# *Centre Universitaire Juridique de Recherche sur les Menaces Criminelles Contemporaines*

## Conférence-débat sur "crime informatique et cyber-guerre"

***Intervention de Daniel Martin le 18 février 1999***

***Les conclusions et opinions exprimées dans cet exposé 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.***

# 1. UNE NOUVELLE ERE MONDIALE:

***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 prévoit un milliard de personnes connectées sur Internet en l'an 2000 !), on est pratiquement parvenu à supprimer toute notion de distance et de temps. Tout se passe en temps réel à la vitesse électronique. Presque tout est disponible sur tout.***

***Après la chute du mur de Berlin, l'effondrement de l'Union Soviétique et la fusion des deux Allemagnes, la donne a complètement changé. 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 primordiale 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 vulnérable.***

# 2. VULNERABILITES

***Des menaces guettent les matériels, les logiciels , les réseaux et les ressources des ordinateurs qui gèrent ces informations. Ces menaces sont internes à l'entreprise ou encore d'origines externes. Elles se traduisent par des destructions physiques, des sabotages immatériels ou la corruption de données.***

## *2.1. L'émergence d'une criminalité de haute technologie:*

***Les criminels se sont rapidement adaptés et ont compris les avantages susceptibles d'être tirés du monde virtuel.***

***En effet, 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 ne peuvent que favoriser le crime organisé.***

***Dans les années 80, seulement dix pour cent des criminels possédaient des notions d'électronique ou d'informatique. Aujourd'hui, la proportion est de quatre-vingt dix pour cent.***

***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 70 à 80.***

***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 90 puis l'explosion Internet ont ouvert l'ère du monde virtuel et immatériel propice à toutes les formes de criminalité.***

***La criminalité de haute technologie recouvre l'ensemble des actes illégaux intéressant l'informatique et les télécommunications tant sur le plan des matériels que des logiciels.***

***Elle concerne la criminalité informatique proprement dite et les contrefaçons ou le clonage de composants électroniques***

***capables de créer des dysfonctionnements dans les systèmes d'information, de télécommunications ou autorisant un usage frauduleux.***

***Rentrent ainsi dans cette définition, toute action illégale dans laquelle un ordinateur est l'instrument ou l'objet du délit; tout délit dont le moyen ou le but est d'influencer la fonction de l'ordinateur; tout acte intentionnel, associé d'une manière ou d'une autre à la technique informatique, dans laquelle une victime a subi ou aurait pu subir un préjudice et dans laquelle l'auteur a tiré ou aurait pu tirer un profit.***

***Les lignes directrices de l'OCDE, dès 1986 ont posé des principes de base de la criminalité informatique: Accès frauduleux , interception des systèmes, violation des règles de sécurité dans une intention malhonnête ou nuisible, violation du droit exclusif du détenteur d'un programme, entrée, altération, effacement ou suppression de données, entrave au fonctionnement des systèmes.***

### *2.2. Le piratage:*

***Il faut savoir que la vulnérabilité informatique des entreprises devient le risque industriel et économique numéro un en France ainsi que dans les autres pays industrialisés.***

***Le piratage constitue certainement le principal vecteur des actes criminels.***

***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, exploitation, création 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 : vers, virus, chevaux de Troie, bombes logiques, trappes, composants trafiqués[i] pour les plus connues.[ii].Nano-machines ou robots minuscules plus petits que des fourmis et capables de s'attaquer au matériel, microbes ou bactéries attaquant le silicium, 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.***

***Quelques exemples concrets:***

***En 1994, un pirate allemand prend de chez lui le contrôle informatique du système d'air conditionné de la Bourse de New York et fait brutalement monter la température du local abritant les ordinateurs qui tombent en panne.***

***En avril 1998, les "MOD", Masters of Downloading" une quinzaine d'individus, américains, britanniques et russes s'infiltrent dans l'ordinateur basé au Colorado, qui contrôle le "Defense Information systems Network", un réseau de satellites de l'US Air Force. MOD veut simplement laisser la trace de son passage dans le système. Mais ils pouvaient aussi bien saboter le réseau et mettre hors d'usage pendant un moment le GPS (Global Positioning system).***

***En mai 98, "The Milworm", un groupe de pirates de 15 à 18 ans pénètre le réseau du centre indien de recherches nucléaires de Bhabha ( Bhabha Atomic research Centre) et y vole des travaux sur les essais nucléaires pratiqués par ce pays en mai 98. Ils détruisent 2 des 8 serveurs du Centre.***

***En août dernier, les Tigres de l'Eelam Tamil baptisés pour la circonstance les Tigres noirs de l'Internet ont lancé une virulente cyberattaque contre le réseau informatique reliant les ambassades du Srilanka dans le monde. Au même moment, les boîtes aux lettres électroniques de toutes les représentations de ce pays ont été inondées de messages pour faire s'effondrer le système.***

***En septembre dernier, 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.***

***D'autres exemples :***

***21 mai 98, la bande de Boston , 7 pirates connus sous l'appellation LOPHT a témoigné devant le Sénat des USA en déclarant être capable de perturber les communications à longue distances et interrompre l'Internet pendant 2 jours en seulement 30 minutes.***

***Au cours d'une autre expérience, les enquêteurs du Congrès ont pu ainsi accéder aux informations concernant les déplacements des diplomates américains, aux dossiers personnels de ceux-ci, aux E-mails. Ils ont pu s'emparer et prendre le contrôle des ordinateurs de la bourse, de la réserve fédérale et des archives des services des impôts.***

***Toujours en mai 98, les experts du centre de surveillance informatique de l'aviation américaine de San Antonio ont vu s'allumer les signaux d'alerte d'intrusions illégales dans une demi-douzaine de réseaux électroniques protégés. De source officielle, les pirates étaient 2 lycéens de 16 ans du nord de la Californie qui travaillaient en liaison avec un adolescent installé en Israël. La chasse pour les identifier a duré un mois.***

***Mais l'oeuvre 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 F.B.I. 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 réussies !***

***Une enquête menée par l'Agence Nationale de Sécurité 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.***

***Le Ministère français de l'Intérieur annonce lui même plusieurs centaines de tentatives de piratage de ses sîtes.***

***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"[iii].qui peut filtrer jusqu'à 2 millions de conversations, fax ou e-mail à la minute, soit près de 3 milliards par jour.***

### *2.3. Internet*

***La tempête INTERNET est venue bousculer encore un peu plus ce monde en mouvement.***

***Il suffit de rappeler quelques chiffres: en 84, 1000 ordinateurs connectés. En 97, plus de 20 millions. Environ 100 millions d'internautes utilisent 12 millions de services disponibles par l'intermédiaire de 3500 fournisseurs d'accès dans le monde. Chaque mois, plus d'1 milliard de messages sont échangés sur le Réseau !***

***Or, Internet n'est pratiquement pas réglementé et comme support des activités humaines il peut bien évidemment véhiculer toutes les formes possibles de délinquance et de criminalité.***

***Les Services de Police et de Sécurité des cinq continents sont submergés par l'explosion de la criminalité déferlant librement sur les nouvelles autoroutes informatiques du réseau. Une dynamique tentaculaire qui, faute d'une législation cohérente et d'actions concertées, peut favoriser l'ascension démesurée de nouvelles puissances criminelles de dimension mondiale.***

### *2.4. Florilège:*

***On peut rapidement citer quelques exemples pratiques pour illustrer ces nouvelles formes de criminalité:***

#### 2.4.1. Contrefaçon:

***Ce délit traditionnel a pris une autre dimension avec l'apport de l'informatique et des réseaux.***

***Les contrefaçons de logiciels sont très nombreuses.***

***Des logiciels sont par exemple téléchargés des Etats-Unis et du Canada par un membre d'un réseau habitant la France, puis adressés à un ou plusieurs complices situés aux Pays-Bas ou dans un des pays de l'Europe de l'Est qui assurent la gravure sur des disques CD-ROM et leur commercialisation.***

***La multiplication des frontières et des auteurs ralentit considérablement les enquêtes et poursuites judiciaires.***

***Selon le Business Software Alliance qui mène le combat contre le piratage de logiciels, les pertes pour les éditeurs de logiciels ont été évaluées à plus de 2 milliards de Francs, seulement pour l'année 1996.***

#### 2.4.2. Chantage:

***Méthode de plus en plus employée pour obtenir des fonds en grosse quantité avec un minimum de risque sur le plan pénal.en comparaison avec par exemple les hold-ups à main armée ou avec prise d'otage.***

***A la fin de l'année 96, des pirates ont menacé une entreprise de saboter ses ordinateurs si une rançon n'était pas immédiatement versée. Pour démontrer la réalité de leurs possibilités, ces pirates avaient au préalable pris possession des fichiers clients de l'entreprise. Dévoiler ces données à la concurrence signifiait la faillite pure et simple. Les pirates ont été arrêtés au moment de la remise de la rançon. Il s'agissait de ressortissants allemands qui avaient pris pour cible une entreprise américaine[iv].***

***Plus récemment, la City-Bank a fait l'objet d'un autre type de chantage à la bombe logique. La localisation d'une simple ligne intempestive de programme capable de bloquer le réseau mondial de la banque contre le paiement de dix millions de dollars était l'ultimatum des criminels. Autant chercher une épingle dans une meule de foin. la banque a dû en plus réexaminer et nettoyer tous les programmes.***

#### *2.4.3.* Fraude téléphonique

***Les criminels volent les numéros de série téléphones cellulaires appartenant à des abonnés de bonne foi et reprogramment ceux-ci dans les puces d'autres appareils. Il s'agit alors de clones tout à fait comparables aux originaux. Seule les plaintes des intéressés permettent de stopper ce type de fraude. Les compagnies de téléphone estiment à plusieurs millions de dollars par mois le manque à gagner. Selon le C.T.I.A., le coût global des fraudes sur les téléphones mobiles serait de plus de 650 millions de dollars pour l'année 1995.***

#### *2.4.4.* Vols de puces

***Faciles à stocker, particulièrement petites et donc transportables aisément avec discrétion, les puces et composants électroniques sont devenus des produits de choix pour la grande délinquance internationale. On estime qu'un tiers des machines commercialisées légalement contiennent des composants à l'origine douteuse. Selon les statistiques de Scotland Yard, en Grande-Bretagne, ces vols auraient coûté plus d'un milliard de livres aux fabricants rien que pour l'année 1995. Le trafic est international. Le vol initial peut se situer en Irlande, les produits transitent dans la journée dans un grand port européen, Amsterdam ou Hambourg. Ils sont ensuite montés sur la côte ouest des Etats-Unis et vendus assemblés au Mexique ou ailleurs. Il est fréquent également que des puces fabriquées en Asie soient dérobées aux USA puis retournent en Asie pour y être assemblées dans des matériels qui sont ensuite réimportés aux Etats-Unis !***

#### 2.4.5. Internet et les cartes de crédit:

***Sur Internet des logiciels de génération de numéros de cartes de crédit ainsi que toutes les informations expliquant les fraudes qui y sont associées peuvent être très facilement visualisés.***

***Comme très souvent les annonceurs demandent pour commander un produit ou accéder à un service de fournir un numéro de carte, que ces données transitent en clair sur le réseau, il est alors très simple pour un pirater de prendre connaissance du numéro et de s'en servir d'une manière illicite !***

***L'Internet, avec ses banques virtuelles, sans banquier sans guichet, sans frontière constitue un défi pour ceux qui luttent contre le blanchiment d'argent.***

***L'Internet, c'est aussi un immense réservoir de connaissances et d'échanges d'informations, quelquefois criminelles.***
***Vous voulez savoir comment fabriquer une bombe artisanale à partir de produits disponibles librement sur le marché, comment vous procurer de faux papiers ou encore obtenir une adresse fictive au Japon ou à New-York ? Rien de plus facile, on trouve tout sur l'Internet.***

***L'Internet, c'est aussi le domaine de la désinformation, de l'intoxication et de la manipulation :***

***Moscou, 1 er juillet 97, la direction de l'agence Tass dément être à l'origine d'une dépêche disponible sur Internet faisant état de l'arrivée inopinée du dirigeant Khmer rouge Pol Pot en Suède.***
***C'est sûrement un acte de piratage, ce n'est pas nous qui sommes à l'origine de cette information a déclaré Pavel Mikhalev, directeur adjoint de l'agence à Reuter.***

#### 2.4.6. Et encore:

***Diffamations, injures, diffusion d'images pornographiques et pédophilie, provocation à la haine ou à la discrimination raciale, contestations et apologies de crimes contre l'humanité, provocation à la commission de crimes ou de délits.; mais aussi les infractions classiques en matière économique et financière: (escroqueries, abus de confiance, infractions à la législation aux lois sur les sociétés); sans oublier les atteintes aux libertés individuelles et les infractions à la réglementation sur les jeux( comme la création de casinos virtuels sur Internet) viennent compléter un panorama malheureusement non exhaustif..***

***Ces formes diverses et variées de criminalité trouvent leur source auprès d'individus, de groupes criminels ou d'Etats.***

***En France, les actions individuelles sont essentiellement axées sur le cracking de logiciels et de jeux vidéo et sur le phreaking des réseaux téléphoniques. On se souvient du cas de l'implantation d'un autocommutateur pirate au sein de celui de la caisse d'assurance-maladie du XIII ème arrondissement. Coût de la fraude : 2,5 millions de francs. Mais on ne peut pas négliger les attaques des pirates. Les ordinateurs du Ministère de l'Intérieur subissent plusieurs centaines d'attaques par jour.***

***Ces attaques répondent à des règles de base très simples :***

- ***Toute entreprise gère sur ses ordinateurs des fichiers automatisés contenant des informations sensibles ou stratégiques,***
- ***Tout système informatique et ses réseaux comporte une ou plusieurs failles qui permettent de contourner les systèmes de sécurité,***
- ***Toute personne ayant accès au système d'information a vocation à découvrir les faiblesses des dispositifs en place,***
- ***La probabilité d'utilisation malveillante est inversement proportionnelle aux risques encourus.***

***Les actions de groupes criminels ou d'entreprises sont plus difficiles à appréhender car les moyens engagés sont à la hauteur des enjeux.***

***On sait cependant que tous les moyens sont bons pour connaître les conditions d'un marché pour un concurrent, pour apprendre à moindre frais les résultats de prospections etc..***

***Les différents groupes mafieux, sans distinction de nationalité, ont vite compris les possibilités dégagées par Internet en particulier pour les casinos virtuels et le blanchiment d'argent.***

***Mais la plus grande menace réside sans aucun doute dans les possibilités offertes aux Etats d'utiliser les moyens quasi sans limites des ordinateurs et des réseaux.***

***Les services spécialisés se sont reconvertis :***

***Selon le directeur de la CIA, le budget total des 13 agences américaines de renseignement était en 98 de 26,7 milliards de***

***Dollars et sera en 99 de 29 milliards, soit l'équivalent de ce qu'il était au moment de la guerre froide.***

***La NSA reconnaît qu'elle traite autant d'informations qu'il y a dans la bibliothèque du congrès ( la plus grande du monde) …toutes les trois heures. Les informations sont recueillies par des bases secrètes qui écoutent les satellites de communication comme Intelsat. Les USA possèdent une cinquantaine de stations dans une vingtaine de pays sur les cinq continents.***

***Ces interceptions se font sur les faisceaux quand ils redescendent sur terre, par l'intermédiaire de satellites d'écoute placés à côté des satellites de communication ( Mercury, Trumpet etc..) qui guettent également les émissions radioélectriques en provenance de la terre. Pour les téléphones portables, d'immenses antennes (taille d'un terrain de foot) peuvent capter les ondes émises par les stations-relais des téléphones mobiles…***

***La liste n'est pas exhaustive. Pour le cas d'Internet, les fournisseurs américains autorisent la NSA à " renifler " tout ce qui se passe sur le Web et à " filtrer " ce qui l'intéresse. Le but inavoué est de pouvoir consulter à distance et incognito le contenu des ordinateurs de ceux qui se connectent sur les sites appropriés.***

***Il est vrai que de bonnes raisons, avouables, sont largement mises en avant comme la lutte contre le terrorisme, la prolifération des armes de destruction massive (nucléaire, bactériologique, chimique), la lutte contre les trafics illicites (drogue, corruption, etc..) ou encore le suivi des conflits pour l'aide à la diplomatie.***

***Mais quand on a de tels outils, on s'en sert mais on ne l'avouera jamais. Il s'agit pourtant d'atteintes à la vie privée, à la protection des consommateurs et elles touchent des libertés fondamentales qui sont pourtant le fondement des démocraties.***

***Plusieurs contrats et marchés ont été perdus bizarrement et la seule explication est que les Etats aident leurs entreprises. Tout le monde connaît le cas de la couverture radar de l'Amazonie et des revirements du gouvernement brésilien.***

***Il reste qu'aujourd'hui, chacun essaie de se défendre et d'attaquer, avec ses moyens propres.***

### *2.5. UN NOUVEAU DANGER PERMANENT: le terrorisme informatique:*

***Londres, le 22 mai 97, une opération conjointe du MI5 et de l'Unité antiterroriste de Scotland Yard a permis l'arrestation d'islamistes proches du Groupe Islamiste Armé. Outre des produits et des formules permettant de penser que ces individus allaient élaborer des attentats, les policiers ont découvert des matériels informatiques puissants démontrant l'utilisation des réseaux pour assurer les communications entre les membres de cette organisation.***

***Ces groupes bénéficient de soutiens et possèdent des moyens informatiques ainsi que les capacités humaines pour attaquer les réseaux informatiques.***

***L'attentat du World Trade Center, le 26 février 1993 peut être considéré comme un acte de terrorisme informatique. Il démontre qu'en raison de dégâts matériels importants plusieurs centaines d'entreprises peuvent être privées de liaisons avec l'extérieur pendant plusieurs jours. Les pertes dues à cet attentat ont été estimées à plus de 700 millions de dollars***.

***Compte tenu des moyens existants sur le marché, en vente libre, avec des investissements ridicules par rapport à ceux correspondants aux armements classiques, il est tout à fait possible pour pratiquement n'importe qui d'attaquer ou de détruire les systèmes d'information d'un pays, de mettre à genoux une grande puissance ou une multinationale.***

***L'équipement de base du terroriste informatique se compose d'un simple micro-ordinateur équipé d'un modem. Le savoir faire peut être puisé dans les nombreux outils de sécurité des réseaux disponibles sur Internet. Grâce à ces programmes, l'attaquant prendra le contrôle des sites mal protégés et fera ce qui lui plaira.***

***Cependant, l'attaque de moyens informatiques, matériels, logiciels et données contenus, traités et transmis par les ordinateurs et les réseaux est un concept difficile à concevoir clairement car la menace est virtuelle.***

***Pour concrétiser les risques encourus, le Ministère de la Défense américain a réuni l'an dernier les plus hauts responsables de la sécurité nationale et les industriels concernés pour simuler une cyberattaque. Un des scénarios était le suivant :***[v]

***"L'Iran tente de tarir la production de pétrole de l'Arabie Saoudite. Washington envisage d'envoyer des troupes dans la péninsule. Les iraniens, se souvenant de l'échec de Sadam Hussein, décident de porter le combat sur le sol américain et de s'attaquer à son point faible : les systèmes d'information. Tout à coup des centraux téléphoniques de bases militaires deviennent inutilisables, comme saturés (virus autorépliquant), d'autres sont hors service (bombe logique). La Maison Blanche envoie du matériel militaire dans le Golf. Un train convoyant du matériel militaire destiné à partir pour l'Arabie vers un aérodrome militaire déraille suite à un problème du système de contrôle du trafic ferroviaire. Plusieurs centres météo tombent en panne. Les avions sont cloués au sol. La Banque Centrale découvre une tentative de sabotage de son système de transfert de fonds. CNN annonce que l'Iran a payé des informaticiens russes et des programmeurs indiens pour détruire l'économie occidentale. Les cours des bourses de New York et de Londres s'effondrent. Plusieurs banques d'importance sont piratées. L'information s'ébruite. Panique chez les épargnants qui veulent à tout prix récupérer leur argent. On signale aussi des programmes pirates de propagande sur les chaînes de télévision. Au même moment Washington est privé de téléphone (même les mobiles) il est alors très difficile pour le Président de réunir ses conseillers. L'ordre de départ des soldats vers l'Arabie est donné, mais ce dernier s'effectue dans le plus grand chaos en raison des problèmes de communication dans les bases de déploiement..."***

***Ces divers travaux ont permis de déterminer des secteurs clés à protéger tout particulièrement: l'énergie, les transports, les télécommunications, les finances, les services d'urgence et les services publics en général. Ils ont constitué la base des ripostes à mettre en place.***

***Le 29 juin, américains et britanniques ont organisé des exercices de guerre de l'information afin de mettre à l'épreuve leurs défenses contre la menace de terroristes ou de pays tiers qui utiliseraient l'outil informatique pour attaquer le pays. Cet exercice a commencé par une attaque du système électrique par des terroristes suivi par une panne générale . Le scénario complexe qui suivait a fait intervenir l'Etat, ses adversaires, les terroristes, des blanchisseurs d'argent, etc…Cet exercice a mis en lumière les défis et les faiblesses du système selon John HAMRE vice-ministre de la Défense.***

***Les pirates disposent de bien d'autres outils: les virus, vers et chevaux de Troie pullulent sur les réseaux. Il en existait 6 en***

***1987, on en compte plus de 8000 aujourd'hui dans le monde. Malgré les vaccinations possibles, les utilisateurs ne sont jamais à l'abri d'infections logiques susceptibles de détruire des données ou des supports matériels comme des disques durs.***

***Malgré la forte croissance de la fraude informatique au cours des dernières années, les utilisateurs toujours plus nombreux ainsi que les responsables des systèmes ne semblent pas avoir pris pleinement conscience des risque encourus. Pourtant, n'importe quel système automatisé installé en réseau peut à chaque instant devenir la cible de pirates.***

***Le manque de sensibilisation des entreprises et l'absence de prise de conscience de beaucoup d'institutions étatiques complètent ce tableau des vulnérabilités propices à la prolifération d'actes néfastes. La protection de l'information est moyenne dans 70% des cas alors que les entreprises reconnaissent qu'elles ne peuvent se passer de leur informatique : 40% plus de 4 heures, 10% plus d'un jour, 20% plus de trois jours, 30% plus d'une semaine. C'est dire l'ampleur des vulnérabilités.***[vi]

## 3. RIPOSTES:

***Les réactions face à ces nouveaux défis passent nécessairement d'abord par une prise de conscience généralisée, puis par des solutions qui s'appuient sur une réforme des systèmes éducatifs et de formation, une meilleure sensibilisation des partenaires économiques et un traitement international du sujet.***

### *3.1. UNE PRISE DE CONSCIENCE:*

***Depuis juin 1997, le Président des Etats-Unis a entre les mains les conclusions de la Commission Présidentielle sur la Protection de l'Infrastructure sensible (PCCIP President's Commission on Critical Infrastructure Protection).***

***L'Overview Briefing rendu public sur Internet*** [vii]***y relève plusieurs domaines sensibles identifiés comme étant si vitaux que leur***

***indisponibilité ou destruction aurait un impact très dommageable pour la défense ou la sécurité.***

***Il s'agit des télécommunications, de l'électricité, du stockage et du transport des hydrocarbures, du secteur des banques et de la finance, des transports, de la distribution de l'eau, des services d'urgence ( santé, police, pompiers) et des services publics en général.***

***Force est de constater que l'informatique et les télécommunications rendent ces secteurs de plus en plus dépendants.***

***L'interdépendance des moyens et des réseaux accroît encore la complexité du problème.***

***Les liaisons avec Internet et les réseaux commutés créent de nouvelles vulnérabilités pour les effractions et les accès indus. En conclusion, la commission considère que la sécurité physique et logique des infrastructures sensibles sera de plus en plus menacée si des contre-mesures ne sont pas prises en considération.***

***De la même manière, les ministres de l'Intérieur et de la Justice des Pays membres du G8 ont constaté qu'ils avaient pris du retard face à la criminalité informatique.***

***Plusieurs critères nécessaires au traitement du sujet ont été identifiés:***

***<u>Le besoin d'un échange d'information</u> entre les gouvernements, mais aussi entre les secteurs publics et privés est indispensable. Les données relatives aux délits informatiques ne sont ni partagées ni recoupées. Sans partage d'informations sur les intrusions, il n'est pas possible d'effectuer des comparaisons de faits notables ou d'analyses sérieuses.***

***<u>La nécessité d'établir un climat de confiance</u> est tout autant évidente. Si les informations sont partagées en temps réel, alors, il devient possible d'identifier, de prévenir et de contrer une attaque aussi bien criminelle que terroriste ou nationale. Encore faut-il avoir confiance en ses partenaires.***

***<u>L'obligation de financer le renforcement des infrastructures et l'étude des risques</u> conditionne l'avenir. La technologie est à la fois une partie du problème et de la solution. Recherche et développement doivent être les éléments à solliciter pour faire face aux nouveaux défis.. Aujourd'hui, les outils disponibles ne permettent que des analyses postérieures aux agressions et intrusions. Il s'agit d'orienter la technologie et de définir des normes de sécurité d'un niveau acceptable dès la conception même des matériels, logiciels et réseaux.***

***Le Président Clinton a demandé au Congrès le 22 janvier une augmentation de 1,46 milliards $ du budget de l'an 2000 pour lutter contre les attaques chimiques, biologiques et informatiques.***

***Cette décision marque réellement le souci de prendre en compte "la guerre de l'information stratégique". Dans ce domaine, la mise en place d'éléments de défense suppose des capacités fortes de créer des systèmes offensifs performants.***

***La Rand vient de rendre un rapport intitulé " Strategic Information Warfare rising" qui expose des scénarios de guerre de l'information de première génération.***

***Ils vont de la domination totale des USA en possession des meilleurs outils offensifs du monde capables de pénétrer les défenses de tous les autres pays, à une coopération de défense de la plupart des pays avec normes de contrôle et traçabilité, en passant par la dissuasion mutuelle de la dizaine de pays hautement compétentsen matière de guerre de l'information et qui collaborent pour éviter la diffusion de ces outils aux autres pays. La situation ressemble comme deux gouttes d'eau à la bonne vieille dissuasion nucléaire.***

### *3.2. LES SOLUTIONS*

***Elles se posent en terme de structures et de responsabilités.***

***Qui est responsable ? La réponse n'est pas simple et peut varier en fonction des Etats, des sensibilités et des cultures. Cependant , il existe une ambiguïté certaine quant au partage de responsabilité entre les représentants de la loi, la défense nationale , l'administration et le secteur privé.***

***Le <u>partage de l'information</u> est un facteur commun entre les sources publiques et privées. Une <u>analyse centralisée</u> permettrait d'alerter en cas d'attaque.***

***Ainsi, le Congrès et la Maison-Blanche préconisent la création d'un Bureau International de la Criminalité Informatique. Pour compléter le dispositif de défense, le Pentagone entend dépenser 3,6 milliards de dollars au cours des années 1999 à 2002 afin de renforcer les mesures de sécurité en matière informatique.***

***Parallèlement, l'industrie informatique américaine ne reste pas les bras croisés et finance elle-même des dispositifs de sécurité. Comme pour la "Guerre des Etoiles", les autres Etats vont avoir du mal à suivre le mouvement, notamment en raison des contraintes budgétaires qui grèvent tous les budgets nationaux.***

***En Europe, et en France en particulier, l'approche est sensiblement différente. Le gouvernement estime que ce n'est pas au secteur privé de se substituer au pouvoir politique pour désigner le point de rencontre entre intérêt public et expansion économique.***

***Le fossé est donc grand entre les différents points de vue.***

***Le dossier de la cryptologie constitue un exemple type.***

***Cette technique est restée longtemps l'apanage des services étatiques, mais elle constitue aujourd'hui un élément essentiel dans la confiance nécessaire à l'utilisation des réseaux mondiaux. Le problème initial de sécurité extérieure se trouve projeté au niveau interne. Un équilibre doit s'effectuer entre une nécessaire libéralisation et un contrôle permettant la protection des états qui ne peuvent favoriser les activités criminelles.***

#### 3.2.1. Réformer le système éducatif et de formation.

***Trop de responsables manquent de connaissances en technologies de l'information. Il s'agit de créer les outils susceptibles de répondre à ce besoin d'ajustement permanent des connaissances et de l'apprentissage des nouvelles technologies.***

***La formation des différents acteurs sur le terrain a besoin d'être engagée sur une grande échelle. Police, Justice, Administrations et partenaires privés doivent adapter leurs connaissances et les actualiser.***

***Le crime informatique n'est plus une affaire de spécialistes il peut toucher tout le monde et la meilleure des préventions consiste à former, à la bas, toutes les parties.***

***La première étape se situe au niveau de l'initiation à l'informatique. C'est à ce moment que les programmes scolaires devraient comporter les premiers éléments fondamentaux de défense et de sécurité. La légitime défense de ses propres valeurs devrait s'apprendre dès l'école, comme le code de la route. Savoir se servir d'un ordinateur c'est bien, en connaître ses limites et les risques encourus, c'est mieux.***

### 3.2.2. Sensibiliser les partenaires économiques:

***La sensibilisation de tous les milieux concernés, en particulier les P.M.E. et P.M.I. qui constituent le tissu profond de l'emploi et du savoir- faire mérite d'être accentuée afin de faire prendre conscience, à tous, des risques encourus. Les moyens nécessaires doivent être dégagés ou redéployés auprès des services concernés pour mener à bien cette mission essentielle.***

***Les services ayant pour rôle la protection du patrimoine doivent être en mesure de procéder à la sensibilisation de toutes les entreprises concernées. Il s'agit d'un travail de longue haleine qu'il faut actualiser en permanence. Souvent les structures existent, mais il faut les activer, les faire fructifier. En un mot il faut garantir un vrai suivi.***

***Les Ministères et l'Administration, surtout en France où le service public est très développé, ne doivent pas être oubliés au profit des entreprises privées. Ces départements renferment les richesses de l'Etat..***

### 3.2.3. Etablir un dialogue entre les structures:

***La plupart des pays ont été conduits à spécialiser un certain nombre de services sur le sujet particulier des risques liés aux nouvelles technologies de l'information. Ces réponses ont été données au coup par coup, souvent sous la pression des évènements et de l'actualité. Les services de renseignements d'abord, mais aussi les services chargés de la constatation des délits, des enquêtes, des poursuites et aussi de l'élaboration des outils de défense ont été impliqués dans la réflexion.***

***Des dialogues, d'abord timides, se sont instaurés, souvent sur un plan bilatéral. Mais les enquêteurs souffrent encore cruellement d'une connaissance partielle du problème. Les victimes répugnent à se faire connaitre et seulement 10% des fraudes informatiques sont signalées aux services de police judiciaire.***

***L'information est détenue et répartie chez plusieurs partenaires tant publics que privés: des services de police aux sociétés d'assurance en passant par les clubs spécialisés en sécurité***

***informatique ou les organismes mis en place pour répondre aux urgences, comme les "Computer Emergency Response Team" (CERT) par exemple.***

***Le rassemblement tant des moyens humains que financiers devrait présider la recherche de solutions dans un contexte permanent de pénurie budgétaire;***

***Le regroupement des compétences mériterait d'être engagé pour supprimer les déperditions d'énergie et augmenter le degré d'efficacité. Des formations communes devraient être concertées.***

***Comme le FBI dispose du National computer Crime Squad, il s'agit de créer les structures et outils souples susceptibles de s'adapter aux fluctuations permanentes du crime.***

***La mise en place d'un véritable Observatoire Central des incidents du monde de l'informatique et des communications garantirait déjà une meilleure information et pourrait constituer la base d'un dialogue fructueux pour une nécessaire coopération internationale.***

#### *3.2.4.* Traiter le sujet au niveau international*:*

***Dans le nouvel environnement global des économies de marché, de l'actionnariat multinational, des normes de fonctionnement et de régulation sûres 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 humaine 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).***

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

***Si un traité international est peu probable compte-tenu des divergences et des diversités nationales, une collaboration internationale visant à donner plus de sécurité semble à portée.***

***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 (U.I.T.) sous l'égide de l'O.N.U. favorise le développement des infrastructures de télécommunications à l'échelle mondiale.***

***Cependant, les Etats restent très jaloux de leurs prérogatives dans les domaines qui touchent leur souveraineté. Il suffit de constater en France les difficultés qui ont présidé à l'élaboration de la politique simplement nationale sur la cryptographie pour s'en rendre compte.***

***L'avènement d'une civilisation de l'information passe pourtant par l'instauration d'un climat de confiance entre partenaires. Encore faut-il garantir la pérennité des informations et s'assurer de l'authentification des correspondants dans une disponibilité acceptable des outils utilisés. Là réside toute la clé du problème et du succès du Commerce Electronique.***

## 4. L'AVENIR PREVISIBLE :

***Le but est simple: faire en sorte que les criminels ne soient à l'abri nulle part et ne puissent pas menacer le fonctionnement de nos démocraties.***

***Mais les voies pour y parvenir ne sont ni simples ni uniques.***

***Chaque pays membre du G8 s'est engagé à créer un point de contact disponible en permanence et capable de suivre les affaires transnationales liées à la criminalité informatique. Les personnels spécialisés seront formés , selon les conclusions, en nombre suffisant.***

***L'accord prévoit également un réexamen des systèmes juridiques capables de garantir des poursuites en cas d'usage délictueux des nouvelles technologies de l'information. Il s'attache également au problème fondamental des perquisitions transfrontières et de la conservation des preuves. Un premier bilan devrait être tiré dès le prochain sommet du G 8.***

***D'une dimension internationale, le problème est également collectif. Il touche aussi bien les gouvernements que les***

***consommateurs. Ainsi, c'est l'affaire de tous.: Syndicats, chambres de commerce et d'industrie, associations, universitaires, parlementaires, responsables des services publics, simples citoyens doivent tous être associés et participer à l'effort collectif face à ce défi colossal du cybercrime.***

***La lutte contre la criminalité informatique est difficile. Il est évident que les lois doivent être ajustées et que l'entente internationale constitue une étape indispensable pour améliorer l'efficacité des mesures prise ici ou là.***

***Le chemin sera long, mais il faudra bien un jour se décider enfin à se donner les moyens durables capables de durcir un bouclier de défense adapté pour faire face efficacement aux glaives de plus en plus acérés du crime organisé.***

[i] 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.

[ii] Voir à ce propos l'ouvrage de Fabrizio Calvi et Thierry Pfister: "L'Oeil de Washigton", la plus vaste opération d'espionnage de cette fin de siècle, paru en 1997 aux Editions Albin Michel

[iii] Echelon, réseau puissant et très sophistiqué d'écoutes téléphoniques révélé par une enquête menée par "Il Mondo" du 27 mars 98.

[iv] Lire à ce sujet "Cyber Mafias", de Serge Le Doran et Philippe Rosé, édité en1998 aux Editions Denoël dans la collection "Documents d'actualité".

[v] Voir la Revue "Politique Internationale" numéro 77 , article " Cyber-terrorisme: le nouveau péril" Daniel Martin. Editions Politique Internationale.

[VI]
voir l'ouvrage de Daniel Martin "Criminalité Informatique" édité en 97 aux Presses. Universitaires de France dans la collection "Criminalité Internationale"

[vii] Sur le site ***http://www.pcpip.gov***