CYBERCRIMINALITE

Le risque n'est pas virtuel !

La criminalité informatique et économique continue à tirer parti des facilités et des failles de l'internet. La maîtrise de cette cybercriminalité nécessite une réponse concertée de tous les Etats. Objectifs : rétablir la confiance dans le monde numérique, minimiser le risque et faire en sorte que les nouvelles technologies et internet ne profitent pas uniquement au crime.

Solange Ghernaouti - Hélie

Professeur à l'Ecole des HEC de l'Université de Lausanne

Directrice du DEA en Droit, Criminalité et Sécurité des Nouvelles Technologies

Dorénavant, les nouvelles technologies sont à considérées comme cible et comme moyen d'expression de nouvelles formes de criminalité. On constate qu'internet est devenu un facteur de rapprochement entre le crime économique et le crime organisé, un facteur d'organisation accrue du crime économique ainsi qu'un facteur de performances. Mais le crime économique n'est pas uniquement réservé à la criminalité organisée. Les outils informatiques et télécoms le mettent à la portée d'individus isolés, qui peuvent se constituer ou non en groupes plus ou moins importants. Par conséquent, les nouvelles technologies offrent un contexte favorable à l'expression de la criminalité et le crime informatique comme sa déclinaison en cybercriminalité devient un moyen pour réaliser des délits économiques.

> « Internet offre une couche d'isolation protectrice aux criminels »

De nos jours, les activités criminelles s'effectuent à travers le cyberespace, par d'autres moyens que ceux habituellement mis en œuvre, et de manière complémentaire à la criminalité économique classique. Non seulement internet offre des conditions exceptionnelles pour de nouvelles entreprises et activités illicites, mais il autorise également la réalisation de fraudes ou délits habituels via l'outil informatique. Les contrefaçons de cartes à puce, les fraudes sur les distributeurs automatiques de billets ainsi qu'aux autocommutateurs et infrastructures de télécommunication, ont été les prémisses de cette nouvelle forme de criminalité de haute technologie. Internet n'est pas le seul porteur de ces potentialités criminelles. En effet, le GSM, les copieurs ou les imprimantes par exemple, comme toutes les technologies du numérique d'ailleurs, peuvent être détournées à des fins criminelles.

Internet au service de la criminalité

De par sa nature et ses caractéristiques, internet offre une couche d'isolation protectrice aux criminels. Ainsi, le fait de pouvoir localiser des serveurs dans des Etats faibles qui constituent des refuges à des opérations transnationales ainsi que le manque de régulation internationale et

de contrôle, offrent des avantages largement exploités par la criminalité. Le criminel tire, en outre, parti de l'a-territorialité de l'internet, de l'inexistence dans certains Etats de lois réprimant le crime informatique et des juridictions multiples dont relève le réseau des réseaux. A l'instar des paradis fiscaux, il existe des paradis numériques où un malfaiteur peut agir ou héberger des serveurs et des contenus illicites, en toute impunité.

La dématérialisation des transactions, les facilités de communication associées aux solutions de chiffrement, de stéganographie et d'anonymat, autorisent des liaisons entre criminels de différents pays sans contact physique, de manière flexible et sécurisée en toute impunité. Ainsi, ils peuvent s'organiser en équipes, planifier des actions illicites et les réaliser, soit de manière classique, soit par le biais des nouvelles technologies. La couverture internationale du réseau internet permet aux criminels d'agir au niveau mondial, à grande échelle et très rapidement.

D'autre part, la spécialisation, le haut degré de compétence économique et le professionnalisme nécessaire à la réalisation du crime économique, font que celui-ci peut être facilité par les technologies de l'information. Internet contribue ainsi à l'acquisition des informations, à une meilleure connaissance des marchés, lois, techniques, etc. nécessaires à la réalisation de délits économiques. Il sert également à l'identification des opportunités criminelles et des risques associés.
Dans ce contexte, le crime économique nécessite des compétences technologiques et un certain savoir-faire dans le monde numérique. Les criminels s'organisent autour de l'échange d'information grâce aux technologies de l'information. Des réseaux de personnes ou de compétences autorisant des organisations criminelles dématérialisées (notion d'équipes virtuelles) peuvent émerger. L'information, bien immatériel des nouvelles formes d'organisations criminelles, est alors au cœur des stratégies criminelles et des processus de décision. Les technologies de l'information deviennent un facteur de production et un élément de stratégie des organisations criminelles.

Par ailleurs, l'uniformisation du monde de l'informatique et des télécoms par l'adoption universelle des technologies internet, la dépendance des organisations et des Etats à l'égard de ces mêmes technologies et l'interdépendance des infrastructures critiques, introduit un degré de vulnérabilité non négligeable dans le fonctionnement normal des institutions. Cela peut mettre en péril leur pérennité ainsi que la souveraineté des Etats.

La généralisation de la mise en réseau des ressources informatiques et informationnelles fait que celles-ci deviennent des cibles attrayantes pour la réalisation de crimes économiques via les nouvelles technologies. Les différentes formes d'attaques informatiques existantes ont pour dénominateur commun qu'elles font courir relativement peu de risques à leur auteur et possèdent des conséquences négatives et des dommages potentiels bien supérieurs aux ressources nécessaires pour les réaliser. L'usurpation d'identité électronique ou la prise de contrôle d'ordinateurs par exemple facilitent la réalisation d'actions illégales.

La disponibilité d'outils d'exploitation des failles et vulnérabilité des systèmes, de bibliothèques d'attaques et de logiciels qui capitalisent le savoir-faire criminel dans un programme, offre des opportunités sans précédent. Cette disponibilité, associée à la dématérialisation des actions, facilite le comportement malveillant des informaticiens qui possèdent la fibre criminelle et des criminels qui possèdent des aptitudes en informatique. Le cyberespace facilite pour certains le passage à l'illégalité, sans parfois de prise de conscience réelle de la dimension criminelle des actes perpétrés.

Le crime informatique est un crime sophistiqué, réalisé le plus souvent au niveau international, avec parfois un effet à retardement. Dans le monde de l'informatique, les traces laissées par les malfaiteurs sont immatérielles. Elles sont généralement difficiles à collecter, à obtenir et à sauvegarder. Ce sont des informations numériques mémorisées sur toute sorte de supports : mémoire vive, morte, réinscriptibles, périphériques de stockage, de sauvegarde, disque dur, disquettes, clé USB, etc.

> « Les facilités de communication associées aux solutions de chiffrement autorisent des liaisons entre criminels de différents pays, de manière flexible et sécurisée »

> « La disponibilité d'outils d'exploitation des failles et vulnérabilité des systèmes, de bibliothèques d'attaques et de logiciels offre des opportunités sans précédent »

La trace numérique obtenue par perquisition informatique pose le problème de sa saisie : identification, localisation des données pouvant constituer une preuve, récupération dans divers supports informatiques ou composants électroniques, effacement de fichiers, de données, origine des messages, etc. Ces données sont d'autant plus difficiles à obtenir qu'elles sont laissées dans des systèmes ressortissants de différents pays. Leur obtention relève de l'efficacité de l'entraide judiciaire internationale et de la rapidité d'intervention. Leur exploitation efficace pour identifier des individus dépend de la durée de traitement de la requête d'obtention qui, hélas, peut mettre plusieurs mois, voire des années...

> « Il est très difficile de remonter jusqu'à l'identité d'une personne sur la seule base d'une trace numérique »

A supposer que la trace numérique soit collectée, il se pose alors la question de sa valeur en tant que preuve contribuant à établir la vérité auprès d'un tribunal (notion de preuve numérique). En effet, les supports de mémorisation sur lesquels des traces ont été recueillies sont faillibles. Ils peuvent introduire un taux d'erreur et un degré d'incertitude dont il faut tenir compte dans l'établissement d'une preuve numérique. De plus, les notions de date et d'heure sont variables d'un système informatique à l'autre et aisément modifiables.

Enfin, il est très difficile de remonter jusqu'à l'identité d'une personne sur la seule base d'une trace numérique, du fait qu'il est difficile d'établir une correspondance univoque entre une information numérique et son auteur, vu l'usage de l'usurpation d'identité.

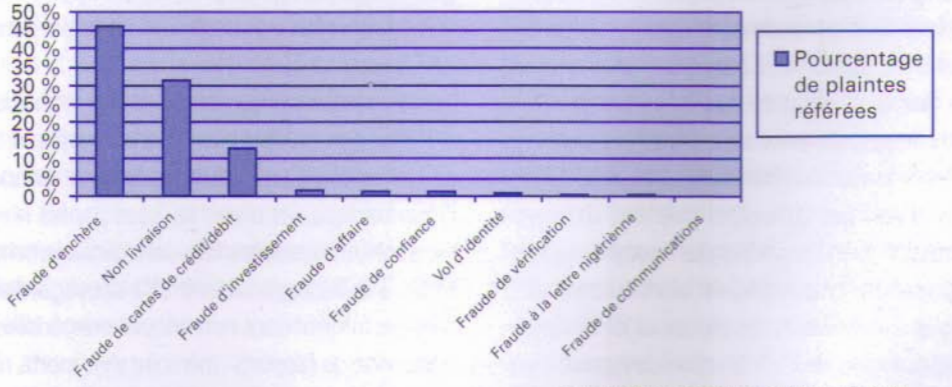
Les coûts associés à la cybercriminalité

Le cybercrime constitue, de plus en plus, la partie visible de la criminalité économique ou organisée. Il devient un véritable instrument de nuisance et de déstabilisation des organisations et des Etats. Grâce à l'informatique et aux télécoms, la fuite d'information, l'espionnage industriel et économique (très difficile à comptabiliser et très largement sous-déclaré), ainsi que l'industrie parallèle et très organisée de la copie à la chaîne de logiciels, de films, de musiques, etc., ont pris une tout autre dimension. Le copyright, le droit d'auteur, comme la violation du secret professionnel, de l'intimité numérique ou de la propriété intellectuelle, sont largement mis à mal par le biais des technologies du numérique. L'atteinte à la propriété, l'appropriation illégale de la propriété d'autrui, l'endommagement, la destruction de la propriété d'autrui ou l'immixtion dans la propriété d'autrui comme la dissémination de contenus illégaux, sont des délits présents et facilités par internet.

La **figure 1** présente, les dix premières catégories de plaintes enregistrées par l'Internet Fraud Complaint Center du National White Collar Crime Center (USA), durant l'année 2002 [Voir biblio. 2].

> « Le cybercrime devient un instrument de nuisance et de déstabilisation des organisations et des Etats »

Figure 1 • Dix premières catégories de plaintes enregistrées par l'IFCC en 2002



Issu de "IFCC 2002 Internet Report Fraud"

Les virus, spam, phishing(1), falsification de sites web, mais également le blanchiment des capitaux, l'évasion fiscale, la désinformation, la manipulation d'opinion, le chantage, la cyber propagande, la guerre psychologique ou de subversion, ne sont que quelques exemples d'expression de la criminalité. De nos jours, les virus n'ont plus pour objectif principal la destruction massive et gratuite de données. Ils deviennent pragmatiques et sont orientés vers la recherche de gains. Leur finalité est bien plus intelligente qu'à leur origine et leur capital embarqué leur permet de réaliser des fraudes. Les virus deviennent des vecteurs de réalisation de la criminalité financière au service, le plus souvent, de la criminalité organisée.

Pour ce qui concerne, par exemple, l'augmentation du spam et des nuisances associées, le CLUSIF(2) a relevé qu'AOL aurait filtré 500 milliards de messages de spam en 2003 et que le spammer le plus prolifique du monde (révélé en décembre 2003 par l'association anti-spam Spamhaus(3)) aurait envoyé 70 millions de messages électroniques en un seul jour ! [Voir biblio. 1].

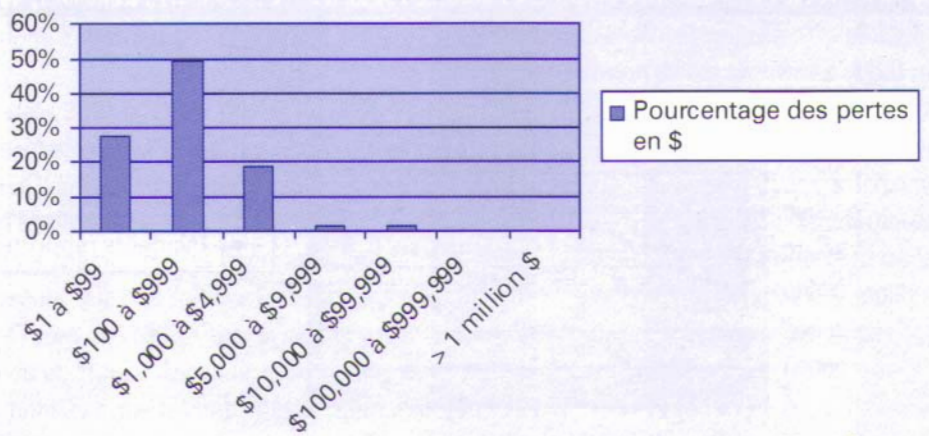
Toujours selon le CLUSIF, aux Etats Unis, en mai 2003 le "Buffalo spammer" a été condamné à payer une amende de 16,4 millions de dollars au fournisseur de service internet Earthlink, pour avoir envoyé 825 millions de messages non sollicités. Selon Ferris Research, le spam aurait coûté au monde des affaires en 2003, 2.5 milliards de dollars aux Européens et 8.9 milliards de dollars aux Américains. Ajouté aux 500 millions de dollars investis par les fournisseurs de service pour bloquer le spam, cet usage abusif de la messagerie électronique devient un véritable problème que l'on ne peut plus ignorer.
Les nouvelles technologies facilitent toute sorte de vol, modifications, sabotage d'information ou de fraudes.

> "AOL aurait filtré 500 milliards de spam en 2003"

Outre les pertes directes consécutives à une fraude, il faut considérer les coûts engendrés par une interruption de service, entraînant une non continuité des opérations, une perte de volume de ventes, des dommages collatéraux, la perte d'image, de réputation, etc., ainsi que les coûts relatifs à la restauration des systèmes dans leur état opérationnel. Cela représente des sommes non négligeables pour les organisations ciblées par des attaques informatiques.

48.252 cas ont été enregistrés par l'IFCC en 2002, dont 36.332 étaient relatifs à des pertes d'argent. Le montant total des pertes, toujours pour 2002, est de 54 millions de dollars contre 17 millions de dollars en 2001. L'IFCC présente une répartition des pertes exprimées en dollars en fonction du pourcentage des fraudes en 2002 (**Figure 2**).

Figure 2 • Répartition des pertes exprimées en dollars en fonction du pourcentage des fraudes en 2002



Issu de "IFCC 2002 Internet Report Fraud Report

> "Le montant total des pertes, pour 2002, est de 54 millions de dollars"

1/ Utilisation de la messagerie électronique pour leurrer et inciter les internautes à livrer des informations sensibles exploitées ensuite à des fins malveillantes.
2/ CLUSIF - Club de la Sécurité des Systèmes d'Information Français https://www.clusif.asso.fr 3/ Association Spamhaus : www.spamhaus.org

On constate que 28 % des pertes sont inférieures à 100$ et que 49,2% sont comprises entre 100 et 1000$. Ces chiffres révèlent que plus des deux tiers des pertes relatives à la criminalité informatique portent sur des montants faibles. Le facteur de proportionnalité entre la gravité des délits et la mise à disposition de moyens de protection, de dissuasion et de réparation nécessaires à la maîtrise de la criminalité, est déterminant. Ainsi, si l'on tient compte de la corrélation entre l'importance des délits et celle des mesures de protection à mettre en œuvre pour s'en prémunir, associé à la véritable difficulté technologique, organisationnelle, légale et économique de telles mesures, on peut comprendre la réalité de la cyber-crimialité actuelle.

> « Plus des deux tiers des pertes relatives à la criminalité informatique portent sur des montants faibles »

Le nombre d'incidents de sécurité rapportés au CERT(4) a grandement progressé depuis le début des années 2000, comme le montre la **figure 3**. De manière concomitante, le nombre d'attaques déclarées aux autorités judiciaires tend également à augmenter au cours des années, ce qui contribue à une meilleure connaissance et prise en compte de la criminalité informatique.

Délinquance et sécurité informatique

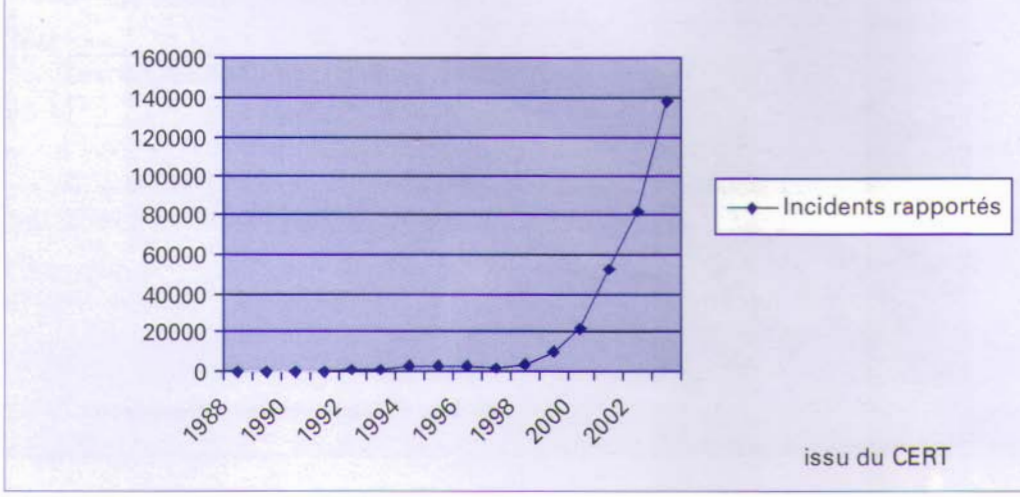
La délinquance informatique constitue une question complexe. La multiplicité des éléments matériels, logiciels, réseaux et des acteurs impliqués, comme l'inexpérience et l'inconscience de certains utilisateurs, favorisent l'expression de la criminalité informatique.

L'inadéquation plus que l'insuffisance des moyens de protection aux risques réels détermine un état d'insécurité ne permettant pas d'établir la confiance dans le monde numérique. Par ailleurs, même si les technologies de sécurité existent, elles peuvent être défaillantes, induire de nouvelles failles, générer de nouveaux risques, être incohérentes, avoir des implémentations complexes ou encore être contournées par des procédures parallèles. De plus, elles sont des réponses statiques à un problème dynamique, mais surtout des réponses d'ordre technologique à des problèmes humains, managériaux et légaux.

L'expertise des attaquants, la sophistication et l'efficacité des attaques, les boites à outils, les outils d'attaques ainsi que le nombre d'attaques, ne cessent de croître. De manière concomitante, on observe une diminution de la capacité des organisations à réagir assez rapidement aux événements majeurs ainsi qu'une maîtrise très relative de la complexité induite par les nouvelles technologies. Non seulement le nombre de personnes, de systèmes et d'organisations connectées à l'internet augmente, mais les infrastructures de traitement et de communication de l'information possèdent des failles intrin-

> « Les infrastructures de traitement et de communication de l'information possèdent des failles intrinsèques de sécurité »

Figure 3 • Evolution du nombre d'incidents de sécurité rapportés (de toute nature confondue) au CERT



4/ CERT Coordination Center, Carnegie Mellon University (http://www.cert.org)

sèques de sécurité, dont l'origine est à trouver dans leur conception ou leur utilisation. Ainsi, des produits vulnérables continuent toujours à être commercialisés.

Paradoxalement, Microsoft a promis, dès novembre 2003, une prime à quiconque pourrait fournir des informations conduisant à l'arrestation et à la condamnation d'auteurs de virus (notion de cyber Far West !). Cinq millions de dollars sont attribués à ce programme international auquel des acteurs comme Interpol ou le FBI, par exemple, sont associés.

Il est à constater que, sans une volonté et une responsabilité de tous les acteurs et un partenariat efficace des secteurs privés et publics, toute mesure de sécurité, qu'elle soit d'ordre technologique ou législative, ne constituera qu'une approche insuffisante et de peu d'efficacité pour la maîtrise de la criminalité informatique.

Pour une approche cohérente

Chaque technologie possède un risque intrinsèque et est porteuse de potentialités criminelles. Elle offre des opportunités de compromission, de fraude, de supercherie, de corruption ou d'escroquerie. Trois attitudes peuvent être adoptées face à un risque : l'ignorer, le transférer ou le maîtriser. A l'heure de la société de l'information, le risque informatique et sa composante criminelle ne peuvent plus être ignorés et l'idée de pouvoir le transférer est utopiste. Il reste donc à le maîtriser.

Les années 2003 et 2004 ont été marquées par l'augmentation significative du volume du spam, qui ne se limite plus à l'internet mais touche également les SMS, et par l'arrestation et la condamnation de spammers. Des opérations de police d'envergure, que cela soit aux Etats Unis (opération E-Con en mai 2003, Cyber-Sweep en octobre 2003) ou en Europe (Espagne, Italie, France, GB, etc.), montrent que les autorités réagissent et s'adaptent à ce nouveau contexte criminel. L'arrestation et la condamnation de quelques auteurs de virus ou de spam démontrent la volonté de restreindre ces nouvelles formes de nuisance. Toutefois, le nombre de condamnations reste très marginal au regard de l'importance quantitative du spam et des virus circulant journellement(5).

On constate qu'il existe un décalage significatif entre les aptitudes des criminels à effectuer des crimes de haute technologie et les moyens mis à disposition des forces de justice et de police pour les poursuivre. C'est généralement aux moyens courants d'investigation pour crimes conventionnels qu'ont recours les forces de justice et de police pour poursuivre les cyber criminels, qui sont identifiés et arrêtés par des moyens classiques. Le niveau d'adoption des nouvelles technologies par les instances de justice et de police aux niveaux national et international reste faible et très disparate d'un pays à l'autre. Bien que de plus en plus de lois soient votées pour combattre le crime informatique, des problèmes d'harmonisation des cadres légaux applicables au niveau international ainsi que la question d'une coopération internationale efficace restent posés.

> « Le niveau d'adoption des nouvelles technologies par les instances de justice et de police reste faible »

La convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001, identifie ces besoins et tente d'y apporter des éléments de réponse. Une solution opérationnelle à la problématique complexe et délicate qu'est la maîtrise de la cybercriminalité, nécessite une réponse globale, concertée et voulue par tous les Etats. Or des divergences importantes résident dans l'appréhension de ces problèmes et des moyens nécessaires à mettre en œuvre pour les résoudre. Les dimensions politiques, légales et économiques dans lesquelles ces questions s'inscrivent, laissent penser que la criminalité informatique et économique continuera à tirer parti de la difficulté à réguler le cyberespace, à appliquer des lois de manière transnationale, et des opportunités technologiques.

> « Des divergences importantes résident dans l'appréhension de ces problèmes et des moyens nécessaires à mettre en œuvre pour les résoudre »

Face à la synergie et à la convergence du crime organisé, du crime économique et du cybercrime,

5/ 85.059 virus connus ont été recensés en décembre 2003 par l'Information Technology Promotion Agency Information Security Center (IPA/ISEC - Japon) - "Computer Virus Incident Reports". 2004. http://www.ipa.go.jp/security/english/virus/press/200401/virus200401-e.html

une réponse complète, multilatérale et transnationale doit être apportée. Elle doit satisfaire aux besoins de sécurité nationale, de respect de la vie privée et à la protection de l'intimité numérique. Elle doit contribuer à limiter à un niveau acceptable la cybercriminalité, à établir la confiance dans le monde numérique, à minimiser le risque de corruption et de menace des pouvoirs publics et à faire en sorte que les nouvelles technologies et l'internet ne profitent pas uniquement au crime.

> “Une réponse complète, multilatérale et transnationale doit être apportée”

Solange Ghernaouti - Hélie

Bibliographie

[1] CLUSIF, An overview of cyber-crime -2003. https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CyberCrime2003.pdf

[2] The National White Collar Crime Center : "IFCC 2002 Internet Fraud Report", 2003

[3] The National White Collar Crime Center : "IFCC 2002 Six-Month Data Trends Report", November 2000