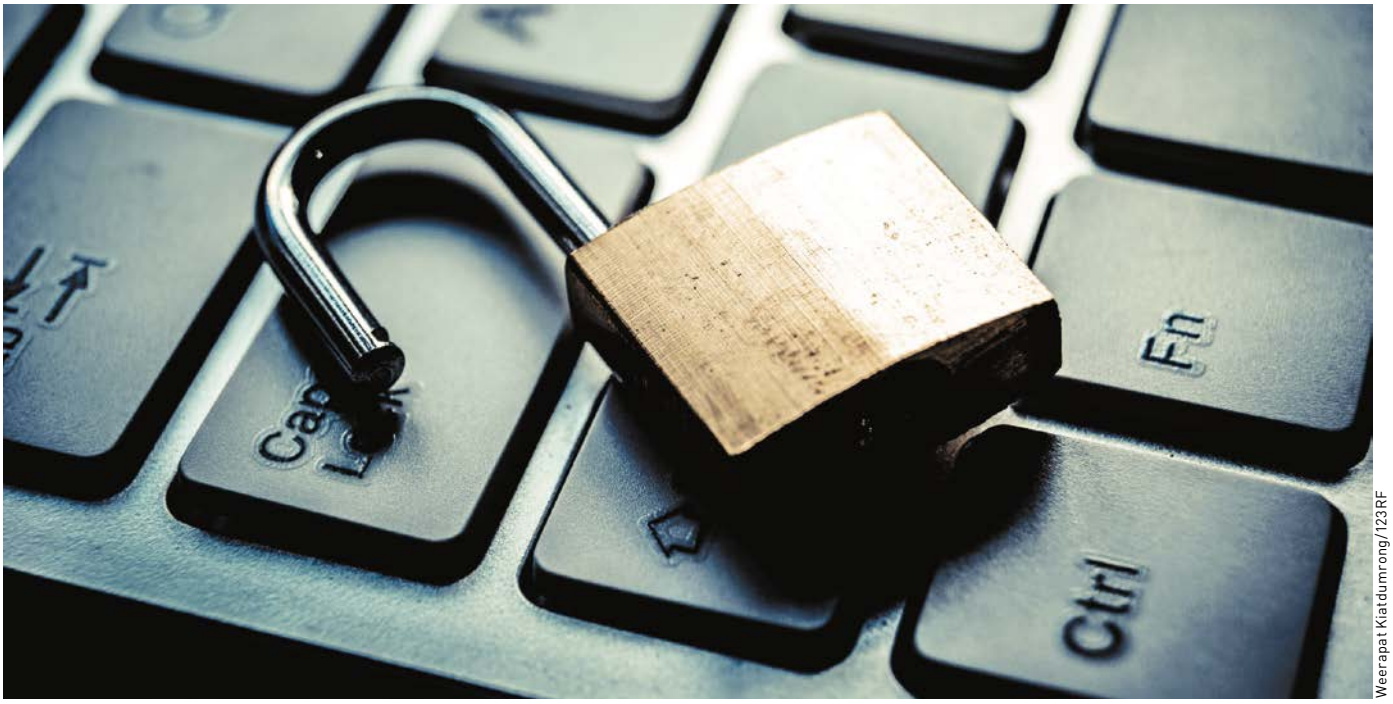
La Suisse est considérée comme un pays riche, dont les citoyens ont un bon niveau de vie. Dès lors, elle est globalement plus ciblée que d'autres pays : attaques sur les infrastructures critiques, attaques par déni de services distribué (DDOS), qui, même quand elles se déroulent à l'étranger, affectent les entreprises et les utilisateurs en Suisse, étant donné la répartition mondiale des infrastructures internet et leur interdépendance en terme de connectivité. Ce type d'attaque (DDOS), suivant son importance, est à même de freiner voire de bloquer l'accès à de multiples services qui dépendent de l'accès à internet, que ça soit à un niveau local ou global. En mars 2016, des sites Web suisses de banques et de commerces en ligne avaient été victimes d'un groupe cybercriminel nommé Armada, qui avait réussi à bloquer l'accès à leurs services suite au refus des entreprises concernées de payer la rançon demandée par les cybercriminels. En septembre 2016, « Internet » a connu l'attaque par DDOS la plus importante jamais observée (Mirai botnet). Sa particularité résidait dans le fait que pour mener à bien leur offensive, les cybercriminels se sont servis d'environ 400 000 caméras connectées à travers le monde, dont les « accès administrateurs » par défaut n'avaient pas été modifiés par leurs propriétaires. Une attaque similaire, dont les effets se sont aussi fait ressentir en Suisse, a eu lieu le mois suivant. Mais ce n'est là qu'un exemple, auquel on peut ajouter les attaques par tentative de phishing, le blocage de l'accès aux fichiers numériques – des particuliers ou des entreprises – par des « logiciels de rançon » (ransomwares, qui bloquent l'accès aux fichiers jusqu'à ce que la rançon soit payée), les vols de données d'entreprises (bancaires ou autres), etc. Ce qui fait la différence entre un pays et un autre, ce sont les moyens que ce pays va mettre en œuvre pour lutter contre la cybercriminalité ou d'autres formes d'attaques initiées par le biais des réseaux connectés, ainsi que le niveau de « conscience » de ses citoyens et des entreprises. Et dans ce domaine la Suisse est à la traîne ! Il y a des manquements considérables dans les moyens de lutte contre la cybercriminalité, et le niveau de connaissance et de réactivité des entreprises et des individus est largement insuffisant. En ce qui concerne les moyens, c'est un problème politique. La Suisse est victime de son fédéralisme, à l'heure où le monde est interconnecté, et fait peu de cas des frontières physiques, culturelles et linguistiques. Seule Zurich possède une brigade autonome de lutte contre la cybercriminalité (les autres cantons ont dans la majorité des cas une unité de lutte contre la criminalité informatique, qui opère en soutien des autres services de polices), et la majorité des magistrats ne sont pas formés aux TIC (technologies de l'information et de la

communication) et les dossiers s'empilent. Pour ce qui est des entreprises et des particuliers, le manque de conscience et de connaissances fait que la Suisse représente – en toute logique – un terrain privilégié pour les cybercriminels. Le 22e rapport semestriel de MELANI (Centrale d'enregistrement et d'analyse pour la sûreté de l'information) illustrait bien cette situation, son thème prioritaire était « la gestion des lacunes de sécurité ». Comme le disait récemment Guillaume Poupard, directeur général de l'Agence nationale française de la sécurité des systèmes d'information, l'Anssi : *« Au sein des entreprises, il y a évidemment un responsable de la sécurité des systèmes d'information : il est indispensable, mais pas suffisant. L'idée, c'est vraiment de se dire que chacun est acteur de cette cybersécurité : le PDG, le directeur juridique, le directeur financier… Chacun a un rôle à jouer, y compris l'intérimaire, généralement oublié dans les procédures, alors qu'il a souvent accès aux systèmes. »* Cette situation, qui fragilise l'économie du pays, respectivement sa compétitivité et donc sa croissance, ne changera pas, tant que les mentalités n'évolueront pas. A l'heure actuelle, il n'y a quasiment rien dans l'enseignement scolaire primaire, secondaire, ou dans celui des hautes écoles, qui puisse permettre à tout un chacun d'intégrer les connaissances nécessaires pour comprendre, assimiler et maîtriser la transformation numérique de notre société (l'ensemble de ces connaissances est regroupée sous la dénomination de « littératie numérique », l'Europe quant à elle a mis en place le programme de formation en culture numérique « DLit2.0 Curriculum »).

http ://www.digital-literacy2020.eu/content/sections/index.cfm/secid.59

Y a-t-il en Suisse des catégories spécifiques de victimes ? Y a-t-il des personnes, des groupes ou des institutions particulièrement menacés par la cybercriminalité ?

Le comportement des cybercriminels est assez logique : ils cherchent à optimiser le rendement de leurs actions criminelles et vont donc s'attaquer au plus faible. En terme de cybercriminalité, ça signifie que les attaques viseront en premier lieu les ordinateurs - ou autres outils ou périphériques informatiques – les moins bien protégés. Pour reformuler la question, on pourrait dire que c'est le potentiel de profit qui définit la cible. Les entreprises seront donc une cible importante, mais l'accumulation de petits profits par la multiplication des attaques sur les particuliers génère beaucoup de revenu tout en créant un risque minime pour les cybercriminels (chaque ordinateur individuel touché étant une nouvelle affaire pour la police et la justice). Il est important de comprendre néanmoins que la majorité des fraudes demandent une intervention ou une « collaboration » de la victime. Dès lors le facteur de réussite d'un grand nombre de ces fraudes en ligne repose sur le manque de connaissance ou l'inconscience de l'utilisateur. Il ne faut pas non plus négliger le fait que certains gouvernements (ou groupes soutenus par des gouvernements) ont parfois des comportements cybercriminels et, qu'à ce titre, les institutions ou certains pôles stratégiques peuvent représenter des cibles de choix. La récente attaque sur la société RUAG en est un bel exemple : les attaquants ont utilisé un logiciel espion (un malware) pour s'infiltrer dans les serveurs de RUAG et piller son patrimoine



Weerapat Kiatdumrong/123RF

« Les cybercriminels tentent d'optimiser leur rendement et vont donc s'attaquer au plus faible. »

neydt/123RF

«Les Hacktivists sont une sorte de Black Blocs numériques, tel que le mouvement Anonymous, avec des revendications d'ordre sociétal et politique.»

intellectuel et industriel. Les instigateurs de cette cyberattaque – qui n'ont toujours pas été formellement identifiés à ce jour – ont pu agir plusieurs mois avant que l'on finisse par détecter leur présence.

Avez-vous des connaissances sur les criminels ? S'agissant de la «criminalité hors ligne», il existe des groupes de criminels spécialisés et des mobiles bien définis. Peut-on observer la même chose au niveau de la cybercriminalité et si oui, sous quelles formes ?

Il n'est pas évident de dresser un «état des lieux» de la cybercriminalité qui soit exhaustif, car c'est un domaine polymorphe qui se compose de nuance de gris. Par exemple, il n'y a pas les «hackers» et le reste du monde. Tout un ensemble de «courants» sont présents et il est important de les définir et de les catégoriser: il y les **«Black Hats»** (comportement criminel); les **«White Hats»** (comportement éthique, hackers éthiques, utiles à la société, ils font remonter des failles de sécurité); les **«Grey Hats»** (un peu des deux); les **«State sponsored hackers»** (comportements criminels – officieusement – soutenus par un Etat, ou nationalistes soutenant de facto leur pays par des actions offensives); les **«Hacktivists»** (forme de Black Blocs numériques, tel que le mouvement **Anonymous,** avec des revendications d'ordre sociétal et politique. A la base, ce ne sont pas des criminels, mais la nature de leurs comportements peut l'être); les **«Cybercriminels»** (extension et développement des activés criminelles classiques dans le monde cybernétique); les **«Script kiddies»** (adolescents généralement, ou personnes utilisant des programmes informatiques créés par d'autres – et possédant un potentiel d'attaques – car eux-mêmes ne possèdent pas le niveau d'expertise pour les développer); les **«Cyber-mercenaires»** (personnes monnayant leurs connaissances informatiques. «L'affaire Giroud» en est un exemple. En 2014, cet encaveur valaisan a été accusé d'avoir embauché un cyber mercenaire pour aller voler des documents l'incriminant sur les ordinateurs de deux journalistes). En résumé, tout ce petit monde représente à la fois la diversité et la complexité des acteurs du monde numérique. Cette complexité est encore accrue par le fait qu'aujourd'hui, les cybercriminels ont des comportements d'entrepreneurs, et certains entrepreneurs (ou des gouvernements) ont parfois des comportements de cybercriminels. On observe aussi la présence de «cybercriminels à temps partiel», qui agissent épisodiquement dans l'obscurité, tout en étant au grand jour employés par des entreprises, car ils évaluent que la prise de risque est minime par rapport aux gains potentiels (théorie des opportunités en criminologie, Walsh, 1986). Il y a aussi ceux qui cherchent des failles de sécurité pour les revendre – entre autres – sur le Darknet (marché gris de la cybercriminalité). Ils ne commettront pas de crimes eux-mêmes, mais fourniront les «armes et les munitions», respectivement les ressources nécessaires à leur mise en œuvre à des cybercriminels (entre autres). C'est un marché très lucratif, et peu risqué. Certaines failles de sécurité peuvent se

revendre plusieurs centaines de milliers de francs. A ce titre, le marché gris des failles de sécurité fournit non seulement les cybercriminels, mais aussi des entreprises, des gouvernements et leurs services de renseignements. Certains gouvernements ont alloué un budget spécifiquement dédié à l'achat de ce type de ressources (failles de sécurité, ou vulnérabilités inconnues des concepteurs des logiciels, pour lesquelles il n'existe pas de parade ou de correctif, et qui par leur nature permettent d'accéder à des programmes, respectivement des ordinateurs en contournant les mesures de sécurité présentes. Ce type de faille est aussi appelé 0Day, ou vulnérabilité Zero day).

En 2012, le Dr Michael McGuire, du John Grieve Centre, a tenté de dresser un portrait de la relation potentielle entre le crime organisé et la cybercriminalité, dans une étude nommée: «Organised Crime in the Digital Age». Selon cette étude, 80% des groupes cybercriminels reposeraient sur une forme de structure organisée, sans pour autant que ces groupes organisés appartiennent tous à une organisation criminelle classique. 43% des membres de ces organisations cybercriminelles avaient plus de 35 ans, et 29% moins de 25 ans. La moitié des groupes comprennent une structure de six personnes ou plus, avec un quart comprenant 11 ou plus. 25% des groupes actifs ont agi pendant moins de six mois.

www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf

Vous avez également une formation en lutte contre la criminalité économique. Pouvez-vous nous parler de la lutte contre la criminalité économique sur Internet ? Quels en sont les points forts ou quels devraient-ils être ? De quels moyens dispose-t-on pour les poursuites pénales et lesquels font défaut ?

Avec la montée en puissance de l'utilisation des TIC, la dématérialisation croissante des services et l'émergence de l'internet des objets (de plus en plus de connexions et d'échanges de données entre des périphériques connectés à des éléments de notre quotidien, où le frigo connecté ne pose pas trop de problème, mais une pompe à insuline, un pacemaker, une voiture, ou encore la serrure d'un appartement, eux, oui), on assiste à une augmentation importante des cas de criminalité économique en rapport avec le domaine du numérique. Le problème est que – comme expliqué à la question 3 – la police et la justice n'arrivent pas à obtenir les ressources qui leur seraient nécessaires pour être en mesure de traiter la multitude de cas qui se présentent à eux. Et les cas suisses ne se limitent pas aux frontières de la Suisse, ils nécessitent la plupart du temps une collaboration au niveau européen ou mondial. Cette collaboration est souvent soumise à des demandes d'entraide judiciaire qui vont prendre du temps, et cette latence profite pleinement aux cybercriminels. Il existe bien la Convention sur la cybercriminalité du Conseil de l'Europe, qui est entrée en vigueur en Suisse en 2012, mais tous les pays ne l'on pas signée, et les cybercriminels exploitent logiquement ce genre de failles. Ils chargent des spécialistes du domaine juridique d'évaluer quelles seront – légalement – les meilleures bases arrière pour lancer leurs attaques.

Si vous deviez conseiller à un avocat spécialisé dans la protection des données des stratégies dans le domaine de la cybercriminalité, quelles seraient vos recommandations pour les actions de poursuite pénale en Suisse ?

Il doit y avoir une vraie réflexion au niveau pénal, et elle ne doit pas être l'œuvre uniquement de juristes et de la «politique». Dans le domaine des TIC, le système de milice a atteint ses limites. Il est nécessaire que les professionnels – du secteur public et du secteur privé – qui, dans leur pratique, luttent contre la cybercriminalité, puissent exposer les problèmes auxquels ils sont confrontés. Les connaissances lacunaires des politiques en matière de société de l'information (y compris dans les commissions spécialisées), impactent extrêmement négativement sur leur capacité à comprendre les problèmes liés à la lutte contre la cybercriminalité. Par exemple, début 2013, Me François Charlet, un avocat spécialisé dans la protection des données, et moi-même, avions été invités par un parti politique pour partager quelques réflexions sur les problématiques liées aux TIC. Suite à cette réunion, il était ressorti que la pénalisation de l'usurpation d'identité était un dossier prioritaire. En 2016, ce qui a progressé, c'est uniquement le nombre de victimes! Il

rangizzz/123RF

«La police et la justice nécessitent une collaboration au niveau européen ou mondial, et des demandes d'entraide judiciaire qui vont prendre du temps; les cybercriminels le savent.»

en va de même avec les fuites de données : l'Europe a mis en place la Directive NIS « Network Security and Information » qui entrera en vigueur en 2018 (www.riskinsight-wavestone.com/2016/03/8822/). Elle contient une obligation de déclaration aux autorités compétentes en cas de piratage d'infrastructures considérées comme étant critiques, d'intrusion dans les systèmes informatiques, ainsi que l'obligation, pour les entreprises victimes de fuite de données, de signaler leur cas aux régulateurs nationaux, et aux personnes touchées, sous trois jours. Elle impose aussi aux acteurs concernés de prendre les mesures nécessaires pour assurer une sécurité efficace de leurs infrastructures. La Suisse – que certains présentent comme le futur coffre numérique du monde – se doit d'appliquer au plus vite de telles directives.

Au niveau des particuliers, là aussi la justice est à la traîne et nombre de magistrats ne semblent pas être connectés avec les réalités de notre société… connectée. J'ai traité des cas de *sextorsion* et de *revenge porn* (pratique qui consiste à diffuser des images intimes, à caractère sexuel, du conjoint sans le consentement de celui-ci), et dans le cas du *revenge porn,* selon le code pénal suisse, la victime – suivant son âge – pourrait être potentiellement considérée comme coupable de création et de diffusion de contenus à caractère pornographique. Non seulement on ne reconnaît pas son statut de victime, mais l'agresseur ne risque pas grand-chose non plus. Dans le canton de Vaud, en 2013, un homme reconnu coupable de la diffusion de vidéos intimes de son ex-copine, sur un site pornographique, n'a été condamné qu'à 50 jours amende avec sursis (les femmes représentent plus de 80% des victimes). Il en va de même lorsque qu'une femme se fait violer : si les agresseurs filment la scène et la partagent dans un groupe WhatsApp – comme c'est déjà arrivé – ou sur le Net, le ou les agresseurs seront éventuellement condamnés pour le viol, mais le juge ne prendra pas en compte le fait d'avoir filmé et partagé le viol, alors que le fait de filmer un viol en vue de partager devrait – dans l'intention – être considéré pénalement comme un acte de cruauté ! Le jugement devrait aussi prendre en compte une obligation légale de retrait des contenus incriminés du Net, sous peine d'une autre sanction en cas d'échec. En résumé, pour que la loi évolue, il faut que les mentalités évoluent. Il est nécessaire que les autorités concernées développent une conscience de la victime et des traumatismes potentiels qui résultent d'une agression en ligne, et du stress posttraumatique dû au risque de réapparition des contenus humiliants pour la victime. Cette évolution des mentalités est aussi nécessaire pour que les magistrats comprennent mieux les contraintes liées au travail d'enquête de la police en rapport avec le Net. Par exemple « l'investigation secrète », qui autorise l'utilisation d'une identité d'emprunt (dont la réglementation a été harmonisée au niveau fédéral et est entrée en vigueur en 2005), doit être plus facile à mettre en œuvre.

De quelle manière la criminalité sur Internet va-t-elle évoluer ? Peut-on s'attendre à de nouveaux types de délits ?
Le spécialiste en criminologie Michael McGuire définit la cybercriminalité comme étant la quatrième ère de la criminalité. Pour ma part, je pourrais résumer la question par « plus de crimes et moins de moyens pour les combattre ». Il ne faut néanmoins pas accepter l'augmentation de la cybercriminalité comme une fatalité. Mais il faut se donner les moyens de la combattre. Et plus encore que les moyens financiers, légaux et policiers, c'est la « connaissance » qui est et sera toujours le « nerf de la guerre » contre ces formes de criminalité. Au final, les cybercriminels utilisent les mêmes technologies que nous. Une grande majorité des cyberattaques et des fraudes en ligne reposent sur la méconnaissance des utilisateurs. Si on prend le phishing, par exemple, ça fait près d'un quart de siècle que le Web existe, et on n'a toujours pas appris aux utilisateurs à lire correctement un lien internet (URL), dont la manipulation est l'élément de base sur lequel repose la fraude.

Quel est le rôle du Darknet dans la cybercriminalité ? La police a-t-elle une chance de détecter les crimes dans le Darknet ou faudrait-il modifier la législation ?
La problématique représentée par ce que l'on nomme le Darknet n'est pas uniquement un problème de législation. Les outils qui permettent l'anonymat, et que l'on associe généralement au Darknet sont les mêmes outils que ceux utilisés par les défenseurs des droits humains ou par des journalistes dans des pays non démocratiques pour rapporter des cas d'atteintes aux libertés individuelles, ou pour dénoncer les mauvais agissements de certains gouvernements ou des cas de corruption. Pour résumer, ces outils sauvent aussi des vies. Donc la solution ne passe pas par un affaiblissement des technologies (de chiffrement par exemple), elle passe par l'amélioration du niveau d'expertise et une meilleure collaboration et un meilleur échange d'informations entre les différents services de police et de justice, tant au niveau national qu'international. De plus, les faits nous ont prouvé que le Darknet n'est pas un espace impénétrable : en 2013, le FBI a réussi à fermer « Silk Road » une des plus grandes places de commerce illégal du Darknet. Puis il a réussi à infiltrer – dès le début de son lancement – Silk Road 2.0 pour le fermer en 2014. Aujourd'hui, une nouvelle version du site existe, et connaît un développement florissant, surtout dans la vente de drogues. Mais quoi de différent avec le monde physique ? On n'a pas réussi à y éradiquer la vente de drogue non plus. Ce que je veux dire, c'est qu'avec les moyens et le niveau d'expertise adéquat, la police est en mesure de lutter sur tous les fronts technologiques.

scanrail/123RF

«Avec les moyens et le niveau d'expertise adéquat, la police est en mesure de lutter sur tous les fronts technologiques.»

Quels sont les principaux conseils pour se protéger de la cybercriminalité ?
Quitte à me répéter : l'utilisateur, qu'il s'agisse d'un individu ou d'une personne morale, doit fondamentalement améliorer son niveau de connaissance. Rien ne pourra se faire sans cela. L'Etat, quant à lui, doit lui mettre à disposition les moyens pour pouvoir le faire. Que cela passe par l'instruction publique, les entreprises, et pourquoi pas l'armée (on pourrait imaginer une formation dispensée pendant l'école de recrue). En France, par exemple, l'Institut national des hautes études de la sécurité et de la justice (INHESJ) et la Délégation interministérielle à l'intelligence économique (D2IE) se sont engagés dans une démarche partenariale visant à former des «Conférenciers en sécurité économique» issus du monde économique : entreprises, pôles, clusters, consultants, etc. L'objectif est de délivrer un message général, uniformisé et cohérent sur la sécurité économique et de promouvoir les outils existants ou à venir. Il est aussi de la responsabilité de l'Etat d'identifier les menaces que les entreprises et les citoyens ne peuvent pas être en mesure d'identifier. Il faut mettre en place des structures gouvernementales, qui utiliseraient les ressources disponibles dans le secteur privé, pour proactivement rechercher les menaces à venir (failles 0-day / vulnérabilité Zero day), évaluer le matériel utilisé dans les infrastructures stratégiques du pays (hardware, software, firmware). Le futur de la sécurité économique de la Suisse, de sa capacité d'innovation et de croissance, est à ce prix. Au niveau légal, les entreprises qui ne protègent pas suffisamment leurs données doivent être pénalisées.

L'utilisateur, quant à lui, a pour responsabilité de comprendre les outils qu'il utilise. Il n'est plus acceptable d'être dans cette forme de déni de responsabilité vis-à-vis de technologies que l'on utilise au quotidien. Alors que dans notre société physique, la grande majorité des gens acceptent la responsabilité de devoir s'informer sur les médicaments qu'on leur aura prescrit, ou sur la composition des aliments qu'ils vont consommer, ou encore sur le mode d'utilisation et le fonctionnement du véhicule qu'ils vont utiliser. Ils rechignent, mais acceptent néanmoins de s'adapter au tri des déchets et aux «nouvelles règles» liées à l'évolution et aux changements qui surviennent dans notre monde physique. Ce n'est pourtant pas différent avec les TIC ! Elles sont à la base de la transformation numérique de notre société, et le monde virtuel n'en est que la «réalité» dématérialisée. Ça reste quand même la société, notre société, celle dans laquelle on vit, et non un «espace virtuel» à part de celle-ci, comme l'a dit Edgard Morin : «dans une société complexe, il faut adopter une pensée complexe». Je me permettrais de reformuler son propos par «prendre le temps d'apprendre à vivre avec son temps, pour ne pas exister hors du temps».