Le World Wide Web, accélérateur de la mondialisation, peut-il constituer la menace ultime sur les grands équilibres mondiaux ?

Mémoire de géopolitique
du lieutenant-colonel André SELLINI
dans le cadre du séminaire
« mondialisation et logique de puissance »
25 mars 2004

Directeur de séminaire
professeur Jean-Louis SCARINGELLA

Le World Wide Web, accélérateur de la mondialisation, peut-il constituer la menace ultime sur les grands équilibres mondiaux ?

SOMMAIRE

INTRODUCTION

Il y a aujourd'hui un demi-milliard d'internautes dans le monde, et l'on compte presque 4 millions de nouveaux internautes tous les mois. Les achats en ligne représenteront 170 milliards d'euros en 2002. En 2001, le montant des transactions sur Internet a pour la première fois dépassé celui réalisé sur le Minitel. En 2002, il lui est cinq fois supérieur. 2,3 millions d'internautes disposent, à leur domicile, d'un accès à haut débit (60% en ADSL et 40% par le câble) - Ipsos - septembre 2002. L'ordinateur est un instrument de travail pour la moitié des personnes actives, c'est un moyen et une source de loisirs pour à peine plus d'un foyer sur trois (38.7% des foyers étaient équipés d'un micro-ordinateur et 24.3% avaient accès à internet en septembre 2002 - source Médiamétrie/Baromètre multimédia).

L'Internet est passé en quinze ans du stade restreint de mode de communication inter universitaire à celui de réseau planétaire. Cet outil de communication, ouvert à un nombre grandissant d'utilisateurs (en France, fin mars 2003, 6,5 millions de foyers sont équipés d'un accès Internet soit une augmentation de 18% par rapport à l'année précédente)[1], facilite les échanges entre les personnes, les entreprises et donne accès à une infinité d'informations contenues dans une quelconque région du monde. Ainsi, à l'aube du XXI^{ème} siècle, ce réseau joue un rôle d'accélérateur de la mondialisation. Son utilisation devient incontournable et même indispensable pour le rayonnement de l'entreprise qui veut s'imposer dans ce nouveau contexte économique ou pour toute puissance dans sa recherche d'un rayonnement planétaire.

Cependant, la philosophie de liberté d'accès et d'échange qui a prévalu lors de la création de ce mode de communication, et qui anime encore la plupart des utilisateurs, ainsi que la relative simplicité et la standardisation des protocoles employés sont à l'origine de sa grande vulnérabilité. Depuis le début des années quatre-vingt, des génies de l'informatique puis des passionnés mal intentionnés mettent leur talent au profit de la criminalité. Les agressions qu'ils réalisent, sur le réseau ou à travers celui-ci, sont de nature à mettre en danger l'économie mondiale et les grands équilibres politiques.

---

[1] Source : Rapport du 4ème Comité Interministériel pour la Société de l'Information (CISI) du 11 juillet 2003.

Les participants à cet instrument du progrès doivent donc faire preuve de la plus grande prudence en mettant en œuvre des mesures de sécurité strictes et coûteuses et en adoptant des procédures de secours qui garantissent le fonctionnement ou la sauvegarde de leur propre système. Si les facteurs techniques conditionnent une utilisation sûre des nouvelles technologies mises à notre disposition, les comportements humains doivent également s'adapter à la nécessité de protection de ce réseau.

Nul doute que le combat, qui a débuté au tout début des années quatre-vingt, entre les agresseurs du réseau et ceux qui s'organisent pour en assurer la sécurité d'utilisation sera acharné. Sans une volonté farouche de l'ensemble des états, le risque de voir le monde économique et le monde politique gravement perturbés augmente avec l'élargissement de la toile qu'Internet tisse autour du monde.

Nous analyserons, dans un premier temps, la vulnérabilité du World Wide Web[2] c'est-à-dire comment certains individus mal intentionnés peuvent profiter des failles de ce système, quelles sont leurs intentions et les motivations qui les animent dans leurs actions de criminel.

Nous aborderons, dans un second temps, le problème de la protection du réseau et de ses utilisateurs par l'observation des conséquences des agressions graves constatées, la définition des moyens dont les entreprises et les états disposent, et ceux qu'ils doivent inventer pour sécuriser leurs systèmes.

[2] Réseau Internet mondial

1 PREMIERE PARTIE : INTERNET, UN SYSTEME TRES VULNERABLE

Pour l'utilisateur privé, le responsable d'une grande entreprise ou le chef d'état, l'utilisation du réseau mondial Internet lui permet d'élargir ses connaissances, son champ d'action ou son influence. Les premiers sont essentiellement exposés à des dangers d'ordre moral (criminalité liée aux mœurs, à l'incitation à la haine, manipulation d'opinion) ou à une nouvelle forme de vol ou escroquerie dans les transactions financières électroniques qu'ils effectuent. En revanche les deux autres victimes potentielles peuvent voir leurs systèmes de communication ou d'information gravement atteints et leur pouvoir anéanti par une attaque majeure à travers ce réseau.

Sans négliger les dangers qui menacent le particulier dans son exploration de la toile mondiale et auxquels il était déjà confronté par l'utilisation des moyens audiovisuels dont il dispose depuis longtemps, il convient de se pencher sur les véritables agressions que subissent le réseau lui-même et les systèmes d'importance stratégique qui y sont raccordés.

1.1. LES DIFFERENTS TYPES D'ATTAQUE

1.1.1. LES TECHNIQUES EMPLOYEES

Les grands systèmes d'information des entreprises ou des états sont organisés, d'une part, autour d'une capacité de stockage d'informations plus ou moins sensibles. Ils sont constitués, d'autre part, d'un réseau permettant la consultation des données par les personnels de l'entreprise possédant des droits requis ainsi que leur mise à jour par d'autres employés situés sur le « lieu de naissance de l'information », habilités également à réaliser ces mises à jour. Le réseau de l'entreprise est en principe privé. Le réseau Internet, quant à lui, permet de relier certains membres de l'entreprise, donc une partie des ordinateurs de l'organisation, à l'ensemble des sites qui sont connectés sur la toile du « Web ».

Toute atteinte à l'un de ces trois éléments de la communication d'entreprise, ou communication opérationnelle pour un état, entraîne un dysfonctionnement qui peut provoquer l'effondrement de cette organisation.

1.1.1.1. La pénétration des systèmes d'information

Une des techniques peut consister à s'introduire dans le système même de stockage des données afin de les supprimer complètement ou de les modifier en agissant directement sur le système. Celui qui s'introduit dans le système peut agir plus discrètement et se contenter de voler les informations les plus importantes de l'entreprise. Lorsque le réseau de l'entreprise est relié à Internet, l'agresseur peut agir depuis n'importe quel endroit du monde en empruntant des circuits indirects pour atteindre sa cible via plusieurs serveurs du réseau. Dans le cas général, le réseau local (LAN[3]) de l'organisation n'est pas connecté à Internet. Pour pratiquer cette intrusion, il convient alors d'intervenir à partir du réseau même de l'organisation et donc utiliser un ordinateur d'un membre de l'entreprise. Cette opération est compliquée et demande une préparation de l'environnement importante (intrusion dans les locaux, connaissance des mots de passe…). Depuis l'explosion du réseau Internet cette technique n'est que très rarement utilisée.

1.1.1.2. Les attaques indirectes

L'architecture et le mode de fonctionnement de ce dernier permettent des techniques plus indirectes, plus discrètes et donc plus efficaces.

En effet, la corruption des données ou du logiciel de l'entreprise peut également être obtenue en envoyant un petit programme (virus) qui fera lui-même ce travail alors que l'auteur de l'agression n'est plus connecté au réseau. Ce dernier est naturellement bien moins détectable, donc identifiable, que dans le premier cas. Ce mode d'action par agression différée est d'ailleurs le plus courant. Il utilise également des variantes du virus qui sont des programmes qui se reproduisent pour infecter un nombre toujours croissant d'ordinateurs (les vers) ou bien qui sont programmés pour agir de manière différée, à une date précise (les bombes logiques) ou enfin qui s'insèrent dans un programme existant et s'active au lancement de ce dernier (les chevaux de Troie).

Ces techniques permettent de contourner la séparation des deux réseaux (Internet et celui de l'entreprise) puisque ce programme peut se loger dans un banal fichier de travail et être transmis par disquette ou sur tout autre support amovible entre l'ordinateur relié à Internet et celui du réseau de la société.

1.1.1.3. La circulation de l'information

Au-delà de l'atteinte physique de leur système d'information, il existe, pour l'entreprise ou l'Etat, des menaces tout aussi destructrices qui peuvent être véhiculées par le réseau mondial de communication électronique. En effet la simple divulgation massive d'information, volontairement erronée, sur ce média peut constituer une attaque majeure pour une entreprise ou un état.

1.1.1.4. La saturation du réseau

Il existe aussi une manière encore plus insidieuse et plus désastreuse encore pour l'Internet dans son ensemble. Elle consiste à créer une saturation des principaux serveurs gérant les domaines du réseau par l'envoi de programmes qui génèrent une diffusion croissante de messages. Ces messages saturent tous les serveurs des FAI[4] et bloquent complètement les accès et toutes les communications sur la toile. Cette technique entraîne la paralysie du réseau mondial durant une période limitée (une ou quelques journées), le temps de découvrir un « anti-virus » qui détruise le programme générateur de ces messages. La question se pose alors de trouver une méthode sûre de diffusion rapide de ce dernier à tous les utilisateurs, alors que le réseau n'est plus opérationnel.

1.1.2. LES DIFFERENTS TYPES DE CRIMES

Après avoir balayé les différentes techniques employées par les délinquants du W.W.W.[5], nous allons voir quels objectifs ils visent dans leurs offensives.

1.1.2.1. Les crimes contre le particulier

La criminalité qui concerne le particulier est très présente sur le réseau. En effet, le nombre d'infractions financières (escroquerie à la carte bancaire en particulier) ou liées aux mœurs (pornographie, pédophilie) ou encore concernant l'incitation à la haine ou à la violence ne cesse de croître. Ces atteintes aux particuliers ont un impact non négligeable sur la moralité, la morale ou le moral d'une nation et contribuer ainsi à son

---

[3] Local Aera Network : Réseau local. Par opposition à WAN : Wide Aera Network

[4] Fournisseurs d'Accès à Internet

[5] World Wide Web

déclin. Cependant, sans en négliger l'importance, nous ne nous attarderons pas sur l'étude de cette criminalité.

La partie de la cyber-criminalité qui nous préoccupe est celle qui contribue de manière plus directe à la déstabilisation d'un état ou à la chute d'une puissance économique, cette chute ayant une influence et des retombées sur les grands équilibres mondiaux.

1.1.2.2. Le piratage

Le piratage des biens culturels constitue une atteinte grave aux entreprises qui vivent grâce à son commerce. Ainsi les auteurs d'œuvres d'art ou de produits culturels voient leur droits bafoués et leur revenus baisser de manière dangereuse. Les sociétés de production sont également mises en danger. En effet, la démocratisation des graveurs de Cédérom a fragilisé les créateurs de logiciels informatiques, notamment les outils de bureautique classiques et les jeux vidéo. L'invention du format de compression de fichiers musicaux (MP3) et de fichiers audiovisuels (DIVX) accompagné de lecteurs de salon compatibles avec ce format provoque une crise grave dans l'économie liée à la musique et au cinéma.

Ce phénomène de piratage est, de plus, accentué par le mode de téléchargement de ces fichiers entre les particuliers reliés à Internet par la technique appelée Peer to Peer. Celle-ci permet à chaque internaute, équipé du logiciel qui convient, d'accéder à une partie du disque dur de tous les autres à condition que ceux-ci aient également installé ce même logiciel.

1.1.2.3. La désinformation

La mise à disposition d'une information dans le monde entier en un temps extrêmement court peut être un moyen également utilisé par les délinquants.

Ainsi, la désinformation peut constituer une agression fatale pour une grande société qui verra sa production accusée des pires maux et devenir invendable. Le lancement d'une campagne de désinformation par le réseau Internet peut rapidement être diffusée dans le monde entier, faisant perdre ainsi à la société victime une grande partie de sa clientèle habituelle ou potentielle.

L'action d'un état pourra de la même manière être complètement discrédité et

son gouvernement confronté à une crise politique majeure lui coûtant le pouvoir. Le caractère mondial du réseau et la rapidité de divulgation de l'information constitue une arme redoutable à l'usage du criminel. De la même manière une nation peut subir une attaque logique consistant en une pénétration de son site institutionnel « Web » pour y laisser des messages revendicatifs. Une telle technique fut employée à partir de Hong-Kong sur le site de la Maison Blanche lors des bombardements sur l'ambassade de Chine à Belgrade par les forces de l'OTAN.

1.1.2.4. L'espionnage

L'espionnage par l'appropriation d'informations sensibles dont peut être victime n'importe quelle puissance (étatique ou industrielle) n'est pas un phénomène nouveau. Aujourd'hui Internet représente une porte d'entrée privilégiée dans les dossiers confidentiels conservés sur support numérique, dans le serveur de données de l'entreprise. L'acte d'espionnage peut également consister à intercepter des documents de travail circulant sur le réseau de l'organisation. Il est encore plus aisé de pratiquer cette interception sur le réseau Internet lorsque les membres de l'organisation visée y font circuler ces informations.

1.1.2.5. Atteinte au fonctionnement du système d'information d'un état

Une agression plus dure des sites fondamentaux d'un état peut également être réalisée au travers du réseau, par le biais d'intrusion directe ou par l'utilisation de programmes véhiculés par ce dernier. Elle pourrait viser à une destruction d'une partie au moins du système opérationnel d'un gouvernement jusqu'à le fragiliser et le mettre en grand danger. Réalisée dans un contexte tendu ou en coordination avec d'autres actions politiques ou médiatiques fortes, une telle attaque peut devenir fatale pour cet état.

1.1.2.6. Préparation d'attentats

On ne peut évoquer la mise en danger d'un état par l'utilisation du réseau Internet sans évoquer le terrorisme. Ce moyen de communication mondial a permis de préparer et de coordonner l'agression contre les deux tours du World Trade Centre et du Pentagone le 11 septembre 2001. Certains sites diffusent des techniques d'actions révolutionnaires, de combat, de lutte sous toutes les formes imaginables jusqu'à des recettes de préparation de bombes artisanales ou plus sophistiquées.

Naturellement, les groupes terroristes, tout comme le grand banditisme, ont recours au réseau mondial pour pratiquer le blanchiment d'argent, les jeux illégaux ou pour organiser les différents trafics (armes, stupéfiants, êtres humains) liés de manière directe ou indirecte à leur objectif fondamental de déstabilisation des puissances politiques.

1.1.2.7. Associations diverses

L'équilibre mondial ou du moins les tentatives d'organisation d'une mondialisation des politiques économiques et commerciales peuvent également être menacées par les nouveaux mouvements qui utilisent Internet dans leur mode de communication, d'information et surtout de recrutement. Ainsi les anti-mondialistes et, plus tard, les alter-mondialistes ont-ils vu leur mouvement prendre très rapidement une ampleur telle que les gouvernements devront prendre en considération leurs revendications dans tous les grands rendez-vous constitués par les sommets type G8 à Evian ou ceux de L'Organisation Mondial du Commerce. D'une manière générale, toute organisation non gouvernementale dispose, avec le réseau Internet, d'un mode de communication lui permettant d'acquérir rapidement une audience importante et donc l'influence nécessaire à l'efficacité des actions qu'elle prévoit d'engager.

1.1.3. LES CIBLES

L'inventaire des infractions que le réseau Internet permet de commettre ou dont il facilite la commission nous a permis d'identifier les principales victimes de la cyber-criminalité.

1.1.3.1. Les particuliers

En effet, dans un premier temps les particuliers qui disposent de l'équipement nécessaire à leur connexion au réseau peuvent devenir victimes d'escrocs ou de voleurs. Ils peuvent également subir des pressions fortes ou des influences qui modifient leur manière de penser et affectent leur moral ou leur moralité jusqu'à créer un danger collectif dans une société organisée. La fragilité économique, sociale ou les carences de l'éducation peuvent largement amplifier le phénomène et plonger certains d'entre eux dans le désespoir ou les faire se tourner vers des organisations sectaires, mafieuses ou extrémistes voire terroristes.

Cette fragilisation des individus constitue naturellement un danger pour les démocraties dont le fonctionnement repose sur un comportement globalement sain des populations. C'est donc essentiellement à ce titre que les criminels les plus dangereux pour les grandes puissances peuvent choisir de prendre pour cible chacun des internautes utilisant régulièrement cet outil de communication et d'information.

1.1.3.2. Les acteurs de l'économie mondiale

La deuxième cible importante pour le criminel ayant l'intention de déstabiliser les grands équilibres planétaires est constituée des sociétés ayant une économie régionale ou mondiale. Les grandes industries ayant une production très importante à travers le monde peuvent subir des agressions visant à discréditer la qualité du produit par une campagne d'information « éclair » diffusée dans les pays clients ou clients potentiels de cette entreprise.

Une société ayant une compétence unique dans un domaine particulier peut subir une intrusion dans son système informatique afin de corrompre ou voler les données sensibles sur des dossiers confidentiels. C'est le fruit de plusieurs années d'effort et l'avance sur les concurrents qui se trouvent ainsi anéantis. Si le danger de l'attaque par le réseau menace les entreprises sensibles par leur taille ou leur domaine d'étude, ce même danger guette également et de manière plus fréquente les petites et moyennes entreprises ou industries dont la puissance financière leur permet de construire un système d'information adapté à un fonctionnement moderne et compétitif mais qui n'ont pu consacrer suffisamment de moyens techniques à la sécurité de ce dernier.

1.1.3.3. Les états

Enfin les états sont des cibles également privilégiées pour les criminels les plus audacieux ou les plus déterminés. Les systèmes d'information fondamentaux des états subissent un nombre grandissant de tentatives (avouées) de pénétration. Si celles-ci n'ont pas réussi aujourd'hui à dégradé de manière significative ces derniers, les gouvernements considèrent ce risque comme majeur. L'utilisation de virus pour perturber l'ensemble du réseau Internet est un bon moyen de priver les grandes puissances d'un moyen efficace de communication. Si, de plus, ce virus est capable de s'introduire sur le réseau interne du gouvernement, le résultat peut être désastreux pour l'organisation des services étatiques.

Compte tenu des outils dont disposent les criminels du « Web » et de l'importance que revêtent aujourd'hui les systèmes d'information dans l'organisation de la vie de l'entreprise ou d'un gouvernement moderne, il apparaît clairement que l'attaque de ses systèmes peut porter un coup fatal à l'équilibre économique ou politique mondial.

Le réseau Internet, qui relie avec une technologie simple et standardisée un nombre de serveurs et d'ordinateurs personnels ou d'entreprise en augmentation exponentielle, facilite l'accès direct ou indirect à ces systèmes d'informations stratégiques. Il constitue à ce titre un vecteur privilégié, rapide et parfois spectaculaire des agressions contre ces puissances économiques et politiques.

1.2. LES MOTIVATIONS DE L'AGRESSEUR ET LES FACTEURS ENCOURAGEANT

Si les techniques qui ont été adoptées dans la création du réseau Internet et son succès, donc son expansion à travers le monde, constituent les éléments clés de son utilisation pour des manœuvres délictueuses et criminelles, ils n'expliquent pas à eux seuls les raisons pour lesquelles ce mode de délinquance est en aussi grande augmentation. L'ampleur inquiétante que prend ce phénomène est également liée au profil particulier de ce cybercriminel.

Les délinquants qui se contentent de pirater des logiciels, de reproduire des œuvres d'art sans autorisation ou ceux qui utilisent le réseau uniquement comme diffuseur d'informations doivent posséder un niveau minimum de connaissances informatiques. La catégorie supérieure est représentée par ceux qui sont décidés à créer des virus ou d'autres programmes agressifs, ainsi que ceux qui tentent de pénétrer des systèmes d'information à distance. Ces spécialistes de la cybercriminalité doivent posséder une compétence technique de très haut niveau, constamment remise à jour et un niveau intellectuel élevé leur permettant d'analyser les organisations afin de détecter les points d'entrée et les méthodes pour réussir leur attaque. Enfin, il leur faut disposer d'un matériel adapté et de suffisamment de temps pour développer leur arme virtuelle.

1.2.1. LES MOTIVATIONS DES AGRESSEURS

Au début de l'aire de l'informatique, il était assez aisé de connaître la liste des personnes capables de réaliser de tels actes. Aujourd'hui, leur identification est nettement plus difficile mais on peut essayer de connaître les motivations qui les

poussent d'un usage ludique ou professionnel de l'outil informatique vers la cybercriminalité et l'attaque des systèmes d'information.

1.2.1.1. Le joueur

Les premiers délinquants de l'informatiques ont commencé à sévir au début des années quatre-vingt en tentant de pénétrer des systèmes informatiques de grandes entreprises (les seules à posséder de telles installations), certains y parvenant. Pour ces premiers « bidouilleurs » informatiques, des as de la programmation, l'objectif est de faire évoluer leurs connaissances et de satisfaire leur curiosité naturelle. Ce sont des joueurs qui rivalisent d'ingéniosité entre eux en considérant les différents niveaux d'intrusion comme des « unités de valeur ». C'est donc le défi technologique et l'esprit de compétition qui sont leurs principaux moteurs. A ces deux notions, peut se rajouter la volonté d'obtenir une certaine reconnaissance parmi ses pairs, notamment pour le jeune adolescent débutant dans la partie. Cette catégorie de délinquants qui ont commencé à sévir dès les balbutiements du réseau ont été baptisés « hackers[6] ».

Ces premiers épisodes de la guerre informatique font l'objet de films[7] qui posent déjà le problème de vulnérabilité des systèmes fondamentaux de l'état tout en popularisant le phénomène du « cybercrime ». Ces fameux « hackers » affirment n'avoir aucune réelle intention criminelle et se défendent donc d'appartenir à la catégorie des pirates ou des « crackers[8] ».

1.2.1.2. Le vengeur

Ce n'est qu'en 1986 et au Pakistan que le premier virus informatique est détecté alors qu'il se propage et infecte les ordinateurs IBM. Cette technique est cette fois destinée à nuire. Elle est alors particulièrement adaptée à un autre type de délinquant : le vengeur. Celui-ci est essentiellement préoccuper par la volonté de faire mal à un

---

[6] Le profil le plus courant du « hacker » est l'étudiantqui a le temps et la persévérance de rester devant son ordinateur durant des heures entières. On distingue quatre niveaux de compétence, du débutant à l'expert : les « Curious Joe », les « Script Kiddies », les « Wannabes » et enfin les « Elites ».

[7] Le film War Games sortie en 1983 raconte comment un jeune adolescent parvient à pénétrer le système informatique gérant les scénarios de guerre nucléaire des Etats-Unis et à provoquer une réaction en chaîne conduisant au déclenchement du feu nucléaire sur l'empire soviétique.

[8] Le terme de « crackers » s'applique pour les « hackers » criminels. Les « crackers » existent à différents niveaux. Cela va du petit délinquant au cyberterroriste gouvernemental en passant par le crime organisé.

individu ou à une entreprise qui se serait passé brutalement de ses services. L'attaque est soudaine et bien souvent efficace, puisque l'auteur connaît bien le système sur lequel il a travaillé mais demeure limitée à une seule cible. Il peut également être animé par l'appât du gain mais ce ne sera qu'une raison secondaire et elle ne lui donnera pas l'énergie nécessaire pour persévérer dans la recherche longue et difficile du moyen d'agir et le courage de passer à l'acte.

1.2.1.3. L'escroc

Certains délinquants sont animés, eux en priorité par le désir de s'enrichir et s'orientent alors vers s'escroquerie ou le vol. Ceux-là considèrent les techniques informatiques et le réseau comme un nouvel outil de travail et font des efforts pour s'adapter à ce nouveau mode opératoire. Ils se limitent généralement à une délinquance financière la plus discrète possible afin de durer et de vivre de leurs méfaits. Lorsque ces délinquants souhaitent s'attaquer à des systèmes réellement sophistiqués, il leur faudra recruter des techniciens de haut niveau qui appartiennent déjà parfois à la catégorie des « hackers » ou directement parmi le personnel de l'entreprise visée.

1.2.1.4. La criminalité organisée

Dans la criminalité organisée, le chef de l'organisation répond à une logique de puissance et obéit à une stratégie offensive dans laquelle la recherche du gain maximal par des procédés multiples et variés reste une constante. Etant présent dans les autres formes de criminalité, il bénéficie d'un grand pouvoir de persuasion et de gros moyens pour recruter les personnes capables de mettre en œuvre les techniques de piratage nécessaires à son action. Ne reculant devant rien, il est dépourvu de tout sentiment national, religieux et entreprend tout pour affirmer sa toute puissance. Le milieu dans lequel il évolue lui impose ce comportement sous peine de disparaître du paysage de manière parfois expéditive. Il puise donc sa motivation dans son désir de puissance et son instinct de survie.

1.2.1.5. Le terroriste

Cousin germain du crime organisé, le terrorisme produit lui aussi des individus prêts à tout tenter pour imposer leur puissance, celle de leur « idéologie ». Internet constitue pour le terroriste le moyen idéal de diffuser ses idées à travers le monde entier, d'échanger des techniques d'action, de recruter de nouveaux adeptes. L'anonymat du

réseau mondial lui permet aussi d'utiliser les techniques de pénétration ou de saturation des réseaux pour détruire une entreprise ou paralyser les systèmes de communication ou d'information d'un état. Complètement exalté par la cause qu'il défend, il est prêt à tous les sacrifices pour atteindre son objectif. Le spécialiste informatique du groupe terroriste sera soutenu dans son apprentissage des techniques informatiques et pourra s'y consacrer totalement, à l'image des prisonniers condamnés à de longues peines qui sont dans les meilleures conditions pour se lancer dans l'écriture d'un mémoire, d'une thèse ou d'un livre.

1.2.2. LES FACTEURS ENCOURAGEANTS LE CRIME

Les raisons fondamentales qui poussent le criminel à agir sont amplifiées par des facteurs extérieurs qui ont un effet dopant pour ce passionné de la fraude. Sa motivation se trouve ainsi décuplée ainsi que son énergie. Ces facteurs sont les particularités de la société dans lequel il évolue et qu'il ressent de manière exacerbée, compte tenu du manque de règles élémentaires d'éducation qui ont caractérisé son évolution.

1.2.2.1. La disparition des références morales ou religieuses

En effet, la disparition progressive des références morales ou religieuses constitue le premier facteur. Les nations occidentales en particulier sont passées, depuis les années soixante et soixante dix, d'une situation où l'autorité des institutions et la rigueur dans le comportement des citoyens étaient les moteurs de la reconstruction d'après-guerre à une situation où le rêve de la liberté individuelle et l'imagination semblait devoir guider l'homme sur le chemin du progrès vers un monde nouveau de paix et d'amour.

Cela s'est traduit par une dérive dans les principes d'éducation des enfants et des adolescents qui sont devenus libres de construire leur personnalité par la méthode de la découverte et la liberté d'expression. La disparition de l'autorité parentale (les parents ne sont jamais sanctionnés pour les délits commis par leurs enfants mineurs), les techniques d'éducation expérimentées après 1968, le vent de liberté soufflant dans le même temps et l'indulgence générale régnant face à la délinquance juvénile ont libéré les jeunes d'hier et d'aujourd'hui de toute règle comportementale et ont permis à un grand nombre d'entre eux de s'épanouir pleinement dans l'accomplissement de leurs méfaits. Internet, symbole de liberté d'expression et de communication est devenu un

outil privilégié pour ces jeunes en quête d'aventure cybernétique.

1.2.2.2. Société de consommation et pauvreté persistante

Cette évolution des mœurs des sociétés occidentales n'est pas étrangère aux formidables progrès techniques qui ont été réalisés après la seconde guerre mondiale. Ceux-ci ont permis d'améliorer de manière spectaculaire la qualité de vie des habitants de l'hémisphère Nord qui passent ainsi d'un mode de vie tourné vers la recherche de la satisfaction des besoins à celui tourné vers la recherche de la satisfaction des envies. C'est la naissance de la société de consommation et des loisirs. Les images de cette société idéalisée par les puissances économiques occidentales sont véhiculées dans le monde entier par les médias, la télévision en particulier, mais aussi par le réseau Internet lui-même.

Ces images entraînent ceux qui les regardent dans le désir irrépressible de posséder tous les produits de confort et de luxe disponibles sur le marché tandis que les plus défavorisés ressentent un sentiment de frustration qui ne fait que s'accentuer au fur et à mesure que se creusent les écarts entre les différentes couches sociales au sein d'un même pays et les différences entre les pays les plus pauvres et ceux dont l'économie s'est envolée. Ce sentiment de haine qui naît de ce contraste insupportable est accentué par l'étalage, dans certaines émissions de télévision, d'un mode de vie fait de luxe inutile, de gaspillage et de débauche. Il entraîne alors un besoin de vengeance d'un monde injuste qui pénalise irrémédiablement ceux qui vivent dans la pauvreté.

1.2.2.3. La célébrité médiatique glorifiée

Parallèlement à cet étalage outrancier de luxe futile, et en conséquence directe de cette tendance à l'« hyper-médiatisation » des nouvelles normes d'un mode de vie moderne, on découvre dans ces émissions de télévision ou dans les magazines populaires les nouveaux héros qui font rêver les jeunesses de tous les pays. Naturellement, ils ne sont pas sélectionnés sur le niveau d'étude ou sur les résultats obtenus au sein de leur entreprise, mais plutôt sur leur originalité ou sur le spectacle qu'ils peuvent offrir au spectateur avide de sensations toujours plus fortes. La recherche de cette gloire passagère constitue encore un élément qui encourage le criminel à se dépasser pour réussir une opération qui le rendra, à son tour, célèbre dans le monde entier. Le réseau Internet sera, par ailleurs, le bon moyen de promouvoir ses exploits et

encourager de nouveaux prétendants au titre de cybercriminel de l'année.

L'ensemble de tous ses facteurs qui sont inséparables de notre nouveau mode de vie et de nos sociétés à l'économie développée, encourage le délinquant en agissant directement sur son affectif et en amplifiant une passion déjà génératrice de son comportement criminel.

C'est sur le réseau Internet, simple d'utilisation, accessible à tous et qui constitue un terrain de manœuvre virtuel idéal où l'anonymat est facilement conservé, que cette passion exacerbée peut le plus aisément s'exprimer. Elle constitue le moteur de la criminalité sur le réseau et donc la carte maîtresse dans le jeu du cybercriminel.

La question est alors de savoir si les mesures de sécurité qui sont déployées sont capables de faire face à cette force délinquante qui s'abat sur le plus célèbre et le plus utilisé des réseaux de communication dans le monde.

2 DEUXIEME PARTIE : LA PROTECTION DU SYSTEME, UNE NECESSITE

L'étude des vulnérabilités du réseau Internet nous a permis de rappeler les différentes techniques dont disposent les cyber-criminels pour transformer un outil de communication mondial exceptionnel d'efficacité en un théâtre d'une guerre sans merci contre les acteurs majeurs des grands équilibres mondiaux. Dans ce nouveau siècle qui s'offre à nous, à l'heure de la mondialisation des économies et des politiques, les nations occidentales qui possèdent l'avantage technologique et industriel et qui sont les principales utilisatrices de ce réseau subissent des attaques multiformes en nombre croissant d'année en année.

Ces attaques entraînent des pertes financières, des effondrements de sociétés commerciales et une menace permanente pour les systèmes d'information et opérationnels des nations. L'organisation de la protection des utilisateurs d'Internet doit impérativement être définies et mise en place rapidement dans le monde entier pour que ce facteur accélérateur de la mondialisation et du progrès ne devienne la cause d'un séisme économique ou politique mondial.

2.1. LES CONSEQUENCES, LES RISQUES

Les conséquences de la criminalité sur le réseau Internet et sur les systèmes d'information qui en dépendent, sont difficiles à chiffrer précisément. Les victimes d'une attaque informatique, lorsqu'elles jouissent d'une certaine notoriété en particulier, ne sont pas enclines à révéler leur mésaventure afin de protéger leur image et leur crédibilité. Quelques sondages, les comportements des grands organismes qui, depuis quelques années, prévoient des budgets importants pour la sécurité de leurs systèmes, ainsi que quelques chiffres d'organismes officiels nous permettent cependant d'évaluer l'importance des dégâts déjà constatés et du niveau grandissant de la menace.

2.1.1. SOCIAUX

La première partie de notre étude nous démontre que le réseau mondial Internet a la capacité d'atteindre le moral des populations en diffusant les images d'un mode de vie propre aux pays riches dans toutes les parties du monde, provoquant ainsi une

exacerbation, chez les habitants des pays victimes de la pauvreté, d'une haine envers ceux qui possèdent toutes les richesses. Difficilement mesurable, cette notion transparaît cependant toujours en filigrane dans la montée de l'extrémisme religieux et du terrorisme.

La moralité des populations les plus vulnérables est sans cesse malmenée par la multiplication de sites incitant à la haine et par la diffusion d'images pornographiques ou pédophiles. Le ministre de l'intérieur français annonce en septembre 2003, lors du 4ème forum mondial de « l'i-démocratie » à Issy-les-Moulineaux une progression de 637 à 7.584 du nombre de sites pédophiles signalés en deux ans en France.

2.1.2. ECONOMIQUES

Si les dégâts de la cybercriminalité sur le plan social n'interviennent qu'indirectement comme facteur susceptible de participer au bouleversement des grands équilibres mondiaux, les grandes entreprises peuvent très rapidement payer le prix fort d'une attaque réussie. Quelques chiffres démontrent l'importance du risque et l'augmentation inquiétante du nombre d'agressions. Ainsi en 2003 on estime que la fraude sur les cartes bancaires s'élève à quelques 400 millions de dollars par an. Les attaques par virus ont été chiffrées à près de 12 milliards de dollars. Enfin, le manque à gagner pour les industries victimes d'atteintes à la propriété intellectuelle et de contrefaçons atteindrait 250 milliards de dollars par an soit près de 5% des échanges mondiaux.

Un indicateur démontre également la fragilité du tissu économique des petites et moyennes entreprises ou industries. En effet, 60% de celles qui ont été victimes d'un sinistre informatique disparaissent dans les cinq années suivantes.

Même si aucun chiffre ne le précise, le risque d'attaque d'un site vital comme celui d'une bourse pourrait provoquer une crise économique mondiale importante et bouleverser complètement l'organisation des marchés financiers.

2.1.3. POLITIQUES

Aux Etats-Unis, le Pentagone à lui seul, a enregistré en un an plus de 22.000 agressions électroniques contre ses systèmes et le FBI a recensé 5.000 infrastructures « extrêmement vulnérables » à la criminalité informatique capable de « déstabiliser l'économie entière d'un pays ». En France, monsieur Sarkozy annonce 1.126 agressions

informatiques (attaques de réseau) pour l'année 2002 et déclare que 300 sites gouvernementaux ont été attaqués. Ces chiffres démontrent la réalité du danger qui plane sur les états de voir leurs systèmes de communication et de décision gravement endommagés.

L'élargissement de la toile cybernétique tissée tout autour de la planète offre aux criminels un nombre de plus en plus important de cibles potentielles. Les attaques les plus redoutables, menées par des délinquants bien formés et passionnés par le défi technologique, sont menées contre les grands acteurs économiques mondiaux ou contre les états puissants disposant de la suprématie dans le domaine des télécommunications et de l'informatique. Cette augmentation mondiale du nombre d'abonnés au réseau, implique dans le même temps une augmentation du nombre de délinquants l'adoptant comme outil de travail.

2.2. LES REPONSES TECHNIQUES

Tant que les réseaux des entreprises demeuraient privés, coupés du monde extérieur (en utilisant des technologies propriétaires notamment), les risques d'intrusions et de piratage étaient plus faibles. Avec le développement d'Internet et l'interconnexion de la plupart des systèmes via le protocole IP les risques au niveau de la sécurité informatique ont été fortement accrus. Les moyens techniques pour se protéger des attaques de cybercriminels sont nombreux, néanmoins ces parades sont très standards et ne permettent de se protéger que de la grande masse inexpérimentée des « hackers ». Voici une typologie des moyens qu'une entreprise peut mettre en œuvre pour se protéger et se sécuriser.

2.2.1. SUR LES SERVEURS D'ENTREPRISE ET LES ORDINATEURS PERSONNELS

La partie la plus sensible du système d'information étant les serveurs de données ou d'application, c'est en priorité cette partie du système qu'il est impératif de sécuriser. Les différentes couches logicielles d'un ordinateur offrent la possibilité de verrouiller l'accès aux données par un nom d'utilisateur et un mot de passe. Il en est de même pour l'application informatique qui agit sur ces données. L'administrateur du système attribue les droits d'accès en fonction des instructions qu'il reçoit de la direction de l'entreprise.

2.2.1.1. L'authentification

Les systèmes d'information sont de plus en plus ouverts vers l'extérieur du fait de l'interconnexion entre les sites à distance, les postes nomades et le réseau principal de l'entreprise. C'est la raison pour laquelle l'identification est devenue un enjeu crucial en terme de sécurité. L'authentification est une procédure qui permet d'autoriser chaque utilisateur d'un ordinateur l'accès à un type d'information

Parmi les nombreuses techniques d'authentification on trouve :

- Les mots de passe.
- Les mots de passe uniques : ils ne servent que pour une requête et sont invalidés juste après.
- Les cartes à puces :le principal intérêt de la carte à puce c'est que l'utilisateur doit la posséder physiquement pour l'utiliser et souvent la compléter par des données que seul l'utilisateur connaît (code par exemple).
- Les super cartes à puces : ce sont des cartes à puce de dernière génération qui comportent un clavier, un écran et une source d'énergie autonome. Ce type de cartes ne nécessite pas de terminal ou de réseau pour fonctionner.
- Les caractéristiques biométriques : empreintes digitales, vocales, signatures.
- Le chiffrement : la possession d'une clef de chiffrage

Ces droits d'accès sont différentiés en fonction des règles de protection du secret habituelles régenter la le principe du « droit d'en connaître ». Nul ne peut avoir accès aux informations qui ne sont pas nécessaires à l'accomplissement de son travail.

2.2.1.2. Protection des postes nomades

Les risques concernant les postes nomades sont de plus en plus élevés. Non seulement les données contenues dans ces postes peuvent être sensibles mais si ces postes sont détournés, ils peuvent servir de point d'entrée dans le système informatique de l'entreprise. Les réponses à ces préoccupations sont le recour à un VPN, virtual private network qui consiste à un cryptage point à point, une utilisation stricte des procédures d'authentification ou encore l'utilisation de solution de chiffrement et de protection au démarrage.

2.2.2. SUR LES RESEAUX D'ENTREPRISE

Entre l'ordinateur individuel et le serveur applicatif, le réseau de l'entreprise constitue un lien qu'il convient également de protéger. Les protections citées auparavant

s'appliquent au serveur dédié à la gestion du réseau avec les mêmes restrictions d'accès aux parties du réseau qui sont nécessaires dans l'exécution de la tâche de l'agent. La plus grande précaution réside dans la séparation absolue du réseau de l'entreprise avec Internet. La mise en place et le paramétrage des « sas » de protection, appelé « firewall ».

2.2.2.1. Les firewalls

Le « firewall » est l'un des moyens les plus fréquents de se protéger : c'est une passerelle entre le réseau de l'entreprise et Internet. C'est un point de filtrage et de contrôle de l'activité de ces réseaux. Chargé d'interdire ou d'autoriser les flux d'informations en entrée ou en sortie, il protège le réseau interne de l'entreprise des accès non autorisés provenant de l'extérieur ainsi que de garantir un certain niveau de sécurité entre le réseau interne et les machines extérieures à celui-ci (typiquement dans le cadre d'un VPN, « virtual private network »). Concrètement, un « firewall » est souvent une machine, un serveur avec un logiciel qui fait le pont entre ces deux réseaux (internet - internet ou deux réseaux internes avec des niveaux de sécurité différents). Le logiciel est chargé du filtrage des « packets » en fonction de leurs caractéristiques : type, source, destination. En outre, le « firewall » permet également un contrôle au niveau applicatif ce qui permet de bloquer le recours à certains outils non autorisés.

2.2.2.2. La détection d'intrusion via un NIDS[9]

La détection d'intrusion (IDS) complète souvent un « Firewall ». Elle permet une surveillance en temps réel des réseaux par une écoute permanente couplée à une réponse adaptée en fonction des anomalies. Là où le « Firewall » se contente d'accepter ou de refuser les requêtes, un système de détection des intrusions permet la mise en œuvre de mesure appropriées comme la déconnexion immédiate des intrus, le lancement de programmes « ad-hoc » ou l'alerte des administrateurs du réseau en cas d'attaque.

2.2.2.3. Le filtrage de contenu

L'idée est de contrôler les échanges d'information au sein de l'entreprise et aussi par rapport à l'extérieur. Parmi les pratiques à proscrire, on trouve l'utilisation non

[9] Network Intrusion Detection System

professionnelle de la messagerie, le non-respect de la confidentialité, le « spamming » (mail non sollicité), le « spoofing » (usurpation d'identité pour le mail), la transmission de virus...

2.2.3. SUR LE NET

La protection sur le réseau Internet est essentiellement réalisée par le cryptage des informations qui y circulent mais aussi par diverses autres techniques qui agissent sur les transactions effectuées sur ce réseau.

2.2.3.1. Le chiffrement (cryptage des données)

Le but premier du chiffrement a été bien entendu la garantie de la confidentialité des informations transmises par l'armée et le gouvernement. Avec le développement des réseaux et de l'informatique non militaire, le cryptage s'est fortement répandu. Les enjeux se sont aussi fait plus pressants avec le développement du commerce électronique qui impliquait la garantie de la sécurité des transactions et notamment de la préservation de la confidentialité des numéros de cartes bancaires. Le chiffrement est très usité entre les banques, les entreprises, les organismes financiers et même les particuliers.

Le principe du chiffrement est le suivant : l'idée c'est de transformer l'information de manière à ce qu'elle ne soit pas compréhensible par une personne non destinataire. Ainsi l'information peut transiter par des canaux publics sans que la confidentialité de la transmission ne soit remise en cause. Il existe plusieurs méthodes de chiffrage :

- Le chiffrement symétrique

La source et la destination de l'information disposent de clé de chiffrement à utiliser avant la transmission de l'information. C'est cette même clé qui va servir à crypter et à décrypter le message.

- le chiffrement asymétrique

Là, il existe deux types de clés : une clé publique qui est à la disposition de tous et qui permet de crypter le message et une clé privée qui seule permet de déchiffrer le message. L'avantage principal de ce type de cryptage est qu'il évite l'échange de clé même par des canaux publics hautement sécurisés.

A noter que le chiffrement est considéré comme une arme de guerre. En France le chiffrement est autorisé depuis 1999 si la longueur des clés ne dépasse pas 128 bits. Il faut une déclaration préalable auprès des autorités concernées pour toute utilisation de

clés de cryptage entre 40 et 128 bits.

2.2.3.2. SSL[10]

SSL signifie Secure Socket Layer et a été créé par Netscape. Il se matérialise par l'apparition d'une petite clé dans le navigateur. Cette clé brisée devient entière si la transaction est sécurisée avec le SSL. Le SSL est donc un protocole d'échange d'information qui permet de garantir confidentialité, intégrité des échanges ainsi que l'authentification des parties. Le fondement de ce protocole est l'algorithme de chiffrement à clé publique RSA (de Rivest-Shamir-Adleman, ses créateurs). Deux paires de clés - une pour le verrouillage et l'autre pour le déverrouillage - à 40 bits sont utilisées.

2.2.3.3. Le protocole SET

Protocole spécialement créé par Visa et Master-Card pour sécuriser les transactions en ligne, son champ d'action se restreint au seul chiffrement des données bancaires alors que SSL permet aussi que crypter images et texte. Les trois éléments qui entrent en ligne de compte dans le processus de sécurisation sont : le client, le vendeur et la banque du vendeur. Les certificats du client et du vendeur sont communiqués par leurs établissement bancaire respectif avant que la transaction soit réalisée. Avec ce type de transaction, le vendeur n'entre jamais en connaissance du numéro de carte bleue, une personne malintentionnée ne peut donc pas non plus faire un usage frauduleux de ce numéro.

2.2.3.4. La PKI ou Public Key Infrastructure

Cette infrastructure regroupe tous les éléments requis par une autorité de certification afin de permettre l'émission des certificats à un ensemble d'individus ou de réseaux ainsi que l'administration de ces certificats. Un certificat identifie deux entités distantes qui souhaitent communiquer ensemble.

---

[10] protocole le plus répandu dans la sécurisation des transactions

2.3. LES REPONSES ORGANISATIONNELLES

Toutes les mesures de protection créées par les informaticiens, avec leurs propres techniques, sont susceptibles d'être contournées par leurs créateurs eux-mêmes ou leurs disciples. Ainsi, bien qu'étant absolument nécessaires, elles doivent être renforcées par des actions visant à former les utilisateurs des systèmes d'information. Les états et les grandes entreprises doivent de plus organiser la défense de leurs systèmes par la montée en puissance d'organismes de lutte contre la cybercriminalité, par la création et l'application d'un arsenal juridique dissuasif. La coopération internationale doit également être renforcée et étendue à l'ensemble des nations.

2.3.1. ACTIONS SUR LE COMPORTEMENT DE L'INDIVIDU

Selon une étude européenne, conduite et publiée par le cabinet Andersen en 2001, on découvre que près de 50% des instigateurs d'attaques sont des collaborateurs internes à l'entreprise. Les résultats sont bien évidemment à relativiser en fonction du taux de réponse des sociétés interrogées et de leur ignorance, souvent constatée, des attaques qu'elles ont subies. Ce constat démontre l'effort qui doit être entrepris dans la formation ou le recyclage des utilisateurs des systèmes d'information sensibles. L'organisation interne de l'entreprise doit enfin prévoir le mode d'attribution des droits d'accès aux informations et le contrôle de cette procédure et de la bonne utilisation de son outil informatique. Les responsables de cette procédure doivent eux-mêmes être sensibilisés à l'enjeu de leur mission et correctement formés pour la mener à bien.

Les mêmes précautions peuvent être prises pour les propriétaires de micro-ordinateurs, en particulier lorsqu'ils accèdent au réseau Internet. Il est donc indispensable qu'une information régulière leur soit dispensée lors de l'achat de leur matériel ou lors de leur raccordement au réseau.

Dans la recherche de solution de protection, une autre méthode peut consister à recruter chez les agresseurs. En effet, certaines entreprises vont jusqu'à se payer les services de « hackers » à l'origine d'attaques contre leurs propres systèmes. D'autres font appel à eux pour tester la fiabilité de leurs logiciels avant leur commercialisation. Même les organisations chargées, en temps normal, de traquer les cybercriminels, n'ont pas hésité à recourir à leurs compétences, tels la CIA, par exemple lors de la guerre du Kosovo.

En matière de prévention encore, les entreprises françaises peuvent se tourner vers des associations telles que Le CLUSIF (Club de la Sécurité Informatique Français) qui regroupe des grandes entreprises utilisatrices d'informatique, ce groupe réfléchit aux moyens de se protéger des attaques informatiques. Les CLUSIR - Club de la sécurité des systèmes d'information régionaux - sont des associations régionales décentralisées et agrées par le CLUSIF. Elles ont pour vocation de rassembler les différents acteurs de la sécurité des systèmes d'information tels que utilisateurs, offreurs de produits ou de services, collectivités publiques. Elles favorisent également les relations avec les universités délivrant des diplômes de troisième cycle en sécurité des systèmes d'information. Elles se positionnent comme relais régional des actions du CLUSIF et agissent dans l'esprit du code d'éthique de ce dernier. Les CLUSI sont des associations localisées hors de France (Italie, Belgique, Suisse et Luxembourg), juridiquement indépendantes et autonomes dans leur fonctionnement. Leurs objectifs sont similaires à ceux du CLUSIF. Elles agissent principalement pour sensibiliser à la sécurité des systèmes d'information, faciliter les échanges d'expérience et d'idées entre les membres, réaliser et diffuser des synthèses sur l'état de l'art et les techniques relatives à ce domaine.

2.3.2. LA REPRESSION

Même lorsque tous les moyens techniques de protection ont été intégrés au système d'information de l'entreprise, et lorsque celle-ci s'est engagée dans le recrutement de spécialistes de la sécurité et dans la formation de son personnel, elle peut malgré tout subir une agression. Dans ce cas défavorable, elle doit avoir le courage de se tourner vers les services de police pour que ceux-ci se livrent à une enquête judiciaire qui sera longue et difficile.

2.3.2.1. L'arsenal juridique

Face aux menaces du cyber-monde, les états ont des arsenaux législatifs sous-développés. C'est le constat dressé par le rapport effectué en 2000 par le cabinet britannique Mc Connell International.

Sur les cinquante-deux pays étudiés par Mc Connell, 8 ont révisé leurs textes dans 6 à 9 de ces catégories : derrière les Philippines, on trouve les Etats-Unis et le Japon, puis l'Australie et l'Inde, car dans ce domaine, les lacunes juridiques ne trahissent

pas forcément un manque de moyens et inversement. Dix pays ensuite disposent de moyens législatifs pour poursuivre les auteurs de trois à cinq types d'attaques : ce sont par exemple l'Espagne et le Canada. Trente-trois pays sont au nombre des grands retardataires du classement, n'ont pas mis leur législation à jour et « ne peuvent poursuivre l'auteur d'un crime informatique ». En effet, dans certains autres, l'accès non autorisé n'est pénalisé qu'en cas d'intention de nuire. Dans d'autres enfin, le vol de données n'est répréhensible que dans les cas où ces données concernent la religion ou la santé d'un individu. Les pénalités associées aux jugements divergent beaucoup également, s'étendant de la simple sommation à de longues peines de prison pour un même cyber-délit.

L'intérêt de cette enquête réalisée en 2000 est de donner un aperçu global des mesures prises contre la cybercriminalité. Des évolutions ont suivi et notamment la prise de conscience de la nécessité d'un consensus international pour aboutir à la normalisation la plus étendue possible dans la façon de gérer ces affaires. Si l'harmonisation des lois au niveau européen paraît une suite logique du processus engagé par l'Union, le cadre mondial apparaît autrement plus complexe quant à la convergence de ces dispositions.

La France est une bonne illustration de la catégorie des « retardataires » et pourtant, la loi Informatique et Libertés de 1978 représentait une avancée majeure. Elle avait été adoptée à la suite d'un scandale à propos de l'indexation des fichiers du fisc sur les numéros de sécurité sociale. A l'époque donc, la France était l'avant-garde.

En France, le code pénal prévoit dans le livre III (Des crimes et délits contre les biens) les trois infractions suivantes :

- Article 323-1 (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30000 euros d'amende. »

- Article 323-2 (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45000 euros d'amende. »

- Article 323-3 (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 45000 euros d'amende. »

Il prévoit dans le livre IV (Des crimes et délits contre la nation, l'Etat et la paix publique), l'article l'infraction suivante :

- Article 411-9 (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

« Le fait de détruire, détériorer ou détourner tout document, matériel, construction, équipement, installation, appareil, dispositif technique ou système de traitement automatisé d'informations ou d'y apporter des malfaçons, lorsque ce fait est de nature à porter atteinte aux intérêts fondamentaux de la nation, est puni de quinze ans de détention criminelle et de 225000 euros d'amende. Lorsqu'il est commis dans le but de servir les intérêts d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger, le même fait est puni de vingt ans de détention criminelle et de 300000 euros d'amende. »

Depuis quatre ans, le Conseil de l'Europe s'est attaché à mettre sur pied une convention capable de répondre aux défis que pose la criminalité informatique. Ce texte qui constitue une première au niveau mondial vise avant tout à garantir la sécurité du réseau et de ses utilisateurs. La convention détermine trois principaux axes de réglementation : l'harmonisation des législations nationales concernant la définition des crimes, la définition des moyens d'enquêtes et de poursuites pénales adaptés à la mondialisation des réseaux et la mise en place d'un système rapide et efficace de coopération internationale. Les infractions retenues sont toutes soumises à deux conditions générales : les comportements incriminés doivent toujours être commis de façon intentionnelle et « sans droit » pour que la responsabilité pénale soit engagée.

La convention prévoit des règles de base qui faciliteront la conduite d'enquêtes et qui représentent de nouvelles formes d'entraide judiciaire. Ainsi sont prévues : la conservation des données stockées la conservation et divulgation rapide des données relatives au trafic, la perquisition des systèmes et la saisie de données informatiques, la collecte en temps réel des données relatives au trafic et l'interception de données relatives au contenu. Ces dispositions sont soumises aux conditions légales des pays signataires mais qui doivent garantir le respect des droits de l'homme et l'application du principe de proportionnalité. En particulier, les procédures ne pourront être engagées

que sous certaines conditions, tel que, selon le cas, l'autorisation préalable d'un magistrat ou d'une autre autorité indépendante.

A côté des formes traditionnelles de coopération pénale internationale prévues notamment par les conventions européennes d'extradition et d'entraide judiciaire en matière pénale, la nouvelle convention exigera des formes d'entraide correspondant aux pouvoirs définis préalablement par la Convention et, en conséquence, que les autorités judiciaires et services de police d'un Etat puissent agir pour le compte d'un autre pays dans la recherche de preuves électroniques, sans toutefois mener d'enquêtes ni de perquisitions transfrontalières. Les informations obtenues devront être rapidement communiquées.

Un réseau de contacts disponibles 24 heures sur 24 et sept jours sur sept est mis sur pied afin de prêter une assistance immédiate aux investigations en cours. Chaque pays doit établir sa compétence lorsque l'infraction est commise sur son territoire, à bord d'un bateau ou d'un avion immatriculé chez lui ou lorsque l'un de ses ressortissants en est l'auteur si l'infraction ne relève de la compétence territoriale d'aucun autre Etat.

Les 43 pays membres[11] du Conseil de l'Europe ont participé à l'élaboration de ce texte ainsi que le Canada, les Etats-Unis, le Japon (observateurs auprès de l'organisation) et l'Afrique du Sud qui ont pris ont part très active dans le processus. Ils pourront donc adhérer à la Convention qui étendrait son champ d'application à la plus grande partie du trafic informatique mondial.

La « convention sur la cybercriminalité » entrera en vigueur le 1er juillet 2004. Ce texte, présenté comme « le premier traité international sur les infractions pénales commises via l'Internet et d'autres réseaux informatiques », a été adopté en novembre 2001. Il lui fallait au minimum être ratifié par cinq États membres pour entrer définitivement en vigueur. La Croatie, l'Albanie, l'Estonie et la Hongrie ont été les premiers pays à s'acquitter de cette formalité. Ils ont été rejoints au cours du premier trimestre 2004 par la Lituanie. La France a signé ce traité, mais ne l'a toujours pas ratifié à ce jour.

---

[11] Albanie, Allemagne, Andorre, Arménie, Autriche, Azerbaïdjan, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Géorgie, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, "L'ex-République yougoslave de Macédoine", Liechtenstein, Lituanie, Luxembourg, Malte, Moldova, Norvège, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Russie, Saint-Marin, Slovaquie, Slovénie, Suède, Suisse, Turquie, Ukraine.

2.3.2.2. Les services de lutte

En France, au sein de la police nationale, L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (O.C.L.C.T.I.C.) a été créé, par Décret interministériel, le 15 mai 2000. Ses compétences, opérationnelles et techniques, s'exercent dans le domaine de la cyber-criminalité, concept qui recouvre le traitement judiciaire des infractions spécifiques à la criminalité liée aux nouvelles technologies et à celles dont la commission est facilitée ou liée à l'usage de ces mêmes technologies. Ses missions recouvrent l'animation et la coordination, opérationnelle et technique, au niveau national. Il lui appartient, également, de procéder à tous actes d'enquêtes et travaux techniques d'investigations, en assistance des services de police, de gendarmerie et de la direction générale de la concurrence, de la consommation et de la répression des fraudes dans le cadre de leur activité judiciaire. Il participe aux travaux opérationnels et stratégiques des enceintes internationales (G8 – Europol – Interpol – Commissions Européenne etc.). Le développement des nouvelles technologies et leurs utilisations frauduleuses plus, rentables et moins risquées que la criminalité « traditionnelle », par des groupes criminels reconvertis a amené le rattachement à l'O.C.L.C.T.I.C. de la Brigade Centrale pour la Répression des Contrefaçons des Cartes de Paiement (B.C.R.C.C.P.) ; celle-ci a, par exemple, en charge la lutte contre les réseaux nationaux contrefaisant les cartes bancaires (Yescards), ou internationaux de piratage des distributeurs automatiques de carburant et de billets.

La brigade d'enquête sur les fraudes aux technologies de l'information (B.E.F.T.I.), service de la Direction Régionale de la Police Judiciaire de Paris créé en février 1994, a pour mission essentielle de lutter contre les atteintes aux systèmes de traitement automatisés d'informations, qu'il s'agisse des réseaux informatiques ou télématiques ou des systèmes de télécommunications (GSM, autocommutateurs d'entreprises…). Son domaine d'action ne se limite cependant pas aux intrusions dans les systèmes d'informations, mais vise également la lutte contre la contrefaçon sur supports numériques, la captation frauduleuse de médias télévisuels cryptés, ainsi que des incriminations traditionnelles utilisant les nouvelles technologies comme support de commission. Il s'agit alors de l'escroquerie (y compris dans le milieu de la télématique),

de détournements de fonds, d'abus de confiance, d'atteintes aux biens (recel de vol), d'atteintes à la personne (injures, diffamation) ou prévues par la loi du 29 juillet 1881 (Loi sur la liberté de la presse) perpétrées sur les réseaux. La B.E.F.T.I. joue également un rôle important dans l'assistance technique sollicitée par les autres services de police lorsque ces derniers sont confrontés à la recherche de la preuve sur supports numériques découverts dans leurs propres enquêtes (disques durs, disquettes, CD Rom,...). Dans ce contexte, la B.E.F.T.I. constate une augmentation régulière de l'utilisation du média Internet dans la commission de nombreux délits avec comme corollaire une augmentation très inquiétante d'enquêtes non résolues. Ce constat s'expliquant essentiellement par un archivage des données techniques insuffisant dans le temps.

Depuis 1992, l'Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN) dépendant du ministère de la Défense, dispose également d'une unité spécialisée dans les enquêtes informatiques. Les activités du département Informatique-Electronique (INL) de l'IRCGN visent à rendre accessibles aux enquêteurs et aux magistrats les informations qui sont contenues dans les supports de preuve numérique :

- les activités techniques ou d'expertise : traitement de l'information, réseaux et télécommunications, électronique ;
- le soutien des unités sur le terrain : notamment lors des perquisitions complexes ;
- la formation : au profit des enquêteurs, des magistrats, mais aussi la sensibilisation des partenaires que sont les opérateurs de télécommunications, les entreprises qui rencontrent des problèmes de sécurité informatique ;
- la recherche et le développement : concevoir de nouveaux outils pour le département ou pour les premiers intervenants sur le terrain.

La Direction de la Surveillance du Territoire (DST) mène une action de surveillance des activités cybercriminelles, dans le cadre de sa mission de protection des atteintes aux intérêts fondamentaux de la nation. Cet organisme a créé un service spécialisé dans l'informatique dès 1986. Les activités de ce service, naturellement discrètes sont de trois ordres : renseigner le gouvernement sur l'évolution des phénomènes de criminalité informatique, sensibiliser les administrations et les entreprises concernées quant aux risques encourus, agir dans un cadre judiciaire su le domaine de compétence de la DST est concerné.

Au ministère de l'économie, des finances et de l'industrie, la cellule Traitement du renseignement et action contre les circuits financiers (TRACFIN), créée par le décret

du 9 mai 1990, assure une mission de coordination des services en matière de lutte contre le blanchiment de capitaux et le transfert de fonds occultes. A ce titre, elle opère une surveillance des virements électroniques de fonds facilités par Internet et les réseaux numériques. TRACFIN a porté 291 dossiers en justice au titre de 2001 – soit une augmentation de 45 % par rapport à l'année précédente –, qui regroupent 24 % des déclarations de soupçon, pour lesquelles l'enquête du service a été clôturée. Ces affaires, mettant en jeu un montant cumulé d'environ 1,27 milliards d'euros, portent davantage sur le blanchiment présumé d'activités criminelles organisées que sur celui du trafic de stupéfiants. TRACFIN participe ainsi au démantèlement de réseaux d'ingénierie financière mis en place pour dissimuler et recycler les produits – d'un montant considérable – de leurs agissements criminels, sans préjudice de son action à l'encontre du financement du terrorisme.

Le développement des « cyberpoliciers » accompagne l'évolution des arsenaux législatifs contre la cybercriminalité. Dans de nombreux pays aujourd'hui, les nouveaux stages de formation que reçoivent les policiers sont des ateliers où l'on s'entraîne à combattre les « hackers ». En 2001, des « cyberpoliciers » de 26 pays européens se sont réunis en novembre pour améliorer les méthodes d'investigation des enquêteurs spécialisés, élaborer un guide des meilleures pratiques en la matière dans le domaine des nouvelles technologies et permettre une plus grande efficacité de la coopération policière dans la lutte contre la cybercriminalité.

Aux Etats-Unis, le National Infrastructure Protection Center (NIPC), le « bras armé » du FBI en matière de cyberdélinquance, vient d'annoncer la mise en place d'un programme baptisé « InfraGard ». Il est déjà testé depuis plusieurs mois dans l'Etat de Cleveland et 500 entreprises y participent. A travers ce programme, l'agence de sécurité américaine cherche à jeter les bases d'une collaboration efficace avec des sociétés du secteur public et privé. Une collaboration fondée sur l'échange de bons procédés : en contrepartie d'informations précises fournies sur les « hackers » aux entreprises, le FBI attend que ces dernières lui signalent les intrusions ou les tentatives d'intrusion dont elles sont victimes.

2.3.3. LA NECESSAIRE COLLABORATION INTERNATIONALE

Chaque état en Europe, et certains autres ailleurs dans le monde disposent de services de police qui progressivement s'adaptent à la nouvelle forme de criminalité véhiculée par les réseaux numériques. Les nations possédant la maîtrise des nouvelles technologies étant les plus concernées par les attaques des cybercriminels ont modifié leur législation en créant des infractions spécifiques à ce nouveau fléau. La convention européenne qui entrera en vigueur le 1er juillet 2004 symbolise la volonté de ces états de s'unir et d'harmoniser leur lutte contre la cybercriminalité et d'organiser le contrôle de l'utilisation du réseau Internet.

Les nations riches, qui tirent de l'usage du réseau Internet un avantage décisif dans la conduite de leur politique ou dans l'expansion de leur économie, ont parfaitement compris la nécessité de contrôler le bon usage de cet outil afin d'éviter toute dérive qui pourrait entraîner un manque de confiance dans ce système de communication et à terme sa remise en cause ou son abandon pur et simple. Les gouvernements de ces pays sont donc décider à collaborer dans la lutte contre la cybercriminalité. Compte tenu de la mondialisation de l'utilisation du réseau, il faut que ces derniers entraînent dans leur sillage l'ensemble des gouvernements du mode entier, sous peine de voir apparaître des paradis cybernétiques comme il est apparu des paradis fiscaux.

2.3.4. LA VOLONTE DE LUTTER ; LES ENJEUX DE LA PROTECTION

Ce combat sans merci contre le cybercriminel ne peut être mené sans une volonté farouche de l'ensemble des pays de la planète, une volonté aussi forte que la passion qui anime les petits génies de l'informatique qui sévissent sur les systèmes d'information depuis maintenant une vingtaine d'années et qui continuent d'améliorer leurs connaissances en échangeant leurs techniques par le réseau qu'ils attaquent. Cette volonté de se protéger ne dépend pas d'une passion des entreprises ou des états mais de la perception qu'ont les responsables de ces entités de la menace qui pèse sur leurs systèmes et des enjeux stratégiques que représente leur protection.

Cette volonté est motivée par l'étude de la menace et des risques, par l'analyse des situations et par le calcul du rapport coût/efficacité de la protection. Elle n'est pas inspirée par la passion, mais par la raison.

CONCLUSION

La technique utilisée lors de la création du réseau Internet et la philosophie de libre accès aux serveurs qui y sont connectés ainsi que de liberté des échanges ont permis au réseau numérique de s'étendre, en une petite vingtaine d'années, à la planète entière. Mais elles auront aussi attiré quelques mauvais génies sur la route de la cybercriminalité. Cette délinquance atteint certes le particulier mais elle constitue une menace grave contre l'économie mondiale et la stabilité politique des grandes puissances démocratiques modernes.

Malgré des systèmes de protection de plus en plus efficaces, le nombre d'attaques menées sur le réseau qui ne cesse d'augmenter démontre les limites de la simple mise en œuvre de ces solutions. En réponse à ces agressions qui peuvent provenir de n'importe quel endroit du monde et dont les effets sont immédiats, les outils juridiques et les services de lutte ne parviennent à identifier et punir le criminel que dans des délais qui se comptent en mois ou en années.

La recherche d'une parade réellement efficace passe naturellement par la mise en œuvre de ses techniques de protection et par l'action de la justice contre les malfaiteurs mais elle doit avant tout consister en la sensibilisation des utilisateurs et des responsables des systèmes d'information stratégiques. Il s'agit enfin pour l'ensemble des pays du monde entier d'harmoniser leur législation et de s'attacher à combattre en un même mouvement ce fléau qui met en péril les grands équilibres mondiaux à l'aube du XXI^{ème} siècle.

Or cette union des nations dans la lutte contre la cybercriminalité ne pourra jamais être obtenue, compte tenu du nombre. La lourdeur des dispositifs à adopter pour garantir la protection du réseau et de ses utilisateurs ne résistera pas à la simplicité et la rapidité de l'attaque du criminel déterminé agissant sur le réseau Internet.

Cette guerre sans merci, entre la passion de l'agresseur et la raison du responsable, tournera inéluctablement à la faveur du passionné.

TABLE DES MATIERES

Bibliographie

Les ouvrages :

- Frédéric-Jérôme Pansier et Emmanuel Jez. La criminalité sur internet. Edition Que sais-je ?
- Serge Le Doran et Philippe Rosé. Cyber mafia. Edition Denoël documents actualité.

Les Revues :

- Diplomatie Magazine n°5, septembre-octobre 2003.
- Sciences et Vie Micro, n°217 de juillet-août et n°220 de novembre 2003.
- Courrier International. Hors série n°23 décembre 2003 janvier 2004.
- L'ordinateur Individuel, n°159 de mars 2004.

Les sites Internet :

- http://www.01net.com
- http://press.coe.int
- http://www.journaldunet.com
- http://www.ifrance.com
- http://news.zdnet.fr
- http://www.internetactu.com
- http://www.linternaute.com
- http://www.observateurocde.org
- http://www.iris.sgdg.org

Les rapports

- Rapport 2000-2001 du GAFI sur les typologies du blanchiment de capitaux.

les conférences

- Daniel Martin. Technologies de l'information : dangers, menaces et ripostes. Les cahiers du CHEAr.