La cybercriminalité : une criminalité à géométrie variable

Daniel MARTIN*

Le concept de cybercriminalité n'est pas défini avec précision, et son champ d'action est extrêmement vaste si on veut bien considérer qu'il concerne toutes les actions délictueuses relevant du Code pénal et touchant, d'une manière ou d'une autre, l'usage des technologies de l'information et de la communication.

C'est ainsi que la fabrication de faux euros réalisée à partir de matériels informatiques entre dans les nouvelles formes de cybercriminalité, tout comme l'implantation de logiciels espions (*spywares*) dans les ordinateurs à l'insu de leurs propriétaires, ou encore les vols de numéros de cartes bancaires et leur usage abusif.

UN CONSTAT POSITIF, MAIS ALARMANT

Les nouvelles technologies de l'information et de la communication se vulgarisent de plus en plus, et le nombre d'internautes ne cesse de croître.

Pendant longtemps, la France a donné l'impression d'être le mauvais élève de la classe en matière de connexions à Internet. Se montrant d'abord très frileux face à l'usage des nouvelles technologies de la communication et de l'information, sans doute inquiets des informations alarmantes diffusées par les médias sur les risques du commerce électronique et les attaques informatiques, les Français étaient en retard.

L'autorité de régulation des télécommunications (ART), par l'intermédiaire de son Observatoire du marché de l'Internet, publie des indicateurs relatifs à l'activité des fournisseurs d'accès à Internet. Et les chiffres du deuxième trimestre 2004 montrent que la France comptait un peu plus de 11 millions d'abonnés à Internet fin juin.

Le plus surprenant est le bond effectué par l'Internet haut débit. Il

* Commissaire divisionnaire honoraire, rapporteur à la Cour des comptes, et expert auprès du Conseil de l'Europe.

Les conclusions et opinions exprimées dans cet article sont celles de l'auteur, à titre personnel, dans le respect de la liberté d'expression. Elles ne reflètent en aucune manière la position d'un service public, d'une administration gouvernementale ou d'une organisation internationale.

fait l'objet d'une croissance très rapide dans notre pays, en particulier grâce à des prix en forte baisse et à une couverture en constante progression. Sur 11 millions d'abonnés, on compte un peu plus de 6 millions pour le bas débit contre presque 5 millions de haut débit. Sur un an, le haut débit a pratiquement doublé le nombre de ses abonnés, et il est vraisemblable qu'il aura définitivement supplanté le bas débit dès la fin de l'année 2004.

C'est l'ADSL qui a la préférence des utilisateurs en couvrant 92 % des accès. La France se place ainsi au deuxième rang européen et au sixième rang mondial, le reste des connexions étant effectué via le câble.

Parallèlement, les matériels sont de plus en plus puissants, les logiciels de plus en plus performants, et les réseaux de plus en plus accessibles.

Mais tout n'est pas parfait. Si aujourd'hui le monde est disponible maintenant à partir de chez soi pratiquement en temps réel et sans limite, la médaille comporte un revers souvent méconnu : en contrepartie, cette fenêtre ouverte est également une porte d'accès en sens inverse aux données entreposées dans nos ordinateurs et sur notre vie privée.

Les paramètres habituels de notre vie quotidienne sont modifiés : les frontières géographiques ont disparu, les transactions se déroulent à la vitesse électronique, c'est-à-dire sans délai, et leur virtualité semble garantir une sorte d'anonymat. Dans le même trait de temps, nous continuons de vivre dans un cadre géographique déterminé avec ses limites physiques, nos démarches sont identifiées et nos actions bien concrètes. Territorialité et souveraineté priment dans le monde matériel. Il suffit de rappeler que nos lois et règlements s'appliquent dans l'espace et le temps pour démontrer les difficultés à faire face au monde criminel qui a compris les avantages des nouvelles technologies : rapidité, virtualité, extraterritorialité et anonymat.

DES VULNÉRABILITÉS AVÉRÉES

Les matériels utilisés peuvent recéler des failles contenues dans des composants défectueux ou encore réalisant des opérations non prévues initialement. Mais c'est surtout aux logiciels que l'on pense en matière de vulnérabilités. Périodiquement, des bugs, souvent importants, sont découverts, démontrant que nos données et nos fichiers sont accessibles, que nos moyens matériels peuvent être utilisés à notre insu. Tous les jours, les sites spécialisés alertent les utilisateurs sur de nouvelles failles jugées souvent critiques et qui touchent généralement le navigateur le plus utilisé au monde : celui de Microsoft. En matière de réseaux, la situation est tout aussi préoccupante : l'apparition du *Wi-Fi*, en apportant un confort indéniable grâce au sans fil, a fait naître de nouvelles possibilités d'intrusion et de captation d'informations. Les réseaux de France Télécom ne sont pas à l'abri des difficultés. Début novembre 2004, une anomalie logicielle localisée dans un équipement de traitement de la voix via Internet a gravement perturbé plusieurs milliers d'appels, notamment certains destinés à des services de secours qui n'étaient pas joignables.

Les moyens informatiques et les

réseaux ont envahi nos sociétés modernes, géantes et fragiles, qui travaillent à flux tendus. Les infrastructures critiques et vitales, celles qui permettent à une société organisée de fonctionner sans chaos, sont très nombreuses. On peut citer l'énergie, les communications, les services publics, les transports, les services financiers, la justice, les services de santé, l'approvisionnement en nourriture et marchandises, les prévisions météorologiques. Or, des informations sont disponibles pour porter atteinte à leur fonctionnement. On sait, par exemple, qu'au Royaume-Uni, les réseaux de fibre optique passent sous les rails des chemins de fer (d'ailleurs en mauvais état) et que les coupures volontaires sont susceptibles de provoquer des ruptures de service. De la même manière, les plates-formes logistiques de la grande distribution qui assurent l'approvisionnement des supermarchés sont loin d'être bien protégées ! Quand on voit ce que représente une simple panne des moyens informatiques de La Poste, interdisant aux clients toute opération sur compte, on imagine les conséquences d'une destruction simultanée des deux horloges atomiques qui gèrent la synchronisation des transactions.

Nous sommes donc bien vulnérables, tant au niveau des structures étatiques qu'au niveau des entreprises et des individus.

DES CHIFFRES DIFFICILES À OBTENIR

Mais comment mesurer cette vulnérabilité ?

Il n'est pas aisé de recueillir des chiffres significatifs en raison du caractère particulier des données. Les individus ne se rendent pas toujours compte du fait qu'ils ont été victimes d'intrusion ou de fraude. Les entreprises ne voient pas l'intérêt de clamer sur les toits leurs failles et le fait qu'elles aient fait l'objet de pénétrations avérées ; très mauvais pour l'image de marque et la cotation en Bourse. Il faut donc se fier aux statistiques des services judiciaires ou aux enquêtes en entreprises pour se faire une idée générale. En fait, ce qui est le plus intéressant, c'est de noter, d'année en année, les tendances et les pourcentages de progression. La cybercriminalité ne cesse de progresser, la situation empire d'année en année, mais on préfère que ces informations ne circulent pas pour ne pas faire fuir les utilisateurs.

Pour mesurer le phénomène, il faut se tourner vers les statistiques diffusées par les pays de culture anglo-saxonne.

Le Computer Crime and Security Survey, édité chaque année par le Computer Security Institute (CSI) en collaboration avec le Federal Bureau of Investigation (FBI) américain, fournit quelques précisions utiles.

Le palmarès

Les entreprises ayant participé à l'étude[1] indiquent qu'elles ont fait l'objet :

- d'attaques par virus dans 78 % des cas ;
- d'utilisation abusive du Net en interne pour 59 % ;

- de vols de portables dans 49 % des cas ;
- d'accès non autorisés aux informations dans 37 % des cas ;
- d'une pénétration des systèmes dans 39 % des cas ;
- de déni de service (ou saturation) dans 17 % des cas ;
- de vols d'informations dans 10 % des cas ;
- de fraudes financières dans 5 % des cas ;
- de sabotages pour moins de 3 % des cas.

Le classement est tout différent, si on tient compte des pertes subies.

Les conséquences des attaques par virus arrivent en tête, suivies par les attaques de saturation et le vol d'informations, loin devant toutes les autres formes d'attaques.

Une étude européenne menée par Andersen Europe concernant les instigateurs d'attaques révèle que celles-ci sont le fait :
- de collaborateurs internes pour 49 % des cas ;
- de pirates indépendants pour 41 % des cas ;
- d'entreprises étrangères pour 4 % des cas ;
- de concurrents pour 4 % des cas ;
- de gouvernements étrangers pour seulement 1 % des cas.

La même étude précise que les supports d'attaque sont :
- Internet dans 48 % des cas ;
- les systèmes internes pour 44 % des cas ;
- la numérotation à distance pour 7 % des cas.

En France, les statistiques d'activités de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (Befti) de la préfecture de Police font apparaître les principales infractions constatées :
- escroquerie pour 23 % des cas ;
- altération, modification, entrave, suppression pour 18 % des cas ;
- accès, maintien pour 14 % des cas ;
- contrefaçon pour 16 % des cas;
- Internet pour 12 % des cas ;
- divers (diffamation, atteinte à la personne, escroquerie, abus de confiance) pour 12 % des cas ;
- fichier nominatif (Commission nationale de l'informatique et des libertés - Cnil) pour 4 % des cas ;
- fraude téléphonique pour 1 % des cas.

L'IMPORTANCE DU FACTEUR HUMAIN

Un fait ressort de toutes les études et enquêtes pratiquées : dans la moitié des cas d'attaques ou de fraudes, on constate une complicité interne. Le mythe du pirate solitaire travaillant la nuit dans la pénombre d'une chambre d'étudiant pour des raisons ludiques est bien écorné ! Il faut chercher en interne la plupart des difficultés qui ressortent le plus souvent d'une mauvaise gestion des ressources humaines. Des complicités internes, volontaires ou involontaires, sont le plus souvent à l'origine des plus grandes attaques.

Les criminels informatiques sont aujourd'hui organisés et utilisent tous les moyens disponibles pour obtenir des informations susceptibles de leur permettre d'accéder aux données recherchées via ce qu'on appelle le *social ingeniering*.

UNE NOUVELLE FORME D'ARNAQUE

Le « Phishing »

Une nouvelle forme d'arnaque explose en ce moment sur le réseau. Il s'agit pour les escrocs d´accéder à des données personnelles, en vue de commettre ultérieurement des infractions en empruntant frauduleusement l'identité de leurs victimes.

Le mariage entre l'astuce humaine ou la technique du *social ingeniering* et la faille technique est redoutable.

L'internaute reçoit un e-mail qui paraît tout à fait officiel et qui n'attire pas la méfiance. Cet e-mail incite généralement à donner « *login* et mot de passe », mais aussi d'autres données personnelles. Le mal est fait.

En voici un exemple : « Cher client de la City. Les services techniques de la Citibank ayant actualisé le logiciel, nous vous demandons de suivre les indications suivantes pour confirmer vos données, votre accès au système pouvant être bloqué. Nous vous remercions de votre coopération. Un membre de Citigroup ».

Les victimes potentielles sont souvent invitées ensuite à cliquer sur un lien qui tombe sur une version trafiquée du site Web d'une société (souvent une banque). La victime mord littéralement à l'hameçon lancé par l'escroc, un peu comme à la pêche à la ligne, d'où le nom de *phishing*.

Au début du mois de mars 2004, la banque Internet australienne, Westpac, a dû prévenir en urgence des milliers de clients à propos d'un e-mail factice qui les incitait à divulguer leurs identifiants sur une fausse page. En janvier, ce sont plusieurs grandes banques britanniques comme Barclays, Citibank et Lloyds, ainsi que le système de paiement Paypal (groupe Ebay), qui ont été victimes de faits similaires, où là aussi un courrier, plus vrai que nature, était envoyé aux clients, les incitant à se rendre sur une page trompeuse. Les escrocs, bien informés et bons pirates, exploitaient une erreur d'affichage des URL du navigateur Internet Explorer.

Le phénomène a pris une telle ampleur qu'une association s'est créée pour observer les tendances et évolutions du *phishing*. Il s'agit de l'Anti-Phishing Working Group (APWG) fondée notamment par des banques, des cybermarchands et des institutions financières. Son dernier rapport indique que dans les premiers mois de l'année, les attaques par *phishing* se sont multipliées tout en gagnant en sophistication. On constate 163 % d'attaques en plus en février 2004 comparé à décembre 2004. Selon le rapport de février 2004, 282 nouvelles attaques ont été enregistrées, soit une augmentation de 60 % par rapport à janvier 2004. Dix nouvelles attaques quotidiennes sont signalées. Le secteur professionnel le plus touché est bien évidemment celui de la finance et des divers services financiers, mais c'est le géant des enchères en ligne Ebay qui est le plus visé et qui reste la cible préférée des *phishers*.

Les banques préviennent pourtant clairement leurs clients. Sur sa page d'accueil, on peut lire, par exemple pour la BNP : « Vos codes secrets sont strictement réservés à un usage personnel. Votre code secret multi-

média et votre code secret de carte bancaire sont confidentiels. Ne les communiquez jamais. Ni par oral, ni par écrit, ni par courrier électronique. En cas de doute, vous pouvez modifier votre code secret multimédia à tout moment. Ne le saisissez pas sans avoir vérifié que vous vous trouvez bien dans l'espace sécurisé de BNPParibas.net. Après avoir consulté vos comptes, déconnectez-vous en cliquant sur le bouton déconnexion ».

Mais force est de constater qu'entre 1 et 5 % des destinataires de ces messages falsifiés y ont répondu.

Il faut dire à leur décharge que ces messages ressemblent de plus en plus à des e-mails officiels, ce qui les rend d'autant plus difficiles à détecter, et on peut donc tomber facilement dans le panneau en l'absence de sensibilisation. D'autant que la méthode est de plus en plus sophistiquée.

Si, jusqu'à présent, le *phishing* se déroulait en deux temps : réception d'un e-mail incitant à ouvrir un lien vers une banque en ligne, puis renvoi à une copie du site de cette banque sur laquelle l'internaute est invité à déposer ses coordonnées bancaires, on vient de découvrir une nouvelle méthode encore plus subtile visant plusieurs banques au Brésil : Banco do Brasil, Bradesco, Caixa Economica Federal, HSBC, Itau et Unibanco.

Plus besoin d'aller consulter le faux site de la banque. À la seule lecture de l'e-mail initial, un logiciel intrusif s'installe alors automatiquement et de manière invisible sur le poste de l'internaute. Ce programme peut alors enclencher deux types de processus : ouvrir directement et indépendamment de toute autre manipulation par l'internaute la fausse page imitée du site d'une banque en ligne, donc sans que l'internaute ait à cliquer sur un lien ; ou encore, et c'est là le point le plus dangereux, renifler les « favoris » de l'internaute, repérer les liens relatifs à une banque et lorsque l'utilisateur souhaitera y accéder, lui substituer la page détournée à la vraie page.

Deutsche Bank AG et Postbank AG, deux des principales banques allemandes, ont également fait l'objet de multiples attaques par *phishing*. En raison de la synchronisation des attaques, les services de police pensent que ces attaques proviennent d'organisations criminelles internationales.

La Suisse n'est pas en reste. En 2003, des escrocs rusés avaient conçu un site qui imitait celui de la Banque nationale suisse (BNS), à la différence près que le site pirate se terminait en « .org » au lieu de « .ch ». Et, contrairement au site original de la BNS, il proposait des services bancaires en ligne.

Ces services purement virtuels permettaient aux criminels de récupérer les adresses électroniques des visiteurs à qui ils offraient « des bénéfices de 40 millions de francs suisses (26 millions d'euros) contre le versement d'une avance de 1 000 francs suisses ».

Les techniques du *phishing* se partagent sur le Net entre *hackers*. Sur certains sites pirates, il suffit de se déclarer (créer une identité et un mot de passe) pour accéder librement aux lignes de code, voire même à des applications construites fournies librement, pour accéder aux technologies et à la panoplie du pirate en ligne. Les vrais pirates informatiques sont peu nombreux, mais leur comportement est de plus en plus mafieux.

Au Brésil, haut lieu de « l'hacktivisme », la police annonce avoir arrêté plus de 50 personnes soupçonnées de pillages de comptes bancaires en ligne. Environ 30 millions de dollars auraient ainsi été dérobés aux clients de ces banques.

Avec le *phishing*, c'est toute la fiabilité et la sécurité des transactions commerciales et des communications qui sont en cause. Avec plus de rigueur et une méfiance exacerbée, ajoutées à des produits mieux verrouillés, on devrait pouvoir faire face à cette nouvelle vague qui, n'en doutons pas un seul instant, sera suivie par d'autres tentatives. L'intelligence et l'imagination des truands sont inépuisables, mais, heureusement, celles des corps constitués qui luttent contre toutes les formes de criminalité le sont tout autant.

Mais les vieilles techniques marchent encore.

LES VIEILLES TECHNIQUES

Racket ou chantage à la réputation

Le National Hi-Tech Crime Unit de Scotland Yard cherche depuis plusieurs mois à démanteler de vastes réseaux d'escrocs menaçant d'extorsion plusieurs bookmakers anglais officiant sur Internet.

Selon Silicon.com, spécialisé dans le domaine de la sécurité informatique, le site de paris en ligne, Blue Square, a reçu la menace suivante : « Soit tu paies (7 000 euros pour commencer), soit on organise une campagne de spam avec des e-mails identifiés en @bluesq.com qui feront la promotion de sites pédophiles. Et après, accessoirement, on te sature ton site par déni de service ».

Le vol de numéros de cartes bancaires

Encore dernièrement, 5 millions de numéros de cartes bancaires ont été volés par un pirate informatique : 2,2 millions de numéros MasterCard et 3,4 millions de cartes Visa. Le FBI mène toujours l'enquête. Même si aucun compte n'a, semble-t-il, été utilisé pour faire des transactions frauduleuses, les organismes bancaires qui gèrent les comptes compromis sont contraints de changer tous les numéros pour éviter à leurs clients de se voir amputer d'une forte somme d'argent.

Les lettres nigérianes

Après les courriers classiques, puis les fax, des Nigérians, se faisant passer pour de hauts dignitaires, ont inondé nos boîtes aux lettres électroniques de messages[2] alléchants demandant aux réceptionnaires de bien vouloir les aider à transférer hors de leur frontière des sommes importantes avec une commission conséquente en guise de récompense. Il s'agissait bien sûr d'une escroquerie internationale. Le pactole est factice, et les sommes avancées pour divers frais de dossier perdues définitivement (une des victimes a perdu plus de 200 000 euros !).

Les autorités américaines, via le FBI, tout comme les services canadiens, ont considéré la menace tellement importante qu'ils ont ouvert un site spécial

pour recueillir les plaintes et des informations susceptibles de remonter jusqu'aux escrocs. Escroquerie d'ailleurs toujours bien montée car les noms, les numéros de téléphone transmis et les références bancaires étaient tout à fait vérifiables par les particuliers appâtés par le gain virtuel. Nul doute que les escrocs bénéficiaient de complicités locales plus ou moins importantes.

La police berlinoise vient de mettre la main sur l'un de ces escrocs d'une manière rocambolesque. Ce dernier, qui s'était vu confisquer par les douanes, à son retour de Suisse, la somme de 50 000 euros en liquide, est tout simplement venu réclamer son dû aux policiers qui se sont tout de même émus de voir un individu bénéficiant de l'aide sociale transporter de telles sommes en liquide. L'intéressé n'a pu fournir aucune explication plausible. Une perquisition à son domicile a alors permis de saisir plusieurs éléments permettant de penser à une escroquerie internationale de grande envergure.

Malgré tout, ces courriers continuent de proliférer sur Internet et sont en provenance de l'ex-Zaïre, d'Afrique du Sud, ou encore du Nigeria, et certains se laissent encore prendre dans ce « pot de miel ».

Le danger de la prolifération de ces messages par Internet réside dans le nombre de gens touchés simultanément, qui est de l'ordre de plusieurs centaines de milliers à la fois. Si seulement 1 % des sondés répondent favorablement, cela représente déjà plusieurs milliers de victimes et des sommes considérables en jeu. Internet permet cette multiplication sans aucun frais !

Les astuces bricolées

Elles marchent toujours aussi bien, si on en croit les affaires qui défraient fréquemment la chronique. Après le « collet marseillais », sorte de piège primaire qui permettait aux délinquants de récupérer les cartes bancaires coincées dans les distributeurs automatiques de billets, voici le mariage de la caméra numérique et des liaisons radios. Plusieurs automobilistes se servant à des pompes automatiques ont eu la désagréable surprise de voir leur compte débité à l'étranger de sommes qu'ils n'avaient jamais dépensées. L'ensemble des données était récupéré par duplication dans le lecteur de cartes de la pompe et les combinaisons de code secret repérées à partir d'une caméra cachée. Les images étaient ensuite transmises à des complices qui fabriquaient de fausses cartes et qui les utilisaient à l'étranger. Pendant la période des vacances, rien de plus normal. Le pot aux roses a éclaté à la rentrée.

LE CYBERTERRORISME

Le cyberterrorisme représente une menace spécifique et méconnue.

On a pu pendant des années imaginer un Pearl Harbor électronique avec la suppression simultanée de tous les services automatisés. Depuis le 11 septembre 2001, on pense plutôt que cyber et terrorisme sont des concepts qui s'opposent. En effet, le terrorisme a besoin de sang et de victimes, d'images fortes, pour créer la terreur, alors que le monde cyber est virtuel et indolore. On sait aujourd'hui que les réseaux

sont un excellent vecteur de prosélytisme pour les terroristes et qu'ils utiliseront plutôt les moyens informatiques pour désorganiser les secours, interdire ou contrecarrer les communications : en un mot, augmenter l'effet de panique d'attentats matériels et donner à la crise une force encore plus grande. Il n'empêche que les infrastructures des États modernes sont très dépendantes des moyens d'automatisation, et que cet aspect de la protection ne peut pas être négligé par les services publics.

LE CAS PARTICULIER DU FINANCEMENT DU TERRORISME

Le 11 septembre 2001 a mis aussi en lumière les implications financières internationales dans le terrorisme. Depuis plusieurs années, le Groupe d'action financière sur le blanchiment de capitaux (Gafi), abrité au sein de l'Organisation de coopération et de développement économiques (OCDE), luttait déjà contre le blanchiment d'argent sale. Cet organisme a mis en œuvre des recommandations spéciales pour refuser aux terroristes et à ceux qui les soutiennent l'accès au système financier international[3].

De plus en plus, les établissements financiers seront amenés à effectuer de véritables missions de police en tentant de détecter, dès l'origine, des mouvements suspects et de les signaler. Ces transferts ne sont pas sans poser de problèmes, et il semble que seul le retour sur information permettra de faire vivre le système. Pour avoir de bons correspondants, ceux-ci ont besoin d'évaluer leur information par retour. Sinon, le système risque de s'embouteiller et de rester inefficace. De nouvelles fonctions et de nouveaux métiers apparaissent, liés à la déontologie et au respect de l'éthique. Mais un autre problème est apparu, celui du noirciment de l'argent propre. Comment contrôler que l'argent récolté dans les mosquées à titre tout à fait louable ne va pas servir à acheter des armes et à fabriquer des bombes ?

Les éléments de riposte

Comment lutter efficacement contre ces nouvelles formes de criminalité qui allient techniques et astuces et qui, le plus souvent, se caractérisent par un aspect international ?

Les ripostes s'organisent autour de plusieurs pôles.

Le pôle national

L'arsenal judiciaire répressif national est bien doté. Les textes existent et sont appliqués, même si les moyens sont encore limités pour faire face à une augmentation certaine de cette nouvelle forme de criminalité. Le ministre de l'Intérieur vient d'annoncer que la lutte contre la cybercriminalité représentait l'une des priorités de l'État, et que les moyens humains et budgétaires allaient être doublés dans les prochains exercices.

En raison du caractère souvent international des affaires traitées, la coopération internationale est indispensable.

Le pôle international

Deux éléments récents méritent d'être soulignés.

Convention du Conseil de l'Europe de lutte contre la cybercriminalité

Cette convention est entrée en vigueur depuis le 1er juillet dernier. Elle change totalement la donne dans le domaine.

Adopté dès le mois de novembre 2001 à Budapest après plus de quatre années de concertation, ce texte, premier du genre, consacré aux infractions pénales commises notamment via Internet et d'autres réseaux informatiques, va enfin être appliqué. Il suffisait, en effet, que cinq pays le ratifient. C'est chose faite avec la Croatie, l'Albanie, l'Estonie, la Hongrie et la Lituanie. La France a signé ce traité, mais ne l'a toujours pas ratifié à ce jour.

À noter que le Conseil de l'Europe a ajouté, en 2002, au texte initial, pour le compléter, un protocole additionnel comportant plusieurs mesures destinées à prévenir et à lutter contre la haine raciale, le racisme, la discrimination et la xénophobie sur Internet.

Ce premier traité international spécifique au cyberespace s'articule autour de trois axes essentiels :
- l'harmonisation des législations nationales dans ce domaine ;
- la définition des moyens d'enquête et de poursuite pénale ;
- la mise en place d'un système rapide et efficace de coopération internationale.

La tâche était difficile, car il s'agit, à la fois, de permettre aux États de combattre la criminalité, de respecter les droits des individus à la protection de la vie privée, de veiller aux intérêts économiques des industriels du secteur, tout en garantissant la sécurité des réseaux de communication.

Le texte est original dans la mesure où il fixe des grandes lignes directrices fondamentales que chaque État signataire s'engage à faire passer dans son droit positif en fonction de sa propre culture, donc en respectant les critères locaux.

Il ne s'agit pas de mettre Internet sous cloche et de l'enfermer dans un carcan de réglementations. Pour que la liberté de chacun puisse s'exprimer, il est devenu indispensable d'établir une règle du jeu commune pour que cet espace de liberté ne se transforme pas en un univers à la Mad-Max où règne la loi du plus fort et où le crime organisé prolifère. Blanchiment d'argent, financement de réseaux terroristes, pédophilie... sont autant de délits qui se servent des supports des nouvelles technologies. Comme pour les actes de piraterie maritime des siècles précédents, un accord de principe sur des éléments de base était indispensable. Cette convention est le maillon qui manquait.

Les lignes directrices de l'OCDE

Comme déjà souligné, la sécurité des systèmes d'information qui envahissent notre vie quotidienne et qui gèrent nos infrastructures vitales comme l'énergie, les transports, les communications, ou encore les services publics, ou les réseaux financiers, est encore loin d'être au niveau souhaitable pour garantir un fonctionnement durable sans faille.

L'OCDE qui regroupe les trente pays les plus industrialisés de la planète a toujours été très sensible sur ce sujet et a d'ailleurs publié, dès 1992, avec une mise à jour en 1997, des lignes directrices relatives à la protection des systèmes et réseaux d'information. Ces lignes directrices ont fait l'objet d'une actualisation en novembre 2002 qui s'apparente plus à une nouvelle vision qu'à une simple mise à jour d'un secteur qui se renouvelle très rapidement.

L'OCDE veut créer un électrochoc au sein des pays membres pour que la sécurité soit enfin prise au sérieux.

Il est enfin admis qu'aucune solution miracle ne viendra faire disparaître les pirates ou encore les virus et autres chevaux de Troie, et qu'il va falloir vivre avec ces menaces. Faire face, c'est avant tout changer de mentalité et d'attitude chez l'ensemble des utilisateurs, en prenant en compte la sécurité comme l'élément central et essentiel des systèmes et réseaux modernes.

Les nouvelles lignes directrices s'intitulent avec beaucoup d'ambition : « Vers une culture de sécurité ». Elles mettent l'accent sur une vision globale de la sécurité, sur la nécessaire sensibilisation et responsabilisation des dirigeants et de tous les acteurs concernés, mais aussi sur la coopération, seule arme capable au niveau international de répondre aux incidents de sécurité dans ses aspects de prévention, de détection et de réaction.

Ces bonnes résolutions auraient pu rester à l'état d'intentions.

Il n'en est rien. Et l'OCDE persiste et signe en ouvrant un site Internet spécialisé[4] qui a pour vocation de lutter contre les risques sécuritaires menaçant nos systèmes et réseaux d'information, en diffusant les meilleures pratiques mises en œuvre par les pays membres.

Dans un premier temps, ce site présente les principales initiatives prises par plusieurs des pays membres pour répondre aux lignes directrices. Au fur et à mesure de l'avancée du concept, il prendra en compte dans les bases de données toutes nouvelles informations pertinentes. Ce site ne se contentera pas d'abriter uniquement des initiatives nationales. Il devrait également centraliser des outils éducatifs dans le domaine spécialisé de la sécurité des systèmes et des réseaux d'information, et ainsi répondre au nécessaire effort de formation qui doit accompagner toute sensibilisation.

Pour l'heure, la France se distingue par son absence et n'a encore transmis aucune information pour alimenter le site. On peut espérer au moins qu'elle mettra en œuvre, comme les autres pays membres de l'OCDE, les mesures adéquates susceptibles d'améliorer la sécurité de nos propres systèmes et réseaux d'information.

Mais ce sujet sensible ne peut rester la seule préoccupation des services publics ou des organisations internationales. Le monde de l'entreprise est en première ligne.

LE MONDE DE L'ENTREPRISE ET LA COOPÉRATION PUBLIC-PRIVÉ

Les entreprises doivent faire face à ces nouveaux défis. Il s'agit de prendre la menace au sérieux et de considérer

la sécurité comme une dimension souveraine à part entière. Il convient d'abord de sensibiliser les personnels et l'ensemble des utilisateurs, d'élaborer une vraie politique de sécurité, une charte d'utilisation des TIC (techniques d'information et de communication), de mettre en place des plans de sauvegarde et de reprise, tout comme des cellules de crise.

La sécurité ne peut plus être considérée comme une dépense, mais plutôt comme un investissement destiné à garantir la survie de l'entreprise. Nous n'en sommes pas encore là, mais il est certain que, dans ce domaine, une coopération public-privé est absolument nécessaire.

Des progrès sont cependant réalisés. Pour les États-Unis, l'étude du CSI, déjà mentionnée plus haut, indique que 99 % des entreprises ayant participé à l'enquête sont dotées de logiciels antivirus, 98 % de pare-feux, que 71 % contrôlent l'accès aux serveurs, que 68 % ont des détecteurs d'intrusion, que 64 % utilisent le cryptage des données en transit, 35 % des mots de passe à usage unique, et 11 % des moyens biométriques d'identification. En France, malheureusement, il faut encore se battre pour garantir les mises à jour périodiques des logiciels antiviraux et le bon paramétrage des *firewalls*.

L'AFFAIRE DES ASSOCIATIONS, DES ONG ET DES CITOYENS

Au-delà des entreprises, la prise de conscience devrait toucher tous les secteurs de la société, car nous sommes tous vulnérables.

Si le nombre d'internautes ne cesse de croître avec des moyens matériels et logiciels toujours plus puissants, la National Cyber Security Awareness (NCSA), une association américaine, qui s'est fixée pour mission d'alerter l'opinion, de faire prendre conscience des risques et de permettre aux particuliers de tester la sécurité de leurs ordinateurs, vient de publier une étude qui permet de se faire une idée précise de la perception par les utilisateurs des risques encourus par l'usage en ligne de ces moyens.

Alors que plus de 185 millions d'Américains possèdent un ordinateur connecté à Internet, plus de 30 % de ceux-ci, et près de 40 % des moins de 25 ans, se croient largement à l'abri des attaques virales, des intrusions et des atteintes possibles à leur vie privée. Selon eux, la probabilité de gagner à la loterie ou encore d'être frappé par la foudre est plus élevée que d'être victime d'un incident informatique ou d'une faille de sécurité.

Or, la dure réalité est là pour les contredire : alors que la probabilité d'être victime d'une brèche de sécurité informatique est de 7 sur 10 (soit 70 % !), celle de gagner le gros lot à la loterie aux États-Unis est de 1 chance sur 135 millions, et celle d'être frappé par la foudre de 1 sur plus de 980 000.

La perception des risques est donc encore très loin de la réalité. Un travail immense de sensibilisation est indispensable pour garantir un minimum de tranquillité en utilisant les NTIC (nouvelles techniques d'information et de communication). On peut penser légitimement que la situation dans le monde, et particulièrement en Europe, n'est guère plus brillante.

La seule solution consiste à poursuivre avec persévérance l'information des consommateurs qui, en règle générale, ne se réveillent qu'une fois victime.

Le site Web du NCSA (StaySafeOnline.info) fournit la liste des dix meilleurs conseils de base à mettre en pratique si possible avant toute attaque :

- utiliser un logiciel antivirus, et ne pas oublier de le maintenir à jour ;
- installer un pare-feu bien paramétré pour éviter les intrusions ;
- choisir des mots de passe difficiles à deviner ;
- ne pas ouvrir les courriels ou les fichiers joints, si la source est inconnue. Prudence même si le message semble émaner d'un correspondant connu ;
- penser à télécharger périodiquement les mises à jour et les sécurités des logiciels utilisés ;
- sauvegarder régulièrement les données sur support amovible ;
- ne pas partager son ordinateur avec des étrangers, et se méfier des échanges de fichiers ;
- déconnecter son ordinateur d'Internet lorsqu'il n'est pas utilisé ;
- vérifier la sécurité de son système au moins deux fois par an ;
- s'assurer que l'entourage sait ce qu'il doit faire en cas d'infection de l'ordinateur.

Si l'utilisation des TIC rend des services inestimables dont on ne saurait plus se passer aujourd'hui, elle engendre de nouveaux risques et de nouvelles vulnérabilités. La dimension des difficultés est planétaire et non plus simplement locale ou régionale. Les organisations internationales sont saisies du sujet. Elles sont si nombreuses et défendent souvent des intérêts contradictoires qu'il paraît bien improbable qu'elles soient en mesure d'apporter dans des délais raisonnables des solutions pratiques aux difficultés qui se présentent au quotidien, en particulier aux entreprises et à la société civile. En fait, le problème principal repose sur le facteur humain et non pas sur les paramètres techniques toujours triviaux. La coopération est indispensable entre les cultures différentes et complémentaires, afin d'aboutir à un *modus vivendi* acceptable par tous.

Tous les maillons de la chaîne doivent concourir au respect d'une déontologie librement consentie.

Le respect de nos libertés et de notre vie privée, la lutte contre la cybercriminalité, ce n'est pas seulement le problème des autres, des organisations internationales, de nos représentants, ou encore d'organismes de contrôle ou d'autorités administratives, c'est bien l'affaire de chacun d'entre nous et de notre motivation profonde !

Comme le disait déjà Thucydide cinq siècles avant notre ère, « La sécurité de la cité tient moins à la solidité de ses fortifications qu'à la fermeté d'esprit de ses habitants ».

Notes

1. Chiffres et étude disponibles sur le site du CSI.

2. Si vous recevez ce type de lettre, n'hésitez surtout pas à le signaler sur les sites du FBI (www.ifccfbi.gov ou plus simplement sur www.fbi.gov où toutes les arnaques sont bien démontées) ou sur celui des autorités canadiennes en adressant un courrier à walf@phonbusters.com. Les divers services de la police judiciaire française restent également à la disposition des citoyens pour recueillir les éventuelles plaintes.

3. Voir à ce propos le site spécialisé du Gafi : www.oecd.org/faft/index.

4. www.oecd.org/sti/cultureofsecurity.