# LA CYBERCRIMINALITÉ : UNE MENACE RÉELLE

DANIEL MARTIN*

## UNE NOUVELLE DONNE

On ne rappellera jamais assez combien le monde a changé, perdant en peu de temps ses repères.

Chute du Mur de Berlin, effondrement de l'Union soviétique, réunification des deux Allemagnes, indépendance des banques centrales vis-à-vis du pouvoir politique, guerre du Golfe, arrivée de l'euro, autant de chocs illustrés par une dure réalité : les anciens ennemis sont devenus des partenaires alors que dans le même trait de temps, les alliés traditionnels sont maintenant des concurrents féroces qui ne se font aucun cadeau.

Aujourd'hui, grâce aux moyens de stockage et de traitement de l'information (PC toujours plus puissants, logiciels performants), grâce à l'amélioration des communications (satellites, fibre optique, réseaux, Internet, etc.) et à la démocratisation de l'accès à ces moyens, on est pratiquement parvenu à supprimer toute notion de distance et de temps. Tout se passe en temps réel à la vitesse électronique. On peut dire que presque tout est disponible sur tout.

Les forces économiques et les facteurs technologiques favorables à la mondialisation ont un développement accéléré. L'innovation dans les télécommunications et les technologies de l'information est toujours en pleine progression. La baisse du coût des communications et des transports favorise les échanges.

On assiste en fait à la conjugaison de trois révolutions simultanées : une révolution technologique par le développement des technologies de la communication, une révolution géographique par la création de nouveaux marchés pour les entreprises, une révolution financière par la mondialisation des flux de capitaux et de la gestion de l'épargne.

Cette nouvelle ère mondiale où la concurrence touche tous les domaines : économiques, politiques, financiers, sociaux, linguistiques, consacre le rôle primordial de l'information, de la connaissance et de l'intelligence. On peut dire que nous sommes entrés dans l'âge de l'information.

Une situation où tous les coups sont permis pour obtenir des marchés, absorber un concurrent, détourner un client, connaître les stratégies adverses, intoxiquer, désinformer.

Dans ce nouveau contexte, notre société est devenue particulièrement vulné-

* Commissaire divisionnaire de la Police nationale, actuellement détaché auprès de l'Organisation de coopération et de développement économiques (OCDE) où il exerce, depuis 1992, les fonctions de Chef du Service d'assistance et de protection. Expert international reconnu en matière de cybercriminalité, il a créé et dirigé le Département des systèmes d'information de la Direction de la surveillance du territoire (DST).

rable. A la fois au niveau des pouvoirs publics par les failles relatives aux infrastructures sensibles, mais aussi et surtout au niveau des entreprises où le risque informatique devient le danger numéro un, sans oublier le niveau des citoyens dont les droits fondamentaux peuvent être violés particulièrement dans leur vie privée ou comme consommateur. Et tout ceci, peut-être même sans s'en rendre compte, car nous abordons un monde virtuel.

En matière d'informatique et de communication, la rapidité d'exécution des instructions réalisées à la vitesse électronique, la confidentialité assurée grâce au cryptage des données numériques et l'immatérialité des transactions qui protègent l'anonymat favorisent la progression de l'utilisation criminelle de ces moyens.

Cette progression s'est déroulée en plusieurs étapes et a collé étroitement à l'évolution des moyens de traitement de l'information.

Piratage de logiciels et contrefaçon des cartes de crédit ont marqué la période de banalisation de l'informatique des années 1970 à 1980.

L'émergence des réseaux locaux et des connexions qui les relient entre eux a engendré, à partir de 1980, les grandes affaires de détournement de fonds et l'apparition des *hackers* qui n'hésitaient pas à s'attaquer à la NASA ou au Pentagone.

L'informatique distribuée et la prolifération des systèmes d'information des années 1990 puis l'explosion Internet ont ouvert l'ère du monde virtuel et immatériel propice à toutes les formes de criminalité.

## L'ÉMERGENCE D'UNE CRIMINALITÉ DE HAUTE TECHNOLOGIE

Le piratage constitue le principal vecteur des actes criminels et représente le danger le plus inquiétant[1]. C'est un phénomène qui n'est pas récent mais dont la prolifération est préoccupante. Hier réservé à une élite, il s'est démocratisé et est aujourd'hui à la portée de n'importe qui possédant un micro-ordinateur raccordé à l'Internet car de multiples outils assurant le *hacking* sont accessibles sur le réseau.

Le piratage ou *hacking*, c'est quoi ?

Il s'agit en fait de l'action d'accéder et/ou de se maintenir frauduleusement dans un système d'informations, de prendre connaissance des logiciels, des fichiers, des données, éventuellement d'altérer le fonctionnement du système, de supprimer ou de modifier des données, d'y introduire des virus, vers, bombes logiques, chevaux de Troie[2].

Le *hacking* n'est pas qu'un sport cérébral permettant de partir à l'aventure sur les réseaux informatiques : discussions, recherches de nouvelles machines, intrusions, exploitations, créations de nouveaux outils..., sans avoir à payer les communications téléphoniques ni les communications réseaux.

Il existe de véritables gangs organisés possédant une structure internationale et dont les motivations, nullement ludiques, vont de l'appât du gain à l'espionnage industriel ou militaire

Toutes les méthodes sont bonnes : pénétration dans les locaux pour voler disquettes, listings, badges, cartes ; relevés de procédures de connexions, vols de mots de passe ; recrutement de personnels informaticiens, dépôts de programmes pièges, mise en place de stagiaires, étudiants, techniciens de maintenance ; branchements clandestins, captation de signaux parasites. Les armes sont multiples et variées : outre les vers, virus, chevaux de Troie, bombes logiques déjà cités, on peut rajouter aussi les trappes et composants ou logiciels trafiqués[3]. Saturation des circuits, armes HERF (*High Energy Radio Frequency*), bombes EMP (*Electromagnetic Pulse*) capables de porter des dommages à tous les équipements électroniques dans le périmètre de l'explosion constituent les risques futurs.

Et nous ne sommes pas dans la science-

fiction : le 9 septembre dernier, à Washington, lors de la conférence Infowarcom 99, pour la première fois, un canon de fréquences radios à très haute énergie (HERF) a fait l'objet d'une démonstration publique. Tous ses composants proviennent de produits accessibles dans le commerce. Les méthodes et plans pour sa fabrication ont été trouvés à partir de sources ouvertes. Ce canon parvient à détruire à distance la plupart des centres électriques existants.

A la même époque, une nouvelle a vite fait le tour des milieux spécialisés. Sur un serveur Internet, on a pu découvrir les messages émis par le Service de sécurité du Président des Etats-Unis.

Mais l'œuvre des pirates ne s'arrête pas là. Les Départements ministériels sont tous visés.

Le *Department of Defense* des Etats-Unis dispose de plus de 2 millions d'ordinateurs et gère 100 000 réseaux locaux en plus d'une centaine de réseaux longue distance. Le FBI considère que les systèmes de la Défense font l'objet de 250 000 attaques chaque année. Selon un office spécialisé du Sénat des Etats-Unis, 162 500 auraient réussi !

Une enquête menée par l'Agence nationale de sécurité (NSA) aurait mis en évidence la possibilité de rendre inopérant, par un acte de piratage, le commandement américain pour le Pacifique dont relèvent près de 100 000 hommes, et de couper en quelques jours le réseau électrique américain.

Les dernières statistiques pour les attaques de sites informatiques militaires sont édifiantes. Elles réussissent dans 88 % des cas, seulement 4 % des sites attaqués ont repéré ces attaques et moins de 0,5 % ont donné lieu à un rapport.

## FLORILÈGE D'ATTAQUES

Dès qu'un ordinateur est connecté sur un réseau, on sait que la liaison mise en place marche dans les deux sens et donc que des pénétrations sont possibles.

Le chargé de mission pour la sécurité des données du Pentagone a reconnu dernièrement que des rebelles mexicains de la guérilla zapatiste avaient attaqué en 1998 le site du Pentagone. Plus récemment, un groupe de pirates s'est amusé à pénétrer dans les sites des grands ministères nippons en y laissant des messages désobligeants et en créant des liens avec des serveurs pornographiques. Ces messages peuvent aussi avoir un caractère politique. La page d'accueil du ministère de la Recherche japonais a ainsi été remplacée par un texte, rédigé en chinois, expliquant que le Japon refuse de reconnaître le massacre de Nankin (1937) et appelant le peuple chinois à protester contre le gouvernement japonais.

Les entreprises ne sont pas à l'abri. Elles possèdent un patrimoine à protéger, un savoir-faire. Dans le contexte actuel, elles sont dans l'absolue nécessité de se faire connaître. Ce qui pose le problème crucial de déterminer ce qui est ouvert et ce qui doit rester fermé, ce qui peut être présenté à l'extérieur et ce qui doit rester secret. Seule l'entreprise est capable de savoir ce qui est vital pour la pérennité de son activité.

La grande dépendance vis-à-vis de l'informatique, l'automatisation tentaculaire, le manque de sensibilisation et les moyens limités consacrés à la sécurité sont autant de facteurs de risques potentiels

En janvier dernier, le fournisseur d'accès irlandais *Connect-Ireland* a fait l'objet d'un abordage, pendant une dizaine de jours, commis par des cyberterroristes qui voulaient punir cette entreprise pour son soutien affiché sur le Net à la cause indépendantiste du Timor oriental. Bilan de l'opération : 3 000 clients privés d'accès et 150 000 F de matériel et de nouveaux logiciels pour reprendre une activité.

En février, plusieurs des plus grands sites de l'Internet ont fait l'objet d'attaques extérieures. *Yahoo*, *Amazon*, *eBay*, *Buy.com* mais aussi CNN.com ont été contraints d'inter-

rompre ou de ralentir leurs activités pendant plusieurs heures. A chaque fois, les réseaux ont été bloqués par un déluge de requêtes en provenance de plusieurs ordinateurs situés dans différentes villes américaines. La méthode est assez simple : les pirates prennent momentanément le contrôle de plusieurs dizaines d'ordinateurs de particuliers et d'entreprises en injectant des ordres pour lancer une attaque à une date et à une heure précises. Au moment venu, la conjonction de millions de requêtes vers un seul site conduit à sa paralysie. On parle alors d'attaque par saturation.

Les intrusions informatiques sont parfois plus intéressées.

Le 24 mars, on apprenait que deux pirates informatiques de 18 ans étaient arrêtés au Pays de Galles. Ils étaient parvenus à pénétrer dans des sites Internet commerciaux de cinq pays différents et avaient dérobé des informations concernant 26 000 cartes de crédit. Les pertes provoquées par ces intrusions pourraient dépasser les trois millions de dollars selon les estimations des enquêteurs du FBI.

Récemment, la première banque virtuelle britannique EGG a fait l'objet d'un hold-up informatique. L'absence de contact matériel entre le client et les guichets de la banque ne permet pas de connaître avec précision l'utilisateur des comptes et ouvre la porte à bien des abus comme par exemple la possibilité d'ouvrir des dossiers de demande de prêt, de percevoir l'argent et de disparaître avec les fonds.

La multiplication des réseaux, la globalisation et l'internationalisation des échanges n'ont fait qu'agrandir ces menaces alors que les réseaux présentent également d'autres risques comme des branchements clandestins sur les lignes, la captation de signaux parasites compromettants, ou l'écoute à grande échelle comme le « Réseau Echelon »[4] qui peut filtrer jusqu'à 2 millions de conversations, fax ou e-mail à la minute, soit près de 3 milliards par jour.

Constatation beaucoup plus grave, il est démontré que l'Internet est devenu un véritable talon d'Achille de nos sociétés. Ordinateurs, serveurs, fournisseurs d'accès, réseaux, sont ce que les routes, les ponts, les chemins de fer étaient avant l'ère de l'information. Il est désormais possible de paralyser les infrastructures stratégiques d'un pays par des attaques informatiques. Les experts de la *National Security Agency*, fin 1997, ont démontré qu'un groupe de cyberterroristes serait en mesure simultanément de couper l'électricité, de bloquer les centraux d'appels des services d'urgence, d'aveugler les contrôles aériens et maritimes, de pénétrer les systèmes du Pentagone, de perturber les services financiers et la Bourse.

Si les Etats et les entreprises sont vulnérables, nos intérêts purement privés aussi. Nous savons tous que les moindres mouvements sur nos lignes de transmission sont analysés, décortiqués pour des raisons de marketing. Les *cookies*, programmes cachés, guettent nos habitudes de consommation. Les fichiers qui en découlent valent de l'or car ils sont revendus ! Mais les fichiers qui gardent des données confidentielles sont également vulnérables. Qu'il s'agisse de données à caractère médical, scolaire, fiscal, ils sont à la merci des pirates si des mesures techniques appropriées ne sont pas mises en œuvre.

## PROFIL DES PIRATES

Les pirates sont des fouineurs assoiffés de connaissance, possédant un goût immodéré pour le *challenge* et tenaillés par l'envie permanente de se glisser dans des endroits interdits. Ils sont souvent avides de publicité. Les premiers pirates étaient extraordinairement doués car ils devaient tout concevoir. Aujourd'hui, ce n'est plus vrai. Comment peut-on les classer ?

Les vrais *hackers* ou *Gentlemen* : ils ne sont pas animés par une intention malveillante, ne cherchent pas à saboter ou à piller les systèmes. Ils forcent les accès uniquement pour montrer les vulnérabilités et en général avertissent les victimes des failles relevées qui ont permis l'intrusion. Ils signent généralement leur exploit par leur pseudo. On les appelle les *hackers* à chapeau blanc. Ils correspondent à un véritable esprit chevaleresque et dénoncent les activités criminelles classiques. Ils adorent se lancer des défis pour réaliser des actions spectaculaires.

Les *hackers* activistes ou *hacktivistes* : ils agissent pour soutenir une cause et retiennent pour valeurs la protection de la vie privée, le libre accès aux informations, l'antiracisme, la lutte contre les sectes. Ils vont jusqu'à attaquer les sites qui violent ces valeurs. On peut parler dans leur cas de mouvance idéologique. Ils appartiennent généralement à un groupe.

Les *crackers* et *hackers* intéressés : ils utilisent en général des programmes écrits par d'autres et trouvés sur le Net pour s'introduire dans des systèmes. C'est l'aspect vénal qui prime. Ils sont prêts à tout. Ils travaillent pour eux ou pour des entreprises et se rémunèrent sur leurs victimes. Ils se livrent à des chantages, demandent des rançons, utilisent les cartes bancaires dont les numéros ont été interceptés sur les réseaux, etc. Ils n'hésitent pas à détruire les logiciels et données.

Les corsaires : certains *hackers* choisissent de rejoindre ou d'aider les services qui luttent contre la criminalité envahissant les réseaux. Ils mettent au service de la loi des moyens intellectuels et permettent la formation des agents de l'Etat qui ne peuvent suivre les nouvelles méthodes qui évoluent sans cesse. Il s'agit d'auxiliaires précieux qui ont compris la perversité et les dangers de jouer à la limite de la loi et qui sont généralement proches de se reconvertir et de sortir du système caché du *hacking*.

Les termes pour qualifier les *hackers* sont en perpétuelle mutation et évolution. On distingue par exemple encore les *phreakers* qui ont pour objectif de téléphoner sans payer, les *carders* qui eux s'intéressent en exclusivité au cassage des systèmes de cartes bancaires.

On peut noter qu'en règle générale, le *hacker* est de sexe masculin, jeune, solitaire, qu'il aime travailler la nuit et qu'il ne compte pas ses efforts pour passer du temps non décompté sur son ordinateur. Ses rares moments de bonheur intense coïncident avec l'instant où il pénètre dans un site interdit. Joie paraît-il indescriptible, mais qui ne dure pas !

## LES RIPOSTES POSSIBLES

Lois et règlements existent pour nous protéger. Mais le Code pénal, les lois informatique et liberté et tous les textes réglementaires sont particulièrement difficiles à mettre en œuvre quand il s'agit d'attaques planétaires difficiles à localiser et quand les preuves sont diffuses et virtuelles.

Dans le nouvel environnement global des économies de marché, de l'actionnariat multinational, des normes sûres de fonctionnement et de régulation sont nécessaires pour fiabiliser les transferts d'informations. Comme pour les procédures de contrôle aérien qui sont très strictement définies, ou encore le Droit de la Mer, il paraît indispensable de fixer des règles. Il ne s'agit aucunement d'être liberticide, mais au contraire, de poser des bornes capables de promouvoir, à travers des principes clairs, un espace de grande liberté.

Pour l'Internet, seul le développement d'une coopération internationale semble pouvoir compléter les efforts normatifs des Etats et la volonté d'autorégulation des acteurs du réseau.

A l'échelle européenne des axes de réflexion ont été lancés, notamment sur la protection des mineurs et la dignité hu-

maine dans les services audiovisuels et d'information. Le Conseil des ministres a adopté des résolutions sur les nouvelles priorités politiques portant sur la société de l'information (21/11/96) et les messages à contenu illicite et préjudiciable diffusés sur Internet (28/11/96).

Pendant la présidence française de l'Europe, un projet de Convention contre le cybercrime « PCCY » sera déposé au Conseil de l'Europe. Garantir la sécurité des transactions et des communications dans le cyberespace et assurer la protection des infrastructures vitales et des réseaux figurent parmi les préoccupations majeures des gouvernements. Elles sont exprimées dans le projet de loi sur la société de l'information (LSI) qui sera prochainement discuté au Parlement.

Au-delà de l'Europe, la coopération internationale est tout autant indispensable.

L'OCDE a dressé les grandes lignes directrices qui portent essentiellement sur la protection de la vie privée, le respect de la personne humaine, la défense des consommateurs et la prise en compte des droits de la propriété intellectuelle.

Parallèlement à ces travaux, l'Union internationale des télécommunications (UIT) sous l'égide de l'ONU favorise le développement des infrastructures de télécommunications à l'échelle mondiale.

L'Organisation mondiale de la propriété intellectuelle (OMPI) qui regroupe 171 pays aura un rôle crucial à jouer dans l'élaboration d'une véritable charte protégeant les droits des créateurs.

Les sensibilisations portent leur fruit et une prise de conscience est en train de s'installer. Tout le monde travaille sur le sujet.

Le G8 a mis au point un programme de lutte en 10 points :
- établissement d'un réseau de points de contact dans chaque pays pour assurer une coopération rapide 24 h/24 ;
- former et équiper la police ;
- revoir les systèmes législatifs pour s'assurer qu'ils sont bien appropriés à la lutte contre les crimes de haute technologie ;
- prendre en considération le crime de haute technologie lors des négociations sur les accords mutuels d'assistance ;
- s'assurer que les preuves et les données informatiques sont toujours accessibles et que les recherches transfrontalières peuvent avoir lieu ;
- développer les procédures pour obtenir les données de transmissions auprès des opérateurs et étudier leur transfert international ;
- travailler de concert avec les industriels pour s'appuyer sur les nouvelles technologies en vue de rassembler et conserver les preuves ;
- permettre la communication par téléphone, par fax ou par e-mail pour offrir l'aide en cas d'urgence ;
- encourager la mise au point de standards pour des systèmes de traitement des données et des télécommunications fiables et sécurisés ;
- développer des normes internationales pour récupérer et authentifier des données électroniques dans le cas de poursuites criminelles.

## QUELLES SERONT LES PROCHAINES ÉTAPES ?

Les pouvoirs publics ne seront pas efficaces sans l'aide des industriels et du secteur privé. Les moyens policiers sont faibles, les preuves difficiles à établir et en plus, les victimes rarement bavardes car elles craignent la détérioration de leur image de marque en cas de divulgation à un procès par exemple. La coopération internationale se met en place difficilement. Trop d'intérêts contradictoires se conjuguent. Le pouvoir est de l'autre côté de l'atlantique et on peut aussi parler de différences culturelles.

Cependant, il va falloir faire avec. Nous

n'en sommes qu'à l'heure de l'apéritif et encore loin du plat de résistance. Nous aurons besoin de toutes les énergies pour connaître les nouveaux produits, les réseaux, les failles possibles.

La société de l'information est en marche. Comme lors de l'apparition des automobiles où il a bien fallu se résoudre à créer une véritable police de la route, il va bien falloir créer des cyberflics qui patrouilleront sur les réseaux virtuels. C'est là que çà se passe. Compte tenu du caractère international des réseaux, il faudra se mettre d'accord sur qui fait quoi et qui a le droit de quoi. Les structures existantes sont insuffisantes. Elles devront être complétées par des moyens partagés et faire appel à un vrai partenariat.

Il faut trouver un équilibre entre les besoins de la justice et les enjeux économiques.

Depuis la conférence de Paris en mai dernier, puis le sommet d'Okinawa, les pays du G8 ont compris que rien ne peut se faire sans tenir compte de l'avis des industriels.

Le Président de la République, ne s'est pas trompé lors de son discours de clôture de la conférence sur la sécurité et la confiance dans le cyberespace en distinguant le rôle de l'État, celui des entreprises et enfin, celui des associations représentant les citoyens.

Il a dégagé cinq orientations :

- la dimension extraterritoriale issue de l'Internet doit être civilisée. Il faut des lois pour garantir la liberté et la sécurité de tous ;
- c'est à l'État de remplir ce rôle en étroite concertation avec les utilisateurs des réseaux. Une co-régulation entre entreprises publiques et secteurs privé est souhaitable ;
- les pays du G8 doivent intensifier les travaux en commun pour construire les cadres juridiques nationaux et internationaux adaptés à la prévention et à la répression du cybercrime ;
- l'ensemble des Etats doit être associé à cet effort en vue d'être au même niveau d'égalité pour faire face à ces nouvelles menaces ;
- les pays du G8 doivent avoir un rôle moteur dans ce domaine pour éviter la prolifération de sanctuaires pour le cybercrime et pour qu'Internet soit un outil au service de tous les hommes.

Ces questions seront largement débattues lors de la prochaine réunion du G8 de Berlin autour des thèmes suivants : la localisation et l'identification des criminels, l'évaluation de la menace en matière de cybercriminalité, la prévention et la protection du commerce électronique et la confiance dans le cyberespace, la coopération et le partenariat entre pouvoirs publics, secteur privé et utilisateurs.

Ces divers développements doivent se faire en assurant la sécurité (cryptage des données), en veillant au respect de la vie privée (informatique et libertés à actualiser) et en garantissant la protection des consommateurs.

Paradoxalement, la traçabilité des transactions et leur conservation par les fournisseurs d'accès devraient permettre de remonter les filières et de connaître les tenants et les aboutissants ainsi que le contenu des échanges. Un plus pour les services de répression ou de régulation. Pédophiles, réseaux de prostitution, casinos virtuels n'ont qu'à bien se tenir... Encore faut-il définir les durées de conservation des données, les services qui vont y avoir accès, régler aussi les difficultés des perquisitions transfrontières, etc.

Il faut vivre avec son temps et si les risques existent bien, des solutions se dessinent pour que le bouclier de défense s'adapte aux attaques du glaive.

La cyberdissuasion, pendant de la dissuasion nucléaire, devrait permettre aux pays bénéficiant d'un haut degré d'intégration d'automatisation des structures de se neutraliser.

En effet, on sera bientôt capable de

lancer des répliques instantanées à d'éventuelles attaques et ainsi de neutraliser immédiatement des actions hostiles en provenance de puissances étrangères ou de groupes terroristes. Plus un pays est automatisé et plus il est capable de porter une attaque, mais en contrepartie, plus il est vulnérable. Ainsi, un nouvel équilibre cybernétique risque de remplacer l'équilibre nucléaire.

Aujourd'hui, vigilance accrue, dialogue accentué, respects mutuels avec sanctions à l'appui devraient nous permettre de venir à bout de ce nouveau Far-West.

Il faut bien se dire qu'en fait, nous ne sommes en présence que de moyens techniques à caractère trivial, qu'il faut considérer comme de simples moyens.

En réalité, le facteur humain constitue le déclic essentiel.

En conclusion, n'oublions pas que le phénomène de l'ouverture sur le grand village mondial est irréversible, ce phénomène concerne aussi bien les utilisateurs que les informaticiens et que donc, *c'est l'affaire de tous !*

## *NOTES*

1. Le nombre d'affaires criminelles liées aux technologies de l'information recensées en France a augmenté de 33,49 % entre 1997 et 1998 passant de 424 à 566 selon les chiffres de la Brigade centrale de répression de la criminalité informatique. Deux tiers de ces affaires portent sur des accès irréguliers aux différents systèmes, dont 81 % concernent des fraudes aux seules communications tandis que dans 40 de ces 379 dossiers, les accès frauduleux s'accompagnent de modifications ou de destructions de données, voire d'entraves au fonctionnement du système. Avec 79 affaires (14 %), viennent ensuite différentes contrefaçons alors que 62 % constituent des escroqueries et 12 (2 %) appartiennent à la catégorie des infractions à la loi informatique et libertés. Près de 90 % des affaires de contrefaçon portent sur les logiciels. Globalement, les usages frauduleux de cartes téléphoniques augmentent de 4 % alors que commencent à apparaître des cas d'utilisation frauduleuse de cartes téléphoniques prépayées. L'utilisation d'Internet à des fins frauduleuses ressort de l'escroquerie à 67 % dont plus de 95 % aux cartes bancaires, le plus souvent utilisées pour le paiement d'accès à des sites pornographiques payants.

2. Selon le CLUSIF, on distingue quatre grandes familles d'infection :

- la bombe logique, programme contenant une fonction malveillante généralement associée à un déclenchement différé et qui modifie un des programmes de l'entreprise ;

- le Cheval de Troie, programme en apparence inoffensif et qui contient une fonction illicite cachée, généralement utilisée pour pénétrer par effraction l'ordinateur et consulter, modifier ou détruire des informations ;

- le ver, processus parasite qui consomme les ressources du système. C'est une infection qui se duplique dans la mémoire vive et le réseau, qui peut se déplacer et contaminer beaucoup de machines connectées ;

- le virus, infection qui se duplique en greffant son empreinte sur les programmes, les fichiers et les zones système. Il comporte généralement trois éléments : un moteur de reproduction, une gâchette de déclenchement et une charge finale. Cette dernière pouvant être la destruction des données du disque dur.

3. Voir à ce propos l'ouvrage de Fabrizio Calvi et Thierry Pfister : « L'Oeil de Washington », la plus vaste opération d'espionnage de cette fin de siècle, paru en 1997 aux Editions Albin Michel.

4. Echelon, réseau puissant et très sophistiqué d'écoutes téléphoniques révélé par une enquête menée par *Il Mondo* du 27 mars 98. Moyens mis en œuvre par le pacte UKUSA qui lie les USA, le Canada, le Royaume-Uni, l'Australie, la Nouvelle-Zélande.