

Solange Ghernaouti-Hélie

LA
CYBERCRIMINALITÉ

Le visible et l'invisible



Presses polytechniques et universitaires romandes

1

INTRODUCTION

LA CYBERCRIMINALITÉ EST UN FLÉAU DE SOCIÉTÉ

Citoyens détroussés, enfants en danger, entreprises ruinées, Etats menacés, les cybercriminels étendent leur emprise en même temps qu'Internet se développe. Nous ne les voyons pas, nous ne les connaissons pas, nous ne nous en méfions pas et c'est leur force. Pourtant, nous sommes tous concernés. Qu'il s'agisse de manipulation d'opinion, d'espionnage, d'usurpation d'identité, de terrorisme, de harcèlement, d'escroquerie, de délinquance, de fraude financière ou de diverses formes de délinquance, la cybercriminalité touche la société dans son intégralité. En utilisant les différents services offerts par Internet, chaque internaute peut s'exposer à une menace d'origine criminelle et devenir la cible ou l'acteur, le plus souvent involontaire, d'un délit. La cybercriminalité est désormais une réalité comme le démontre l'actualité régulièrement depuis plusieurs années. Elle entraîne des conséquences plus ou moins importantes pour les individus, les organisations et les Etats.

Ainsi, par exemple, le site génération-net.com rapportait en septembre 2005 le cas d'une escroquerie ayant touché plusieurs centaines de victimes dont quelques-unes étaient suisses : « Tout a commencé suite à une plainte déposée en avril dernier par une victime habitant en Haute-Corse. Cette personne, ayant payé 580 euros d'adhésion à un club financier accessible sur Internet, a ouvert un compte pour y placer 130 000 euros. Ne voyant pas les intérêts promis par le club arriver, elle s'en est inquiétée et a fini par déposer plainte. Il aura fallu cinq mois d'enquête aux gendarmes spécialisés dans la délinquance économique et

financière de la section de recherche d' Ajaccio pour faire le lien avec un couple qui avait depuis fermé son site basé aux USA, laissant sans réponse les réclamations de plus de 700 personnes tant en France, qu'en Allemagne, en Espagne, en Belgique, en Suisse, aux USA ou au Canada. Accusés d'abus de confiance commis en faisant appel au public, ils auraient extorqué ainsi plus de 1,2 million d'euros. Il s'agissait d'un homme âgé de 23 ans, aidé de sa mère de 40 ans, qui proposaient avec la société New Import Club, via plusieurs sites Internet (libershop.com, liberto.com...) des contrats de placement financier avec des taux d'intérêt allant jusqu'à 28%. Ces contrats étaient, comme vous l'imaginez bien, tous faux.

Les technologies du numérique sont devenues des moyens de réalisation d'activités criminelles. Internet constitue désormais un vecteur privilégié de propagation de celles-ci, comme nous le verrons tout au long de cet ouvrage. Comme on pouvait le lire par exemple sur le site de la revue *Challenges* le 19.03.2009 : « Un employé de la Banque HSBC France détourne 900 000 euros... Sa méthode: après avoir "craqué" les sécurités du système informatique, cet homme de 36 ans a ponctionné ces sommes d'argent en organisant de faux virements sur des comptes bancaires appartenant à des complices qui lui servaient d'intermédiaires ».

Les plaintes suivantes, citées en exemple sur le site du Ministère de l'Intérieur français pour sensibiliser les internautes à être vigilants, sont courantes : « J'ai déniché une annonce sur un site proposant une voiture à un prix très attractif. Après plusieurs échanges avec le vendeur, j'ai reçu un courriel au nom du site définissant les modalités de paiement. Je ne me suis pas méfié et j'ai réglé le bien en passant par un service de transfert d'argent. En fait, c'est le vendeur escroc qui avait envoyé ce courriel ! L'argent a été retiré le jour même. Je n'ai jamais reçu le bien que j'avais payé. » Ou « J'ai reçu un courriel de ma banque me demandant mon identifiant de connexion et le mot de passe de consultation de mon compte en ligne. Ils m'avaient alors expliqué qu'ils avaient besoin de mettre à jour mes données de connexion. Le problème c'est que ce n'était pas ma ban-

que. Mon compte a été vidé.» (source : www.interieur.gouv.fr, 06.01.2009)

Trop souvent, la complexité de la technologie joue en faveur des cybercriminels. Mais cela n'est pas une fatalité. Même si les solutions de sécurité sont parfois faillibles, cet ouvrage expose qu'il est faux de croire que l'on est désarmé face à cette nouvelle criminalité. Largement illustré par des cas réels, il propose une synthèse claire de ce qu'est la cybercriminalité et la manière dont elle s'exprime. Il présente des clés pour apprendre à déceler les menaces, à connaître les comportements à risque et à repérer les multiples formes de cybercriminalité sur Internet. Il apporte également des réponses pragmatiques aux préoccupations des jeunes citoyens ou des personnes plus âgées qui utilisent de manière extensive ou épisodique Internet, à des fins privées ou professionnelles.

L'ouvrage est structuré après cette introduction en quatre chapitres indépendants qui peuvent être lus en séquence ou non.

Le chapitre 2 répond aux questions : Qu'est-ce que la cybercriminalité ? Comment s'exprime-t-elle ? Quels sont les risques et les menaces pour les individus, les organisations et les Etats ? Qui sont les cybercriminels ?

Le chapitre 3 identifie les raisons pour lesquelles les criminels se sont approprié Internet et propose des éléments de compréhension pour répondre aux questions suivantes : A qui profite le crime ? Pourquoi les solutions de sécurité sont-elles faillibles ? Qui est responsable de la sécurité ? Qui contrôle la sécurité ?

Le chapitre 4 traite de la problématique de la cybercriminalité et de ses conséquences pour les Etats, sous les angles de la dépendance, des conflits, de la guerre de l'information, des attaques informatiques majeures et du terrorisme.

L'avant-dernier chapitre propose un panorama des escroqueries en tout genre dont peuvent être victimes les individus et les organisations. Il aborde également les questions de la dignité des personnes et de l'identité sur Internet et offre des éclairages sur les peurs associées à l'usage d'Internet et aux réponses sécuritaires.

Quelques perspectives concluent cet ouvrage.