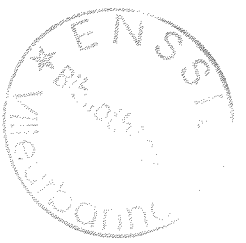
enssib
Ecole Nationale Supérieure
des Sciences de l'information
et des Bibliothèques

Diplôme Professionnel supérieur
en Sciences de l'information et des Bibliothèques

Rapport de stage

Criminalité informatique

LIANG Jiansheng



Sous la direction de

Rodolphe SARIC

Service de Documentation Générale du Secrétariat Général d'Interpol

1999

Si vous connaissez votre ennemi et si vous savez ce que vous valez, vous n'avez pas besoin de craindre vos prochaines batailles. Si vous savez ce que vous valez et rien sur votre ennemi, pour chaque victoire remportée, vous subirez une défaite. Si vous ne connaissez rien sur vous-même ni sur votre ennemi, vous succomberez à chaque bataille.

Sun Tzu-L'art de la guerre

Criminalité informatique

LIANG Jiansheng

Résumé :

Ce rapport se divise en deux parties : un aperçu général sur le Secrétariat Général d'Interpol et la criminalité informatique. l'auteur dresse un panorama de la criminalité informatique, analyse les comportements, les procédés et les outils utilisés par des malfaiteurs et expose les moyens techniques et juridiques au niveau de la protection et de la prévention contre la criminalité informatique. Les approches d'Interpol en la matière ont été également exposées.

Descripteurs :

informatique, criminalité informatique , police, droit, sécurité informatique, virus .

Abstract :

In the first part of this report are presented the characteristics of Interpol's General Secretariat ; the second part offers a panorama of the phenomenon of computer crime, analyses criminals' behariours, tricks and tools , and displays the technical and juridical means used in the protection and prevention against computer crime. Interpol's approache in the subject have also been explained.

Keywords :

computer ,computer crime, network security, virus, police, law,

Table de matières

INTRODUCTION 7

PREMIÈRE PARTIE :

BRÈVE PRÉSENTATION D'INTERPOL ET DU STAGE 9

1. QU'EST-CE QU' INTERPOL ET QUELS SONT SES MOYENS D'ACTIONS ? 9

1.1. MÉCONNAISSANCE DE L'ORGANISATION 9
1.2. QUELS SONT LES ATOUTS D'INTERPOL ? 9
1.2.1. Le centre d'information criminelle 10
1.2.2. La veille de la criminalité internationale 11
1.2.3. La mémoire criminelle mondiale 12
1.2.4. La coopération internationale : une mission fondamentale 13

2. LES ACTIVITÉS PRINCIPALES DE MON STAGE 14

2.1. FAMILIARISATION AVEC LE LOGICIEL DOCUMENTAIRE FULDESK 14
2.2. APPRENTISSAGE DU LANGAGE HTML 14
2.3. RECHERCHE DOCUMENTAIRE ET COMPOSITION D'UN DOSSIER THÉMATIQUE SUR LA CRIMINALITÉ INFORMATIQUE 15

DEUXIÈME PARTIE :

LA CRIMINALITÉ INFORMATIQUE 16

1. UNE NOUVELLE MENACE : CRIMINALITÉ INFORMATIQUE 16

1.1. LA GENÈSE DE LA CRIMINALITÉ INFORMATIQUE 16
1.2. LA DÉFINITION DE LA CRIMINALITÉ INFORMATIQUE 19
1.3. LE POIDS DU CYBERCRIME 21

2. LES FORMES DE CRIMINALITÉ INFORMATIQUE 23

2.1. TYPE D'INFRACTIONS INFORMATIQUES DONT L'ORDINATEUR OU LE RÉSEAU INFORMATIQUE SONT LA CIBLE 23
2.1.1. Accès et interception non autorisés 23
2.1.2. Modification de logiciels ou de données 24
2.1.3. Fraude informatique 24
2.1.4. Reproduction illicite 25
2.1.5. Sabotage informatique 25
2.1.6. Infractions moyens informatiques (autres) 26
2.2. TYPE D'INFRACTIONS INFORMATIQUES DONT L'ORDINATEUR OU LE RÉSEAU INFORMATIQUE SONT LES INSTRUMENTS 27

3. LA TYPOLOGIE DES CRIMINELS ET LEUR MOTIVATIONS 28

4. LA CRIMINALITÉ INFORMATIQUE LA PLUS FRÉQUENTE 30

4.1. PIRATAGE INFORMATIQUE 30

4.2. PIRATAGE TÉLÉPHONIQUE 32
4.3. MODIFICATION DE LOGICIELS OU DE DONNÉES 33
4.3.1.Les virus informatiques *33*
4.3.2. Cheval de Troie *34*
4.3.3. Bombe logique *35*
4.3.4. Les vers *35*
4.4. LA PÉDOPHILE SUR INTERNET 36

5. LA SÉCURITÉ INFORMATIQUE 38

5.1. LA PROTECTION TECHNIQUE CONTRE LES PIRATES 38
5.1.1. Les comportements des pirates *38*
5.1.2. les procédés et les outils utilisés par les pirates *40*
5.1.3. Protection par mot de passe contre les pirates *41*
5.1.4. Le cryptage : une arme contre le piratage informatique *43*
5.1.5. L'installation d'une paroi antifeu (firewall) *45*
5.2. ERADIQUER LES VIRUS INFORMATIQUES 46
5.2.1. Le mécanisme des virus informatiques *46*
5.2.2. Les signes révélant le virus *47*
5.2.3. Les antidotes aux virus *48*

6. LA PRÉVENTION ET LA RÉPRESSION JURIDIQUES 50

6.1. DES APPROCHES MONDIALES CONTRE LA CRIMINALITÉ INFORMATIQUE 50
6.1.1. Le droit pénal national face à la nouvelle criminalité *50*
6.1.2. L'harmonisation et la coopération internationale *52*
6.2. INTERPOL ET LA CRIMINALITÉ INFORMATIQUE 53
6.2.1. La constitution du Groupe de travail d'Interpol *54*
6.2.2. Message « criminalité informatique » *55*
6.2.3. La Conférence Internationale sur la criminalité informatique *55*
6.2.4. Les deux outils documentaire d'Interpol *57*
6.3. LE SYSTÈME INFORMATIQUE ET LES RÉSEAUX D'INTERPOL 58
6.3.1.L'architecture du Réseau d'Interpol *59*
6.3.2. La situation actuelle du réseau d'Interpol *59*
6.3.3. Le système ASF (Automated Search Facility) *60*
6.3.4. Les systèmes informatiques *61*
6.3.5. Le système ICIS (Interpol Criminal information Systèm) *61*
6.3.6. L'archivage électronique *62*
6.3.7. Les mesures de sécurité d'Interpol pour protéger son réseau *62*

CONCLUSIONS 65

BIBLIOGRAPHIE 68

INDEX 72

Remerciements

Je tiens à remercier Monsieur R. KENDALL, Secrétaire Général d'Interpol, ainsi que Monsieur Souheil EL ZEIN directeur juridique qui ont donné l'accord au déroulement de ce stage dans l'Organisation.

Je souhaite également exprimer ma profonde gratitude à Madame Catherine CHEVRIER, chef du service de documentation générale pour la cordialité de son accueil dans son service et pour sa sollicitude, et plus particulièrement à Monsieur Rodolphe SARIC pour sa disponibilité, son aide tout au long de ce stage et surtout ses précieux conseils m'aidant ainsi à réaliser ce rapport .

De même, j'aimerais adresser mes remerciements à toutes les personnes du service de documentation générale qui ont contribué à rendre ce stage agréable dans une ambiance conviviale et sympathique.

Je voudrais aussi témoigner toute ma gratitude à M. Wang Donghai , grâce à sa recommandation , j'ai eu la possibilité de faire mon stage dans une telle organisation.

Enfin, que Mme Sylvie CHIVILLOTTE et M.Mohamed HASSOUN, les deux responsables du cycle du DPSSIB, trouvent ici l'expression de mes sincères remerciements .

Introduction

A l'occasion de mon stage d'étude qui s'est déroulé du 1er juin au 30 septembre 1999 au Secrétariat Général d'Organisation Internationale de Police Criminelle -Interpol à Lyon, dans le service de documentation générale, il m'a été offert d'effectuer une étude sur la **criminalité informatique** qui est justement une des préoccupations d'Interpol.

La montée de la délinquance informatique engendrée par le développement rapide des sciences de l'information et des nouvelles technologies de communication inquiète de plus en plus les pays , les organisations, les services de police et les particuliers concernés. Ces dernières années cette criminalité qui menace la sécurité de la société de l'information a été prise très au sérieux par les autorités de justice de tous les pays.

La criminalité informatique ne recouvre pas une catégorie d'infractions clairement définie, mais un ensemble flou d'activités illicites liées à l'informatique. Elle est un vaste domaine, dont les frontières ne sont pas toujours faciles à définir. Chaque pays a une législation différente à ce sujet.

La plupart des spécialistes ont tendance à proposer une classification qui distingue les affaires où l'ordinateur ou le réseau informatique sont la cible de celles dans laquelle l'ordinateur ou le réseau informatique sont les instruments. Le système de codification des infractions informatiques du Secrétariat général d'Interpol recense près de trente types d'infractions.

Parmi toutes ces types d'infractions informatiques, les cas des intrusions informatiques, des piratages téléphoniques, des virus informatiques et de la pédophile sur Internet sont la criminalité informatique la pus fréquente.

Pour mieux se protéger des pirates, mieux vaut bien les connaître. Donc il est indispensable de savoir les motivations, les techniques, les comportements et les moyens des criminels informatiques pour établir les mesures techniques et juridiques de protection et de prévention susceptibles de réduire les risques.

La prévention et la lutte contre la criminalité informatique pose une série de problèmes techniques, juridiques et de coopération internationale. Mais cela ne concerne pas seulement la police judiciaire, la prise sociale de conscience de l'importance de la sécurité informatique à tous les niveaux de la société est extrêmement important. Donc nous tous, les habitants qui vivent dans un espace virtuel devons maîtriser certains rudiments de la sécurité informatique.

La lutte contre cette nouvelle forme de délinquance a été débattue par diverses organisations internationales et de nombreux groupes d'experts, particulièrement

Interpol qui travaille depuis plus de 13 ans dans le domaine de la criminalité informatique. Et toute ces organisations ont fourni d'importantes contributions en la matière.

Avant d'exposer ce sujet il m'a semblé d'autant plus utile de présenter brièvement dans la première partie du rapport, le Secrétariat Général d'Interpol notamment en tant que le centre de l'information de police, la veille de la criminalité du monde et la mémoire criminelle mondiale, que ces particularités ne sont pas encore très bien connues par le public. Si non , on ne saurait comprendre la fonction et la contribution d'Interpol dans la lutte contre la criminalité informatique. Dans cette première partie mes activités principales du stage ont été également résumées.

Première partie

Brève présentation d'Interpol et du stage

1. Qu'est-ce qu' Interpol et quels sont ses moyens d'actions[1] ?

Il existe beaucoup de méthodes pour connaître Interpol, on peut présenter cette organisation internationale sous l'angle historique, politique, juridique ou institutionnel. Moi, je préfère d'abord à l'observer aux yeux de notre métier , c'est à dire du point de vue de l'information. Cet aspect d'Interpol qui n'est pas très bien connu par le public reflète justement sa véritable fonction.

1.1. Méconnaissance de L'Organisation

Du 1er juin au 30 septembre 1999, j'ai eu l'honneur de faire mon stage d'étude à au Secrétariat général de l'Organisation Internationale de Police Criminelle (OIPC)-Interpol, une des plus importantes organisations internationales après l'ONU.

Après une formalité complexe qui comprend une enquête sur le candidat au bureau central national concerné et la signature d'une déclaration de loyauté ainsi que d'une convention de stage entre l'Ecole Nationale Supérieure des Sciences de l'Information et des Bibliothèques et le Secrétariat général d'Interpol, ma candidature de stage a été acceptée et j'ai fini par recevoir une carte d'entrée électronique qui peut ouvrir les portes de l'Organisation dans la quelle travaillent ensemble 360 personnes dont 131 policiers de nationalités différentes.

Ce stage a changé totalement ce que j'imaginais sur cette Organisation. Le siège d'Interpol abrite la plus formidable machine de guerre contre le crime international, mais ici on ne voit pas de revolvers, ni de chapeaux mous, ni d'éprouvettes et poudre blanche, on y trouve des écrans , des terminaux informatique à profusion, des bureaux clairs et nets, des costumes et cravates élégants et surtout tant de visages souriants et sympathiques.

1.2. Quels sont les atouts d'Interpol ?

[1]. Il s'agit ici seulement du point de vue de l'auteur du rapport. Pour bien connaître l'Organisation, il convient de voir son site sur Internet : http ://www.interpol.int

L'Organisation Internationale de Police criminelle (OIPC)-Interpol est une organisation intergouvernementale rassemblant 177 pays membres. Elle est connu sous le nom d'Interpol. Depuis 1989, elle a son siège mondial à Lyon, France. L'Organisation a pour but de favoriser la coopération policière internationale.

La criminalité internationale devient de plus en plus globale. En tant que telle, il faut une réponse globale. Mais donc par quels moyens d'action Interpol atteint-elle cet objectif ? quels sont ses atouts et sa force de frappe ? quel est le mécanisme de fonctionnement de cette machine de guerre contre la criminalité internationale ?

1.2.1. Le centre d'information criminelle

Interpol ne compte pas du tout sur des policiers armés, ni des détectives, Elle n'effectue jamais de filature ni d'opération comme le mythe véhiculé depuis des décennies par le cinéma et les romans policiers. Au contraire, ses atouts sont son système d'information, son réseau de communications et ses échanges rapides d'information entre 177 pays membres.

S'il n'est pas facile d'entrer dans le bâtiment du Secrétariat général d'Interpol, on peut communiquer avec celui-ci au moyen du réseau de communications d'Interpol, qui est le plus important du monde. Interpol, loin de travailler dans l'isolement, est une organisation ouverte dont le travail concerne tous les policiers.

Le Secrétariat Général a un rôle de coordination. Il est chargée de centraliser les informations et de s'occuper des affaires relevant de la criminalité internationale. Il se charge également de préparer les notices criminelles internationales.

Au sein de chaque pays membre, l'ensemble de la coopération policière internationale passe par le Bureau Central National (B.C.N.) qui est un service de police désigné par son gouvernement pour être le représentant d'Interpol dans le pays et représenter le pays auprès d'Interpol. Le B.C.N. reçoit et centralise toutes les informations provenant de l'étranger et les communique aux services nationaux intéressés. Une des principales activités de l'Organisation procède du fait que les B.C.N. échangeant des informations sur les infractions et les malfaiteurs doivent envoyer copie de leurs messages au Secrétariat général. Ces messages sont enregistrés dans une base de données informatisée, qui permet aux officiers spécialisés du Secrétariat général d'analyser les informations relatives aux activités criminelles et les faits connexes afin d'en faire la synthèse. Les résultats de ces analyses sont ensuite transmis aux B.C.N.

Faciliter l'échange rapide d'information entre 177 pays membres très divers procure une stimulation vive et soutenue, surtout étant donné les grandes différences existant en terme de ressources disponibles tant financières que technologiques. Et les pays membres représentent un éventail très étendu de cultures, de langues et de systèmes

politiques et judiciaire. C'est pourquoi, Interpol s'est doté d'un système de communications d'un niveau égale partout dans le monde[2].

Accéder aux données exactes et vérifiées provenant des services de police de 177 pays, à vitesse la plus haute et raisonnable et fiable, donne aux Etats membres d'Interpol une capacité énormément accrue pour lutter contre la criminalité internationale et pour oeuvrer ensemble dans ce but. A l'échelle planétaire d'Interpol, des technologies mise à l'épreuve dans les domaines des télécommunications, de l'analyse criminelle et de la gestion documentaire de l'information ont été développées autour d'une messagerie électronique de type X400. Elles offrent ainsi, un ensemble important de communications policières qui bénéficie aussi d'un chiffrement numérique unique. L'information criminelle, base de toute coopération policière entre les pays membres, est exploitée, classée, scannée, stockée et analysée, à partir de mémoires magnétiques et optiques d'une technologie sûre et unique. La maîtrise de ces technologies, fait d'Interpol, le partenaire privilégié dans le domaine de la coopération policière internationale .

1.2.2. La veille de la criminalité internationale

Depuis 1989[3], Interpol vit sous régime hautement informatique. L'Organisation possède un réseau moderne et sécurisé de télécommunications. Près de 500 000 affaires en cours sont actuellement dénombrées. Ses moyens sont à la mesure de ses exigences de communication. Environ 12000 messages par jour et 1,5 million par année[4] sont reçus ou expédiés depuis les satellites des pays les plus développés jusqu'au morse de quelques uns. Depuis la mise en place du Système AMSS, le temps de diffusion des informations est passé de 78 heures à 15 secondes. Il permet une utilisation chiffrée des informations transmises par un système de messagerie électronique.

Les informations sont traitées devant les terminaux informatiques, quatre grands groupes de travail se répartissant la tâche par vocation linguistique : français , anglais, espagnol et arabe qui sont les quatre langues de travail d'Interpol. Les informations sont ensuite ditribuées entre les divers services concernés : délit contre les biens, délits financiers , fausses monnaies, trafic de drogues...

Chaque semaine, depuis Lyon le « weekly intelligence message » (message de renseignement hebdomadaire) est distribué aux 177 Bureaux Centraux Nationaux d'Interpol, il contient des renseignements ultra-confidentiels sur une nouvelle forme de criminalité, un nouveau moyen d'opérer, une trace d'un criminel recherché. C'est une forme de « mise en alerte » planétaire.

---

[2]. Cf. Raymond Edward Kendall, Secrétaire général d'Interpol, Interpol fête ses 75 ans au coeur de la coopération internationale policière, *the Diplomatic Letter* n°44, 10/1998.

[3]. Le 27 novembre 1989, le nouveau siège d'Interpol a été inauguré à Lyon, Interpol s'est doté des systèmes informatiques les plus modernes , cela a marqué une nouvelle ère pour les communications de police.

[4]. Selon l'article : Incursion au coeur d'Interpol. *Lyon international magazine, 01/10/1998.*

1.2.3. La mémoire criminelle mondiale

Le service des notices internationales d'Interpol diffuse en outre électroniquement aux services de police des Etats membres des renseignements classés en cinq catégories : « notice rouge [5]» pour les personnes qui font l'objet d'un mandat d'arrêt international avec demande d'extradition et qui doivent être immédiatement interpellées et remises à la justice du pays de demandeur ; « notice bleue » concernant des personnes liées à une affaire criminelle ; « notice verte » pour des personnes susceptibles de commettre des infractions ; « notice jaune » concernant des personnes disparues et « notice noir » concernant l'identification d'un cadavre. Les ordinateurs d'Interpol conservent en permanence 260 000[6] patronymes, la plupart accompagnés de photos, d'empreintes digitales et une liste d'alias. Parmi ces noms criminels internationaux environ 10% font l'objet d'une « notice rouge ».

Interpol est doté d'un service de documentation générale sur tous les phénomènes et toutes les disciplines qui ont un rapport avec l'Organisation et les missions de police. On trouve dans la bibliothèque d'Interpol 8000 ouvrages de différents pays concernant l'activités policières. Ici le passé et le présent d'Interpol se contemplent. D'un coté les archives en papier; de l'autre la mémoire informatique qui peut fournir en quelque secondes toutes les informations .

Dans la salle des archives sont stockées environ 6000 fichiers signalétiques des malfaiteurs de dimension internationale arrêtés dans tous les pays membres d'Interpol, et régulièrement mise à jour. Un archivage électronique de tous les renseignements communiqués permet aux services de police dont l'accès direct a été autorisé de consulter les bases de données sélectionnées grâce au système de recherche automatique ASF. Les bases de données concernent aussi bien les individus impliqués dans des infractions internationales, que les saisies de drogue, de fausses monnaies , les vols d'oeuvres d'art, une collection d'empreintes digitales de malfaiteurs internationaux...

Dans le cadre de la lutte contre les faux-monnayeurs, Interpol recense et collectionne systématiquement tous les billets de banques émis au sein des pays membres. Tout faux billet tombant entre les mains de policiers à travers le monde arrive à Interpol. Il est ensuite expertisé, passé à travers une grille informatique originale et chacun de ses défauts de fabrication est mis en lumière. Toute cette collection de faux est ensuite réunie dans la revue « contrefaçon et falsification » diffusée aux membres d'Interpol. Mais également vendue aux banques, agents de change... Avec cette revue et une loupe on peut dire à 70% si un billet est vrai ou faux.

Les bases de données implantées à Lyon contient aussi 10 millions de véhicules volés[7], 14,000 oeuvres d'art dérobées, les portraits et signalements de 28000 personnes disparues dont plusieurs centaine d'enfants .

---

[5]. Sur le système des notices rouges d'Interpol, voir : les notices rouges *Revue international de police criminel n°468/1998-9.*

[6]. La chiffre mentionnée dans un document provisoire du Secrétariat général d'Interpol : *La guide d'Interpol* .

[7] . Idem la note 5.

1.2.4. La coopération internationale : une mission fondamentale

Interpol est né d'une idée conjointe du Prince Albert 1er de Monaco et du chef de la police de Vienne en 1914 au cours du premier Congrès de police judiciaire organisé dans la principauté. Parmi les préoccupations à l'ordre du jour, la possibilité de constituer un fichier central international et d'unifier les procédures d'extradition. C'est l'acte de naissance de la Commission Internationale de Police Criminelle basée alors en Autriche, qui fonctionnera normalement jusqu'en 1940. Sa sphère d'influence reste strictement limitée à l'Europe. Après une mise en sommeil imposée par la seconde guerre mondiale, une conférence qui se tient en 1946 à Bruxelles réactive la coopération policière internationale, créé l'acronyme « Interpol », et transfère le siège à Paris. Après une étape à Saint-Cloud, le siège lyonnais est officiellement inauguré le 27 novembre 1989. Aujourd'hui Interpol se définit avant tout comme une organisation internationale forte de 177 pays membres.

La lutte contre la criminalité internationale par la coopération de policière, telle pourrait être la définition simplifiée de l'activité d'Interpol. Car la recherche et la découverte des auteurs d'infractions ne s'arrêtent plus aux frontières. Les moyens de déplacements rendus de plus en plus performants favorisent la mobilité des personnes recherchées. La complexité de la société moderne, les phénomènes de mondialisation et la progression spectaculaire des échanges internationaux au cours du XXe siècle ne font que multiplier les occasions de délinquance ou criminalité organisée sur une vaste échelle. Autant d'affaires qui possèdent pour la plupart des ramifications internationales sans compter les réseaux du terrorisme. Aussi les arrestations nécessitent-elles des échanges constants d'informations, d'identification, d'investigation entre autorités compétentes. Un rôle où Interpol excelle , puisque ses membres jouent à la fois le rôle d'officiers de liaison en coordonnant des équipes multinationales sur le terrain, et d'investigation, en faisant bénéficier des informations dont elle dispose parmi les plus vastes banques de données sur la criminalité internationale qui existent au monde.

Ainsi Interpol constitue en fait la mémoire criminelle mondiale et le centre de synthèse et d'information. Il effectue la veille de la criminalité mondiale. C'est un énorme outil de coopération et d'entraide technique, alimenté par les polices de 177 pays, qui vont en retour y puiser des informations. En terme de bibliothéconomie, c'est une bibliothèque numérique criminelle la plus grande du monde.

2. Les activités principales de mon stage

Pendant la période de mon stage à Interpol, J'ai participé aux tâches de Service de Documentation Générale (Direction III) qui est chargé de rechercher, analyser et diffuser les informations générales relatives à l'évolutions des différents aspects de la criminalité internationale et des moyens mis en oeuvres par les Etats membres et les instances internationales pour prévenir et lutter contre la criminalité.

2.1. Familiarisation avec le logiciel documentaire FULDESK

Les bases documentaires du Service de DocumentationGénérale comportent la base « Documentation », la base « Livres », la base « Interpol » , la base « Presse » et la base « vidéo », soit plus de 20 000 documents.

La base de donnée documentaire d'Interpol est réalisée par le service de documentation générale en utilisant le logiciel documentaire FULDESK qui est un des outils principaux du service de documentation générale pour recueillir et consulter des sources informations.

Fuldesk est un logiciel permettant de créer des applications de gestion documentaire adaptées aux besoins de chacun. Basé sur le moteur de recherche Fulcrum SearchServer 3.5, il bénéficie de toute sa puissance :

- recherche sur des bases locales et/ou fonctionnement en mode client/serveur sur plusieurs serveurs simultanément
- recherche structurée, en texte intégral ou intuitive, opérateurs booléens, troncatures...
- indexation et visualisation des documents dans leur format natif (traitements de textes, tableurs, logiciels de présentation, images)

Les écrans permettant de spécifier les critères de recherche, d'afficher la liste de résultats et de présenter les données structurées sont totalement paramétrables : le concepteur de l'application peut définir le type, la position, la taille et le libellé de chaque champ.

En saisissant des données et en faisant la recherche documentaire thématique j'ai bien connu le système du logiciel et les structures des fichiers et maîtrisé ses différents modes d'affichages et d'impression.

2.2. Apprentissage du langage HTML

En profitant du stage près de mon superviseur de stage monsieur SARIC qui est spécialiste en matière du langage HTML, je n'ai abandonné aucune possibilité pour

faire l'apprentissage de ce langage avec lui et l'appliquer le plus possible à créer des pages webs. Petit à petit je me suis habitué au langage HTML avec lequel j'ai crée et perfectionné mon site web personnel[8].

2.3. Recherche documentaire et composition d'un dossier thématique sur la criminalité informatique

Pendant ma période de stage je me suis concentré principalement sur la recherche documentaire et la composition d'un dossier thématique dans le domaine de la criminalité informatique dont la prévention fait l'objet d'une activité d'Interpol. Ce thème constitue fmalement le sujet de mon rapport de stage. Nous l'avons défini pour les raisons suivantes :

- La criminalité informatique a une liaison étroite avec la science de l'information et le métier de documentaliste, il s'agit à cet égard de la sécurité informatique, de protéger de données et des systèmes d'informations .
- La criminalité informatique provient de la société informatique, elle arrive avec le développement de la technologie de l'information. Ainsi la menace et la lutte dans l'espace virtuel est un sujet permanent qui n'appartient pas qu'aux affaires policières juridiques, mais concerne chaque cybernaute.
- La criminalité informatique est un phénomène relativement nouveau qui pose une série de problèmes techniques, juridiques et de coopération internationale qui n'ont pas été pris en compte auparavant. C'est justement une des préoccupations récentes d'Interpol.

[8]. Le site web sur Internet : http ://www.chez.com/jiansheng

Deuxième partie

La criminalité informatique

1. Une nouvelle menace : Criminalité informatique

1.1. La genèse de la criminalité informatique

L'ordinateur ne date pas d'aujourd'hui. Il a déjà permis aux Américains, il y a quelque cinquante ans, d'obtenir la maîtrise de l'atome et de mettre fin ainsi à la Seconde Guerre mondiale. Vingt cinq ans plus tard (20 juillet 1969), les gigantesques « computers » de la NASA(National Aeronautics and Space Administration) leur frayaient la voie de l'espace, pour envoyer le premier homme sur la lune. Mais il s'agissait alors d'installations d'une dimension, d'un coût et d'une complexité telles que seuls des Etats ou, à la rigueur, de grandes compagnies pouvaient se les procurer et les utiliser, en faisant appel à des techniciens de haut niveau. Autant dire qu'à l'époque, ce qu'on appellera plus tard l'informatique, était une affaire de spécialistes de haut vol, et totalement inaccessible au commun des mortels.

La situation actuelle est radicalement différente. Au cours des dernières années, la miniaturisation des ordinateurs, la simplification extrême de leurs procédures d'utilisation, l'abaissement considérable de leur prix, ont fait qu'ils sont devenus un outil de la vie courante et qu'ils régissent de plus en plus tous les domaines de l'activité humaine.

Aujourd'hui, les ordinateurs , les systèmes d'information et Internet occupent une place prépondérante dans notre vie . Notre société est de plus en plus dépendante de l'information. Où que nous soyons, quoi que nous fassions , nous risquons d'avoir affaire, directement ou indirectement à un ordinateur, ou un système d'information. Lorsque nous payons avec notre carte de crédit, réservons une place dans un avion, plaçons de l'argent sur notre compte en banque et même lorsque nous passons un simple coup de téléphone, c'est toujours un ordinateur ou un système qui s'occupe de nous. le développement de la technologie de l'information a bouleversé tous les secteurs de la société et la naissance d'une société informatique influencera tous les aspect de la vie quotidienne.

Les criminels savent aussi tirer parti de la technologie informatique pour commettre des crimes et porter préjudice aux utilisateurs peu méfiants.

En 1983, seuls 200 ordinateurs étaient connectés à Internet. Aujourd'hui, des millions d'ordinateurs sont désormais reliés entre eux dans le monde entier par l'intermédiaire de différents systèmes de télécommunication dont le plus connu est Internet[9]. L'idée de base d'Internet est venus des militaires américains qui en 1968 ont voulu avoir à leur disposition un système de connexion qui résiste à toutes les attaques y compris nucléaires. Si une voie est coupée dans la communication, les paquets d'informations munis chacun d'une adresse finale et d'un code permettant de les ordonner s'orientent vers un autre chemin pour parvenir à destination. Grâce à ce réseau, l'utilisateur peut entrer en communication avec un réseau situé en presque n'importe quel point du globe. Si l'utilisateur dispose du mot de passe ou du code d'autorisation voulu, il peut ainsi accéder à tous les fichiers du système. il est généralement admis que la capacité du Réseau Internet à stocker et à diffuser d'énormes quantités de données constitue un bienfait pour la société, mais que sa capacité à favoriser la prolifération d 'activités illégales constitue aussi un danger. Il en va de même pour les criminels qui sont , eux aussi, capables d'en tirer profit.

L'attaque à distance d'un système informatique est possible via les lignes de télécommunication ou les liaisons satellites en passant par d'autres sites directement reliés. Tous les pays sont touchés. A Bruxelles, les pirates ont cassé les comptes du président de la CEE. en Suède, ils interrompent une partie du réseau téléphonique. En Australie, c'est une bande organisée qui, en liaison avec les pirates américains, s'échangent des numéros de cartes de crédit par BBS et organisent pendant six mois un véritable raid sur certaines banques américaines ainsi que sur les organismes de défence nationale américaine et de grandes sociétés telles Général Motors et Westinghouse.

Les banques chinoises ne sont pas à l'abri d'intrusions frauduleuses. En novembre 1991, première attaque informatique officiellement révélée en Chine, un comptable de la Banque agricole de Chine est accusé d'avoir effectué de faux dépôts. En avril 1993, un autre pirate est condamné à mort pour intrusion et détournement de 192 000$ et exécuté[10].

Il ne faut pas négliger les aspects systèmes et réseaux. avec un certain niveau d'expertise, il est techniquement possible de s'introduire et de contrôler tout système informatique.

Pour s'en convaincre il suffit de se rappeler du célèbre « ver WORM » de 1988. Un seul individu, Robert Morris, fils du responsable de la NSA(National Security Agence) de l'époque crée et diffuse sur le réseau INternet un programme qui se propage sur plus de 6 500 machines interconnectées. Par chance, lobjet de ce « WORM » n'était pas malveillant mais visait seulement à démontrer avec quelle facilité il était posssible d'infecter des machines en utilisant quelques failles de sécurité.

---

[9]. Il s'agit de 40 à 80 millions d'utilisateurs sur Internet, selon M.Duncan, lutte contre la criminalité sur l'inforoute, *la Gazette de la GRC,* vol59, n°10, 1997.

[10] . *Les intrus sont parmi nous*, Sébastien Socchard, Abstract UNIX.

Autre exemple révélateur : un établissement bancaire avait installé deux distributeurs automatiques de billets dans deux points de la ville, avec une spécificité : ces distributeurs faisaient uniquement du change (monnaies étrangères). Pas de carte de paiement, mais des billets pour obtenir la devise de votre choix. Chaque début de semaine, la banque s'apercevait que des sommes considérables de billets avaient disparu sans explication et sans échange avec telle ou telle monnaie. Les soupçons s'orientèrent sur tout le monde, depuis les convoyeurs de fonds qui alimentent les distributeurs en fin de semaine, jusqu'aux employés de la banque, soupçonnés d'avoir trouvé un stratagème pour faire telle ou telle chose, en passant par un pirate et ainsi de suite. Il n'y avait pas aucune effraction. En fait, quelqu'un venait chaque veille de week-end dans un hôtel avec un micro-ordinateur et un modem. Il s 'agissait d'un des techniciens qui avait installé ces distributeurs. Il savait que la banque avait demandé que les deux distributeurs soient dotés de modems, afin qu'un employé puisse réactualiser chaque jour les taux de change. La banque avait oublié de changer les numéros de téléphone après l'installation, et aucun mot de passe n'était en place. L'individu se connectait sur la prise de téléphone et, jouant sur la lire italienne, il multipliait le taux de change officiel par un taux plus important, allait récupérer son argent, revenait à son hôtel et remettait par le biais du modem le taux de change officiel.. Il prenait soin ensuite de retourner dans le fichier qui avait enregistré son appel pour effacer son passage.

Les derniers chiffres révélés par le Pentagone après analyse du fonctionnement des équipes de pirates qui ont pour mission d'attaquer des sites informatiques militaires avec autorisation hiérarchique sont édifiants : ces attaques réussissent dans 88% des cas, seulement 4% des sites attaqués ont repéré ces attaques et moins de 0,5% de celles-ci ont donné lieu à un rapport.

Les technologies informatiques et de communication servent également à perpétrer des crimes conventionnels qui étaient jusque là contrôlables. Par exemple il est facile aujourd'hui de distribuer de la pornographie enfantine par l'intermédiaire des lignes de télécommunication, cette activité, lorsqu'elle est exécuté à l'échelle internationale, permet de contourner les contrôles douaniers. Une enquête réalisée en 1994 aux Etats-Unis indique que le réseau Internet renfermait alors 450,000 images ou fichier de nature pornographique et que ceux-ci avaient été consultés à plus de six millions de reprises[11]. Il faut comprendre qu'on peut décomposer des images et d'autres formes de données en bits et en octets électroniques.Une fois parvenus à destination, ces éléments sont recomposés pour former une image, un film ou un fichier de texte intégral. Essentiellement, le produit ainsi obtenu s'apparente à une bande vidéo pornographique. tout cela est particulièrement inquiétant, car il est bien connu que les pédophiles profitent de l'anonymat du réseau Internet pour échanger du matériel pornographique. Le même genre de scénario est appliqué pour la transmission de logiciels protégés par des droits d'auteurs, de la littérature haineuse et d'autres documents illégaux.

Si les forums électroniques sur Internet donnent aux citoyens du monde la facilité de dialoguer à propos de tout et de rien, ils autorisent aussi les malfaisants à se rencontrer

[11]. Idem notice précédente.

voir à s'organiser ou à mettre sur pied des commerces peu licites dans le plus parfait anonymat.

La tentation est grande pour certains Etats de contrôler des ressources d'Internet. Selon Vinton Cerf des créateurs du réseau, ce contrôle est techniquement impossible[12]. essayer de censurer Internet reviendrait à vouloir censurer toutes les communications téléphoniques dans le monde...franchement personne ne pense que ce soit faisable.

Et le cryptage ? Il permet de sécuriser les transactions financières, mais il donne aussi aux malfrats l'occasion de transférer sans trace et en toute impunité des fonds d'origine illicite.

L'inspecteur-chef Bryan Drew du National Criminal Intelligence Service du FBI, lors d'une conférence d'Iterpol sur « les crimes contre les enfants » a révélé que les réseaux internationaux de pédophiles utilisent de nouvelles techniques de codage pour protéger le secret de leurs communications. Les 3 000 pédophiles répertoriés par les services de renseignement britanniques, et branchés sur Internet, ont la possibilité de protéger leur messagerie en utilisant une « clé » personnelle pratiquement inviolable. « il faudrait au moins dix ans à nos ordinateurs opérant en pool pour casser ses codes individuels » précisait Bryant Drew. Les pédophiles échangent ainsi des informations, leurs expériences et des photos qui peuvent être diffusées à des dizaines de milliers d'exemplaires en l'espace d'une journée.

La liberté de choix des noms de domaine sur Internet continue à poser de nombreux problèmes juridiques car tant que l'on applique la règle selon laquelle « le premier arrivé » est « le premier servi », l'usurpation du nom d'autrui apparaît comme une fatalité contre la quelle il est difficile de réagir. Sur Internet, il est fréquent que la dénomination ou la marque d'autrui soit déposée comme nom de domaine. L'O.I .P.C.-Interpol, elle-même, n'a pas été épargnée dans la jungle d'Internet, et a dût lutter pour que des sites utilisant son nom sans son autorisation ne prospèrent pas. Bien que les signes distinctifs des organisations intergouvernementales soient protégés par l'article 6 ter de la Convention de Paris ? Interpol a dût agir en justice contre la société A.W.S. qui avait abusivement ouvert un site sous le nom « interpol.info.fr ». L'Organisation a enfin obtenu gain de cause auprès de la Cour d'appel de Paris[13] .

Avec l'évolution rapide des technologies informatiques et des système d'information et de télécommunication de notre société, une nouvelle forme de criminalité s'est développé : **la criminalité informatique** .

1.2. La définition de la criminalité informatique

[12]. Propos recueillis par Marc Chalamet, *Le Parisien* du 6 mars 1996.

[13]. Pour savoir de plus, voir les reportages : la protection des signes distinctifs d'Interpol, *la Semaine juridique,* 20/05/1998 et Utilisation du nom Interpol : un trouble manifestement illicite, *Expertises*, 01/02/1998.

La « criminalité informatique » - équivalent de la notion « fraude informatique », « délinquance assistée par ordinateur », « criminalité liée à l'informatique » et « cybercriminalité » qui sont presque sur toutes les lèvres aujourd'hui ne recouvre pas une catégorie d'infractions clairement définie, mais un ensemble flou d'activités illicites liées à l'informatique.

La criminalité informatique est un vaste domaine, dont les frontières ne sont pas toujours faciles à définir. Chaque pays a une législation différente à ce sujet , et a réagi plus moins vite face à ce problème.

Dans les ouvrages et documents qui traitent de la criminalité informatique, on trouve de très nombreuses définitions, dont certaines sont restreintes et précises, et d'autres larges et générales. Il faut indiquer la définition qui ait été donnée par Donn B.Parker[14] et a été adoptée par le ministère de la justice des Etats-Unis. C'est une des premières définitions sur la criminalité informatique. Pour Parker, la criminalité informatique est « tout acte illicite nécessitant une connaissance spécialisée de l'informatique, au stade de la perpétration, de l'enquête de la police ou des poursuites pénales ».

Dix ans plus tard, un groupe d'experts réuni dans le cadre de l'Organisation de coopération et de développement économique(OCDE) a adopté cette autre formulation : « l'abus informatique est tout comportement illégal, contraire à l'éthique ou non autorisé, qui concerne un traitement automatique et /ou une transmission de données »[15]. Dans le cadre de ses travaux sur ce sujet , l'OCDE a retenu plusieurs caractéristiques de la criminalité informatique :

- l'entrée, l'altération, l'effacement et /ou la suppression de données et de programmes dans l'intention de commettre un transfert illégal de dons, de commettre un faux ou d'entraver le fonctionnement du système informatique et /ou de télécommunication ;
- la violation du droit exclusif du détenteur d'un programme informatique protégé dans l'intention de l'exploiter commercialement et de le mettre sur le marché ;
- l'accès dans un système informatique et/ou de télécommunications ou l'interception d'un tel système fait sciemment et sans l'autorisation du responsable du système, en violant les règles de sécurité ou dans une intention malhonnête ou nuisible.

Toutefois, l'impossibilité de parvenir à une définition internationale a pour résultat de créer des difficultés pour connaître l'étendue réelle de cette fraude et pour en mesurer le volume économique. Car, l'absence d'une définition généralement admise empêche une comparaison des diverses statistiques rassemblées dans certains pays.

[14]. Ministère de l'intérieur de la France, *la criminalité informatique à l'horizon 2005*, FORS, Paris, octobre, 1991.
[15]. OCDE, *la fraude liée à l'informatiqu : analyse des politiques juridiques*, OCDE, Paris, 1986.

En 1989, le Conseil de l'Europe a retenu une approche plus formelle sur la criminalité informatique[16] , il a proposé une liste minimale et une liste facultative des délits informatiques qui devraient être réprimés dans le cadre des législations européennes.

1.3. Le poids du cybercrime

En l'absence d'instruments de mesure précis, le coût global du monde entier de la criminalité informatique demeure une inconnue. Les études ponctuelles réalisées dans les principaux pays concernés ont néanmoins permis de mieux cerner le sujet et d'en apprécier l'ampleur. Les formes de phénomène criminel et des risques liés aux technologies informatiques en général diffèrent selon les pays, la recherche des facteurs explicatifs de ces clivages demeure au stade des hypothèses. Les comparaisons internationales sont très difficiles à établir, les données exhaustives étant peu homogènes, voire inexistantes. Ces différences ne peuvent être précisément mesurées.

L'analyse des positions relatives des pays développés en matière de risques informatiques, à partir d'un ensemble d'hypothèses , montre que, globalement, toute comparaison ne peut s'effectuer sans références à la dynamique d'informatisation de l'économie. Le niveau des risques, la structure et le montant des pertes sont en effet étroitement dépendants des caractéristiques de l'environnements des entreprises et des organisations. Les spécificités des environnements économique, socioculturel, technique et juridique forment un système d'interactions, dont les risques informatiques résultent. Malgré tout, les comparaisons et mesures internationales , relèvent en effet des difficultés méthodologiques complexes.

Bien qu'il soit difficile de connaître avec précision l'ampleur réelle de la criminalité informatique, les enquêtes et les estimations réalisés par certains organisme permettent de dégager les principales caractéristiques de la criminalité au niveau mondial.

La dépense informatique mondiale est très concentrée : plus de la moitié aux Etats-Unis, environ 30% en Europe et près de 10% au Japon.[17] Les risques potentiels et le montant des pertes dus à la criminalité informatique sont donc également très concentrés, il semble que la hiérarchie des risques corresponde au degré d'informatisation.

Selon les estimations communiquées en France par le Centre de documentation et d'information de l'assurance (CDIA), la proportion[18] des pertes provoquées par des accidents ou des malveillances dans l'exploitation des moyens informatiques par rapport aux pertes globales est passée de 37% en 1985 à 58% en 1994, et ceci pour un mondant évalué actuellement à 6,4 milliards de francs français. Le nombre de fraudes

---

[16]. *Politique de lutte contre la criminalité liée à l'ordinateur en Europe et nouvelles formes de criminalité informatique*, rapport du dr. Manfred, Mohrenschiager présenté lors de la Conférence organisée conjointement à Luxembourg par le Conseil de l'Europe et la Commission des Communautés européennes, le 27 mars 1990.

[17]. *Criminalité informatique*, Paris : Presses Universitaires de France, 1988. (*Que sais-je ?* ; 2432).

[18]. Daniel PADOIN, *La police judiciaire contre les crimes sur les systèmes d'information*, Revue Internationale de Police Criminelle, n°457,1996.

informatiques signalées aux services de police judiciaire est très inférieur à celui connu des société d'assurances et présenté chaque année par le CDIA.

Depuis 1995 , le CSI (Computer Security Institue), avec l'aide du FBI (Federal Bureau of Investigation), fait chaque année des enquêtes sur ce sujet et édite son étude Computer Crime and Security Survey. L'étude tend à fournir des données statistiques sur des pertes directes engendrées par la criminalité informatique pour les entreprises.

Les résultats de l'analyse réalisée par le FBI et CSI sur Computer crime and Security 1997 montre une augmentation de 7% des accès à de l'information non autorisée par rapport à 1996. Les pertes totales cumulées sont supérieures à 100 millions dollars. 75% ont eus des pertes financières dues à des pénétrations au sein des systèmes informatiques 59% sont en mesure de quantifier les pertes occasionnées.

Selon son enquête de l'année 1998 sur les 521 grandes entreprises ou organisations gouvernementales interrogées, plus de la moitié ont rapporté avoir connaissance de pertes financières directes dues à la criminalité informatique. les pertes globales sont en augmentation[19] par rapport à 1997 (137 millions de dollars en 1998 contre 100 millions de dollars en 1997), Mais seules 31% peuvent les quantifier. Ainsi, s'il est possible de dire combien coûte la réparation d'un réseau ou l'arrêt de l'activité d'une chaîne de production pendant une semaine à une entreprise , il est plus difficile d'estimer le montant des pertes provenant du vol d'informations, de données, ou de la fraude à la propriété intellectuelle. Et c'est justement les tentatives d'infraction de ce type qui s'intensifient le plus, avec 30% d'augmentation par rapport 1997.

En effet, le premier délit informatique signalé aurait eu lieu aux Etats-Unis en 1958, mais la première criminalité informatique, identifiée comme telle et poursuivie au niveau fédéral (une altération d'états bancaires à Minneapolis) n'est intervenue qu'en 1966. Dans les pays nordiques, le premier délit informatique poursuivi, un cas de contrefaçon de logiciel caractérisée, a été commis en février 1968 en Finlande[20].

En général, dans le domaine de la criminalité informatique, les données sous-estiment fortement la réalité. Car lorsque les sociétés sont concernées par des actes illicites, moins d'un tiers d'entre elles le déclarent. Cette répugnance des victimes à dévoiler les défaillances de leurs systèmes informatiques s'explique essentiellement par des raisons d'image commerciale. On la retrouve dans tous les pays touchés par ce phénomène. La peur de la publicité négative et l'inquiétude de communiquer leurs mésaventures à leur concurrents prenant le dessus sur l'envie de retrouver l'auteur le la fraude. Aux Etats-Unis, seulement 1 à 2% des crimes informatiques sont détectés (d'après le FBI) ; en France, un tiers des pertes n'est probablement pas déclaré.

Il est clair que le phénomène de la criminalité informatique a des implications économiques importantes, même s'il est parfois difficile de les chiffrer précisément.

---

[19]. *Cybercriminalité et hackers professionels,* **http ://www.bull.fr/securinews/courant/cyhack.html**

[20]. Daniel PADOIN, précité.

2. Les formes de criminalité informatique

Actuellement, les criminologues distinguent un large éventail d'infractions liées à l'informatique, qui vont du vol de matériel ou de logiciel au piratage le plus ingénieux et à la propagation volontaire de virus, en passant par la simple manipulation frauduleuse des entrées. Leur nomenclature présente parfois des variantes, en fonction des définitions retenues.

La plupart des spécialistes ont tendance à proposer une classification qui distingue les affaires où l'ordinateur ou le réseau informatique sont la cible des affaires dans laquelle l'ordinateur ou le réseau informatique sont les instruments.

2.1. Type d'infractions informatiques dont l'ordinateur ou le réseau informatique sont la cible

Ce type porte essentiellement sur une atteinte à la confidentialité et à l'intégrité et la disponibilité des données.

Pour transmettre rapidement des informations sur la criminalité informatique, le Secrétariat général d'Interpol a mis au point un message type « criminalité informatique » normalisé qui a été présenté lors de la première Conférence internationale sur la criminalité informatique le 19 avril 1995. Le Secrétariat général recommande à tous les pays membres d'Interpol de l'utiliser pour communiquer ou demander des informations sur des infractions liées à l'informatique. Dans ce message type les définitions de diverses infractions liées à l'information sont précisées

Le système de codification des infractions informatiques du Secrétariat général d'Interpol recense près de trente types d'infractions[21] dont l'ordinateur et le réseau sont l'objet. Il est basé sur la Liste minimale des infractions établie par le Comité Européen du Conseil de l'Europe sur la criminalité informatique dont le principe est repris dans le projet de Convention relative à la criminalité dans le Cyberespace. Elles sont classées en six catégories.

2.1.1. Accès et interception non autorisés

- **Piratage informatique (hacking) :**

  « Accès non autorisé à un système ou à un réseau informatique. »

- **Interception illicite de données informatiques :**

[21]. Interpol Manual of standards and procedures *Computers and Crime*, 1996.

« Interception, sans droit et par des moyens technique, de communications à destination, en provenance et au sein d'un système ou d'un réseau informatique. »

- **Usage privé illicite de temps ordinateur :**

« Utilisation clandestine d'un système ou d'un réseau informatique, visant à éviter le paiement. »

- **Autres accès et interception non autorisés**

2.1.2. Modification de logiciels ou de données

- **Bombe logique :**

« Altération de programmes ou de données informatiques par l'insertion d'une bombe logique. »

- **Cheval de Troie :**

« Altération de programmes ou de données informatiques par l'insertion d'un cheval de Troie. »

- **Virus informatique :**

« Altération de programmes ou de données informatiques par l'insertion ou la propagation d'un virus informatique. »

- **Ver informatique:**

« Altération de programmes ou de données informatiques par l'insertion, le transfert ou la propagation d'un ver informatique. »

- **Autres modification logiciels**

2.1.3. Fraude informatique

- **Fraude informatique concernant les distributeurs automatiques :**

« Fraude et vol concernant des distributeurs automatiques de billets. »

- **Contrefaçon informatique :**

« Fraude et vol concernant des systèmes informatiques, par la fabrication de faux. »

- **Fraude informatique concernant les jeux:**

« Fraude et vol concernant des matériels de jeu. »

- **Manipulation informatique frauduleuse :**

« Fraude et vol par manipulation de programmes ayant pour objet l'introduction de fausses données ou la falsification de données produites par un système informatique. »

- **Fraude informatique liée aux moyens de paiement (terminaux points de vente) :**

« Fraude et vol concernant des moyens de paiement ou des terminaux points de vente. »

- **Piratage téléphonique :**

« Accès non autorisé à des services de télécommunications, obtenu sans respecter les protocoles et les procédures. »

- **Autre fraude informatique**

2.1.4. Reproduction illicite

- **Reproduction illicite de jeux informatique :**

« Reproduction, diffusion ou communication au public, sans droit, d'un programme informatique protégé par la loi. »

- **Reproduction illicite de logiciels :**

« Reproduction, diffusion ou communication au public, sans droit, d'un programme informatique protégé par la loi. »

- **Reproduction illicite de topographie de semi-conducteurs :**

« Reproduction sans droit de la topographie, protégée par la loi, d'un produit semi-conducteur, ou exploitation commerciale ou importation à cette fin, sans droit, d'un topographie ou d'un produit semi-conducteur fabriqué à l'aide de cette topographie. »

- **Autres reproductions illicites**

2.1.5. Sabotage informatique

- **Sabotage matériel informatique :**

« Entrée, altération, effacement ou suppression de données ou de programmes informatiques, dans l'intention d'entraver le fonctionnement d'un système informatique ou d'un système de communication. »

- **Sabotage logiciel informatique :**

« Effacement, détérioration ou suppression illicite de données ou de programmes informatiques. »

- **Autres sabotage informatique**

2.1.6. Infractions moyens informatiques (autres)

- **Infraction kiosque télématique (B.B.S.[22]):**

« Utilisation d'un B.B.S. en vue de stocker, d'échanger ou de diffuser des informations liées à une infraction. »

- **Vol secret de fabrique par voie informatique :**

« Obtention par des moyens illégitimes ou la divulgation, le transfert ou l'utilisation sans droit ni autre justification légale d'un secret commercial ou industriel, dans l'intention de causer un préjudice économique ou d'obtenir un avantage économique illicite. »

- **Matériels délictueux :**

« Utilisation d'un système ou d'un réseau informatique pour stocker, échanger, diffuser ou transmettre des matériels délictueux. »

[22]. Bulletin Borard Systèm. Serveur de messages et de l'informations accessible en ligne.

2.2. Type d'infractions informatiques dont l'ordinateur ou le réseau informatique sont les instruments

Ce type d'infraction relève de ce qu'on peut appeler la délinquances assistée par ordinateur, elle comprend les cas où l'ordinateur facilite le travail des criminels mais n'est pas essentiel. Et leur qualification pénale se rattache à celle des infractions classiques .

La société contemporaine est à l'ère de la révolution dans la domaine de la technologie de l'information. Les ordinateurs sont maintenant à la portée de la plupart des individus, au double point de vue de l'accessibilité et du coût. Un système informatique qui, il y a quelques années aurait occupé une grande salle peut aujourd'hui ne pas prendre plus de place qu'une machine à écrire et être d'un prix modeste. Du fait de la multiplication de ces petits systèmes informatiques, il n'est guère surprenant qu'ils commencent à être utilisés dans le cadre d'activités criminelles par les malfaiteurs, au même titre que d'autres instruments tels que les armes à feu et les voitures.

L'utilisation à grande échelle des ordinateurs a rendu certains domaines de la vie moderne tributaires de l'informatique. Le commerce, la banque, les transports, les archives publiques, les sources d'énergie nucléaire et les procédés automatisés de fabrication ne constituent que quelques exemples de domaines vitaux dans lesquels les systèmes informatiques jouent un rôle important. Dans de nombreux cas, tels que le contrôle du trafic aérien et les appareils de traitement médicaux sophistiqués, la protection des ordinateurs est directement liée à la protection de la vie humaine.

La liste des délits commis sur Internet , qui s'enrichit de jour en jour de nouveaux délits, comprend des actes qui entrent dans la typologie classique de la majorité des pays membres d'Interpol[23] : délits spéciaux en droit des affaires, délits d'atteinte aux droits de la propriété intellectuelle et industrielles, jeux de hasard, opération de vente pyramidale, détournement de fonds, etc.

En plus des activités criminelles traditionnelles, tels que racket , trafic de drogue et corruption qui l'accompagne, le blanchiment de l'argent et le délit d'initié, Internet a fait fleurir une multitude d'infractions liées à la circulation de l'information telles que les violations du droit d'auteur, les violations de la vie privée et du secret des correspondances, les délits de presse et de diffamation, la publicité mensongère, la diffusion de messages extrémistes ou contraires aux bonnes moeurs susceptibles d'être vus ou perçus par des mineurs, etc. A ces infractions, il convient d'ajouter des infractions qui mettent gravement en jeu le respect des libertés et droits fondamentaux de l'individu, comme le commerce illicite de base de données à caractère personnel et la pédophilie.

[23]. Souheil El ZEIN, L'indispensable amélioration des procédures internationales pour lutter contre la criminalité liée à la nouvelle technologie, 1998.

3. La typologie des criminels et leur motivations

La criminalité informatique est essentiellement orientée vers le profit, mais sans pour autant que tous les criminels informatiques aient des motivations similaires. D. Parker en distingue ainsi 7 catégories[24] d'après l'analyse de 1 000 cas recensés au Stanford Research Institute :

Les « amateurs », les plus nombreux, constituent la première catégorie de criminels informatique, détenant précisément ces postes de confiance grâce à un certain niveau de connaissances des techniques informatique. Le plus souvent, ils commettent un délit à cause de problèmes financiers, afin de compenser des difficultés professionnelles ou pour satisfaire leurs penchants égoïstes.

La seconde catégorie regroupe les « détraqués » ; ils utilisent la violence et souffrent de déséquilibres psychologiques plus ou moins graves.

La troisième concerne le crime organisé qui pourrait s'intéresser à l'informatique car les gains potentiels sont importants et les risques moins élevés que dans ses activités traditionnelles. Mais les cas sont relativement peu nombreux, soit parce que la mafia a encore peu investi dans le crime informatique, soit parce qu'elle ne s'est pas fait prendre. Mais lorsqu'elle utilise l'informatique, il s'agit d'opérations criminelles de grande envergure. En 1985, la mafia avait contacté indirectement un expert informaticien dans une société de services pour qu'il élabore un système de compensation interbancaire sur le modèle du réseau Swift utilisé par près de 1 700 banques de 54 pays. La mafia souhaitait prendre en charge le coût de développement du logiciel, tout en se réservant la possibilité de le contrôler et de prélever de façon frauduleuse une partie des flux financiers circulant sur le réseau. Heureusement l'opération n'a pas abouti, la femme de l'informaticien étant sur écoute téléphonique.

Les puissances étrangères forment la quatrième catégorie : les motivations essentielles sont l'espionnage ou le vol de secrets commerciaux.

Les criminels professionnels constituent la cinquième catégorie qui n'appartenant pas au crime organisé, ils sont également peu nombreux à commettre des délits informatiques, car relativement marginalisés, ils ont plus rarement des opportunités. Il leur est plus difficile d'assimiler les techniques informatiques et ils préfèrent souvent exercer des activités plus classiques (hold-up, racket, trafic de stupéfiants...). Les cas connus concernent essentiellement des escroqueries effectuées à l'aide d'ordinateurs.

La sixième catégorie regroupe les « casseurs de systèmes », ils utilisent les failles dans les procédures d'accès aux systèmes informatiques. La perfidie ou la supercherie ne seraient pas nécessairement à l'origine de la fraude ; ils cherchent tout simplement à

[24]. D.-B. Parker, *Combattre la criminalité informatique*, Paris, Ed. Oros, 1985, p. 18.

atteindre un but, sans vouloir en tirer profit, tout simplement « pour se faire plaisir ». Ce ne sont pas forcément des professionnels. Beaucoup d'entre eux sont des collégiens, ou des étudiants.

La dernière catégorie rassemble les « extrémistes idéalistes », essentiellement des groupes terroristes.

Une typologie plus sommaire est proposée par Bologna[25] ; il distingue les comportements des criminels informatiques : économiques (recherche de gains financiers), égocentriques (la recherche de reconnaissance sociale, le gain n'étant pas primordial), idéologiques (revanche sur la société) et psychotiques caractérisés par la perte du sens des réalités.

En fait, selon Philippe Rosé[26] quel que soit le degré de précision des typologies et leurs dénomination, les motivations essentielles correspondent à quatre catégories de criminels informatiques

Tout d'abord, les « utilitaristes » qui ont pour objectif le gain financier ; ils effectuent principalement des détournements de fonds . ensuite, les « entrepreneurs » agissent par jeu ou par défi en pénétrant les réseaux et les systèmes informatiques. Ils pratiquent le piratage des logiciels et des données et sont spécialistes de la recherche des mots de passe. Ils contestent leur assimilation aux autres criminels informatiques, se considèrent inoffensifs et affirment utiliser un code de déontologie (ne pas créer de dommages aux systèmes qu'ils pénètrent). Les « agressifs », la troisième catégorie, agissent guidés par le désir de compenser une frustration personnelle ou professionnelle. Ils utilisent les bombes logiques, les chevaux de Troie, les virus, le vol de données et de fichiers... Enfin, les « destructeurs » ont pour but de nuire aux entreprises ou organisations aux quelles ils s'attaquent, par le sabotage ou le terrorisme.

Il est évident que le criminel informatique n'a pas une motivation unique, ses objectifs sont souvent variés et complémentaires. Les typologies ne font que suggérer un découpage possible ; les frontières entre les différentes catégories de criminels sont souvent difficiles à établir.

[25]. G.-J. Bologna, An Organizational Perspective on Enhancing Computer Security, Communication au Congrès Sécuricom, 1986.

[26] . Philippe Rosé, *Criminalité informatique*, Paris : Presses universitaires de France, 1988. Philippe Rosé. (*Que sais-je ? ;* 2432)

4. La criminalité informatique la plus fréquente

Si l'on se base sur les archives criminelles d'Interpol, sur les statistiques nationales et internationales et sur les informations officieuses qui circulent, on constate que les cas les plus connus et les plus fréquents sont les piratages informatiques (activités des « hackers »), les piratage téléphonique, les modifications des logiciels et des données et la pédophile sur Internet.

4.1. Piratage informatique

Le piratage informatique est également appelé souvent « intrusion » et « hacking ». C'est une pratique consistant à entrer par effraction dans un réseau informatique, en forçant ou en contournant les dispositifs de sécurité d'un ordinateur. Le piratage n'est pas à prendre à la légère, la plupart des principaux systèmes informatiques dans le monde étant connectés à des réseaux.

Interpol a donné de cette infraction la définition suivante : « accès non autorisé à un système ou un réseau informatique. »

« Accès » signifie « intrusion dans tout ou partie d'un système et des programmes ou données qu'il contient ». La méthode de communication importe peu : l'accès peut être local et direct ou à distance et indirect, par exemple via une liaison satellite ou d'autres systèmes informatique.

Les pirates utilisent fréquemment des messageries ou serveurs télématiques permettant des échanges d'informations entre utilisateurs. En échangeant des numéros informatiques à composer et en profitant de mots de passe périmés et d'autres failles dans les systèmes informatiques, ils peuvent avoir accès à des systèmes informatiques et obtenir des informations précieuses. Dans le cadre de leurs activités, ils ont inventé un nouveau jargon ou langage et utilisent des pseudonymes pour dissimuler leur véritable identité.

Le piratage constitue une infraction spécifique dans certains pays, alors que dans d'autres, la législation traditionnelle en vigueur est invoquée pour traduire les auteurs en justice. Certains considèrent cette pratique comme un jeu ou un passe-temps, mais les victimes la prennent au sérieux. Parce que parfois, le piratage ou l'accès non autorisé à des systèmes informatiques constitue la première étape d'une infraction plus grave, telle que l'espionnage ou le sabotage.

Devant la conférence des ambassadeurs, le 28 août 1998, un commissaire de la DST, Daniel Martin[27], a évoqué des cas tout récents d'attaques de systèmes informatiques par des groupes organisés de pirates. En mai, une équipe de « hackers » âgés de quinze à dix-huit ans, The Milworm, est ainsi entré dans le réseau d'un centre de recherches atomiques indien et y a volé des travaux sur les derniers essais nucléaires ordonnés par les autorités de New Dehli. En août, des partisants des Tigres tamouls, rebaptisés pour l'occasion les Tigres noirs de l'Internet, ont lancé une attaque contre le réseau reliant les ambassades du Sri-Lanka, bloquant les boîtes aux lettres électroniques de toues ses représentations dans le monde. En septembre, les messages émis par le service de sécurité du président des Etat-Unis ont été diffusés sur un serveur Internet.

Une autre sorte de piratage informatique consiste à entrer illégalement sur le serveur web et à modifier les pages existantes.

En mai 1996, un office spécialisé du Sénat des Etats-Unis avertit : « des entités hostiles peuvent s'emparer de systèmes d'information de la Défense, affectant gravement notre capacité à déployer et soutenir nos force armées ». Il signale aussi 162 500 infiltrations réussies dans les ordinateurs de la Défense nationale américaine en 1995[28].

Le 29 décembre 1996, un pirate a attaqué un site de l'US Air Force et a remplacé la page principale par des images à caractère pornographique. Le résultat a été que le « DefenceLINK » du pentagone, qui inclue environ 80 homepages, a été débranché pendant plus de 24 heures pour que les officiers s'assurent qu'il n'y avait pas d'autres brèches de sécurité sur le système.

Pendant l'été 1996, des hackers se sont introduits sur le serveur web de l'US Depertmentof Justice en plaçant des croix gammées et des images d'Adolf Hitler qu'ils assimilaient au département de la justice américaine. Ils voulaient protester contre la position du gouvernement américain à contrôler l'Internet.

Le 30 aût 1999, le système de messagerie électronique Hotmail de Microsoft a été attaqué par des pirates informatiques[29] . Ils ont donné libre accès aux boîtes aux lettres de quelque 40 millions d'utilisateurs de la messagerie électronique Hotmail via un site Internet basé en Suède. Ce site créé par des pirates permettait à tous ceux qui le souhaitaient d'accéder librement au contenu des boîtes de n'importe quel utilisateur de Hotmail. Il suffisait simplement de connaître le nom d'un utilisateur pour pouvoir prendre connaissances de ses messages, sans le mot de passe habituellement requis. La société Microsoft, opératrice de Hotmail, une messagerie électronique gratuite parmi les plus populaires, a finalement été contrainte de fermer pour que ses ingénieurs modifient les serveurs abritant le système de messagerie. Le problème a été résolut le lentemain mais ses boîtes aux lettres sont restées accessibles six heures durant.

[27]. voir Dossier Délinquance, *Le Monde*, 22/09/1998.

[28] . Daniel Martin, *la criminalité informatique*, Presse universitaires de France, avril 1997, Paris.

[29] . Selon la source de l'Agence France Presse , le 30 août 1999, Paris.

4.2. Piratage téléphonique

Le piratage téléphonique est souvent appelé phreaking en anglais. Il peut se décrire comme le détournement de services de télécommunication par divers procédés, dans le but d'éviter les grosses factures de téléphone ou les oreilles indiscrètes .

Interpol donne du piratage téléphonique la définition suivante : « Accès non autorisé à des services de (télé) communication, obtenu sans respecter les protocoles et les procédures. »

Les premiers cas de piratage téléphonique recensés remontent aux année 60 . A cette époque , le piratage informatique était une activité essentiellement pratiquée par des adolescents qui savaient obtenir la tonalité et passer gratuitement un appel local d'une cabine téléphonique en provoquant un court-circuit au moyen d'une pince ou d'une épingle à cheveux placée entre le microphone et le monnayeur. Ils connaissaient aussi certainement d'autres moyens de passer des appels téléphoniques sans payer.

La commutation des lignes utilise des fréquences vocales que l'on peut reproduire avec un ordinateur et une carte sonore. Petit à petit les techniques se sont perfectionnées, Le premier véritable outil des pirates c'est ce qu'on appelle en anglais le boxing, une petite boite remplie de composants électroniques qui permettant de reproduire exactement cette fréquence, soit 2600 hz, c'est-à-dire, de façon générale, l'utilisation d'équipements électroniques dans le but de leurrer les centraux téléphoniques . Les « boîtes »(boxes) génèrent des signaux sonores qui trompent le central, et celui-ci répond par exemple en libérant des lignes ou en arrêtant le compteur d'unité.

Les pirates ont inventé différents types de « boîtes » (boxes), désignés chacun par sa couleur[30]. La boite noire comporte un ou deux interrupteurs ; elle est reliée à la ligne téléphonique du destinataire de l'appel et permet de lui téléphoner gratuitement .L'activation de la boîte supprime le signal qui indique que le destinataire de l'appel a décroché et qui déclenche le compteur. la boite blanche (cheese box) permet de mettre en relation deux personnes qui appellent deux numéros différents correspondant au même local. Un correspondant appelle un des deux numéros et reste en communication tandis que la deuxième personne appelle l'autre numéro, la communication étant établie entre les deux l'intermédiaire de la cheese box. La boite rouge permet de générer des signaux identiques à ceux qui sont émis lorsque l'usager d'une cabine publique introduit des pièces dans la fente de ma machine. La boite violette reliée à la ligne d'une personne qui passe des appels à longue distance, envoie au central téléphonique le même signal que s'il s'agissait d'un appel local, de telle sorte que l'appelant n'a pas à payer le prix des communication s à longue distance.

La « boîte » la plus répandue est la « boite bleue ». Elle existe depuis longtemps déjà, mais elle a été modifiée et perfectionnée au cours des années. Le pirate compose un numéro et à l'aide de sa boite bleue, génère un signal à 2600 Hz juste au moment de la

[30]. Raymond McGoverna, la fraude aux télécommunication, *Revue internationale de police criminelle*, n°464, 1997.

connexion. Ce signal trompe le central téléphonique local en lui indiquant que la communication est terminée. Le pirate compose alors sur sa boite bleue le numéro du correspondant auquel il veut parler, et la communication est établie. Le central interprète cet appel comme provenant d'un autre central et ainsi la communication n'est pas facturée au pirate.

Un autre moyen simple de frauder consiste à obtenir les codes permettant de passer des appels à longue distance. Lorsque ces codes ont été introduits, ils comportaient seulement six à huit chiffres. Ils pouvaient être piratés soit manuellement à partir d'un téléphone à touches, soit par des moyens informatiques, à l'aide d'un ordinateur et de logiciels conçus à cet effet. Il est possible de se procurer ces codes en appelant le numéro d'accès propre à chaque compagnie de téléphone, en essayant un code puis en composant le numéro du correspondant ; si la communication est établie, c'est que le code utilisé était le bon.

Un autre type de piratage téléphonique est l'utilisation détournée des téléphones cellulaires. Avec ce type de téléphones, aucune connexion physique n 'est nécessaire, et il est facile d'écouter les conversations au moyen de scanners, Les téléphones cellulaires sont aussi facilement reprogrammables : les malfaiteurs peuvent ensuite les utiliser sans payer leurs communications, qui seront facturées aux véritables propriétaires.

4.3. Modification de logiciels ou de données

Il s'agit des insertions des programmes malveillants. L'objectif est d'altérer des données ou des programmes, ou de gêner leur utilisation, en mettant de ce fait en péril l'intégrité ou la confidentialité du système lui-même ou de ses sorties.

4.3.1.Les virus informatiques

Dans le manuel de criminalité informatique d'Interpol, on en donne la définition suivante : « altération non autorisée de données ou de programmes informatiques par l'insertion ou la propagation d'un virus »

Les virus informatiques sont des programmes informatiques qui se reproduisent jusqu'à paralyser le fonctionnement normal de l'ordinateur. Ils infectent discrètement les programmes sur disques et peuvent être difficiles à déceler. Les conséquences d'un virus peuvent aller de la simple farce à la destruction complète des données. Les utilisateurs propagent souvent involontairement les virus lors des opérations quotidiennes telles que l'utilisation d'un disque sur plusieurs machines.

Il existe à l'heure actuelle des milliers de types de virus informatiques[31]. Chacun a ses caractéristiques propres, mais tous altèrent les fichiers de données ou les programmes. Mais plusieurs catégories de virus informatiques ont été analysées par des fonctionnaires de police spécialisés ou des professionnels indépendants. De ce fait, la plupart des virus peuvent être facilement décelés et des remèdes être trouvés.

Les virus informatiques sont de véritables entités internationales. Ils se transportent de toute évidence d'un ordinateur à l'autre et d'un pays à l'autre. Les modes de propagation des virus informatiques sont principalement suivants :

- logiciel informatique piraté ou illicite
- logiciel partagé
- disquettes offerts par les revues informatiques
- logiciel non breveté
- jeux informatiques, souvent copiés dans les écoles et les lycées.
- l'utilisation de messageries ou serveur télématiques et le téléchargement des données comportent un risque élevé d'infection par virus.

4.3.2. Cheval de Troie

La définition de cet infraction : « altération non autorisée de données ou de programmes informatiques par l'insertion d'un Cheval de Troie .»

Le Cheval de Troie est un programme dissimulé dans un système informatique . Contrairement aux virus informatiques, le Cheval de Troie ne se multiplie pas nécessairement. Il consiste à ajouter quelques lignes d'instructions dans une programme existant qui ont pour résultat de faire exécuter par l'ordinateur des opérations non programmées. Très souvent , une « trappe » est pratiquée, permettant l'accès non autorisé à un programme ou un ordinateur. Les pirates l'utilisent fréquemment pour se ménager une entrés dans les systèmes en mettant les mécanismes de protection en échec et en se servant un accès au moyen d'un code secret.

L'affaire de la « disquette du SIDA» (1989) en constitue un exemple. 20000 disquettes contenant un programme d'information sur le SIDA et contenant aussi un programme caché qui modifiant l'un des fichiers du système, ont été envoyées de par le monde, dans un emballage faisant croire qu'elles provenaient de l'OMS. Lors de l'utilisation du programme, le traditionnel texte de la licence s'affiche, mettant en garde l'utilisateurs contre l'utilisation frauduleuse du logiciel et l'invitant à payer le logiciel. Et en fait , lorsque l'utilisateur lançait le programme , un compteur caché démarrait qui, lorsqu'il atteignait 90, chiffrait tous les fichiers de données et rendait l'ordinateur inutilisable.

[31]. Les experts en virus estimaient qu'il existait près de 6500 virus et que chaque jour il en apparaissait deux ou trois. *le Guide clandestin de la sécurité des ordinateurs* écrit par Michael Alexander, International Thomson Publishing France, Paris, 1997, p.33.

4.3.3. Bombe logique

La définition : « altération non autorisée de données ou de programmes informatiques par l'insertion d'une Bombe logique .»

La Bombe logique est un mécanisme logique introduit par les malfaiteurs, qui se déclenche lorsque l'ordinateur exécute une tâche donnée. Une fois déclenché, le mécanisme lance un petit programme dont l'exécution affecte le fonctionnement de l'ordinateur ou du réseau de différentes manières : arrêt complet de l'ordinateur, affichage de pages d'écran vierges, destruction de données, etc.

Il s'agit du nom donné à la pratique illicite consistant à introduire une simple modification dans le code source du programme, qui déclenchera un processus de destruction. La bombe logique sera activité par une date ou par un événement particulier, tel que présence ou absence de données. Les auteurs de la bombe logique sont généralement eux-mêmes programmeurs.

4.3.4. Les vers

Interpol donne à cette infraction la définition suivante : « Altération non autorisée de données ou de programmes informatiques par l'insertion ou la propagation d'un ver informatique dans un réseau informatique. »

Les vers sont des programmes destructeurs analogues aux virus, qui sont créés pour les réseaux informatiques. et altérer des données. Ils se reproduisent intégralement en créant des copies conformes d'eux-mêmes.

On les trouve dans les réseaux informatiques et les ordinateurs sur lesquels travaillent plusieurs utilisateurs. Il se déplacent en utilisant les communications inter-ordinateurs comme moyen de transport. Ils sont en général conçus pour s'attaquer aux gros systèmes informatiques. Les vers se rencontrent peu ; ils sont moins fréquents que les virus.

L'affaire la plus connue et la plus dévastatrice est le ver d'ARPANET. Le 2 novembre 1988, un étudiant de l'université de Harvard a lâché un ver sur le réseau ARPANET. Le ver s'est transmit de machine en machine grâce à une faille dans le système de messagerie électronique. Le ver sature les machine s contaminées en se reproduisant. Très vite, l'ensemble des communications sur le réseau est très fortement ralenti. Les administrateurs systèmes n'ont pas eu d'autres chois que de déconnecter leurs machines du réseau.

4.4. La pédophile sur Internet

Actuellement Internet jouit d'une immense popularité. Il est généralement admis qu'entre 50 et 90 millions de personnes, disséminées un peu partout dans le monde, utilisent le réseau Internet. Or l'intégration de ce mode de communication à la culture populaire accroît le risque qu'il soit utilisé à mauvais escient. Le réseau Internet, qui est un réseau à longue distance, ou plus précisément une infrastructure permettant le transport des données, a été conçu pour échanger efficacement des informations sur le plan international. Ce réseau est mondial et ne connaît pas de frontières. Il est très difficile à contrôler et constitue par conséquence un moyen de dissimulation très efficace pour les utilisateurs . Les malfaiteurs, qui ont très vite découvert ses avantages, ont décidé de l'utiliser pour des activités illégales.

La pédophilie est un exemple particulièrement saisissant de criminalité ayant pris de l'ampleur grâce à Internet. L'exploitation des enfants à des fins sexuelles est un problème mondial, Ainsi on estime que l'industrie du sexe fait plus d'un million de nouvelles victimes chaque année. Selon une étude menée par la Carnegie Mellon University, à Pittsburgh, en Pennsylvanie, la diffusion d'images à caractère sexuel constitue l'une des plus importantes activités criminelles utilisant les réseaux informatiques. Pendant longtemps, les pédophiles opéraient dans des cercles assez restreints . Désormais, ils ont la possibilité d'offrir ou d'acquérir du matériel photo ou vidéo dans le monde entier. et cela , juste en pianotant sur le clavier d'un ordinateur . Les pédophiles peuvent y reproduire des informations ou des photos, Internet est en fait apparu très insidieusement. l'anonymat y est préservé, la distribution de documents est simple et la quantité de matériaux que le réseau peut transporter est sans limite.

Depuis quelque temps, on constate un accroissement des forums qui s'adressent aux pédophiles en leur offrant des adresses, des informations ou tout simplement des images. Ces échanges d'informations sont facile grâce à Usenet, une sorte de messagerie implanté e dans Internet. Au lieu d'envoyer un message à une personne, l'utilisateur participe à des « newsgroups » sur des thèmes particulier. Selon le Groupe de travail d'Interpol, sur 25.000 « newsgroups » , 0,07% contiennent des matériaux pédophiles . Rien qu'en janvier 1998, 6.000 photos pédophiles ont ainsi été diffusées[32].

Avec le web, les réseaux de pédophiles s'étendent sans souci des frontières ni des législations. Sur Internet certains sites sont de véritables « boutiques porno virtuelles ». Selon des spécialistes, il y a plus de 5.000 sites de pornographie[33], ce chiffre étant en augmentation constante. Beaucoup sont protégés par une diversité de logiciels de cryptage estimés à quelques 350 logiciels en libre circulation. En outre, une enquête réalisée en 1994 aux Etas-Unis en vient à la conclusion que le réseau Internet renfermait alors plus de 450 000 images ou fichier-textes de nature pornographie . En fait les sites pédophiles se sont multipliés aussi sur Internet. Ces sites ne sont pas pour autant

[32]. Souheil EL ZEIN, *l'indispensable amélioration des procédures internationales pour lutter contre la criminalité liée à la nouvelle technologie,* 1998.

[33]. Raymond Edward Kendall, Secrétaire général d'Interpol, Interpol fête ses 75 ans au coeur de la coopération internationale policière, *the Diplomatic Letter* n°44, 10/1998.

accessibles au premier internaute venu. On ne s'y retrouve jamais par hasard, pour les atteindre , et surtout y rester, il faut s'entourer de précautions : pseudonyme, mots-clés, langage codé, numéros de carte bancaire...Les intrus ont tôt fait d'être repérés et « expulsé » par les habitués du lieu.

5. La sécurité informatique

Les ordinateurs renferment de plus en plus de secrets personnels , professionnels et étatiques. Les médecins leurs confient des informations médicales sur les patients ; les entreprises leurs données stratégiques ; les banques les comptes de leurs clients...Mais ces données sont-elles bien protégées ? On peut en douter quand on constate le formidable essor du piratage informatique.

Nos ancêtres ont édifié de nombreux châteaux forts pour se protéger. Déjà, à leur époque, ils avaient évalué les menaces et appliquaient une politique de sécurité défensive fondée sur un périmètre restreint : l'enceinte. De nos jours, la sécurité de l'information est vitale au bon fonctionnement des systèmes économiques et concerne l'ensemble des acteurs. Il faut également bâtir pierre par pierre les fortifications de nos politique de sécurité[34]. La mise en place d'une défense informatique inclut des solutions techniques et des règles humaines. Surtout la sécurité est assurée avant tout par des hommes. C'est une évidence souvent oubliée en informatique, qui suppose la volonté de l'ensemble des personnes d'appliquer les règles de la politique de sécurité.

5.1. La protection technique contre les pirates

Toute sorte de gens peuvent désirer s'infiltrer dans des systèmes d'information. Cela va des curieux qui sondent le système simplement pour voir ce qu'il y a dessus, aux pirates qui veulent détruire des données ou nous nuire d'une manière différente.

Sur Internet le problème de la sécurité informatique se pose aujourd'hui plus que sur n'importe quel autre réseau. Internet est un énorme réseau de réseaux répandus de par la planète, il est le précurseur des autoroutes de l'information , il s'agit d'un lieu où tout le monde veut être actuellement. Aujourd'hui, à moindre coût et avec quelques connaissances informatiques, n'importe qui peut de chez lui, se connecter sur Internet . Et toute personne possédant un ordinateur qui se connecte sue Internet peut subir une malveillance informatique.

5.1.1. Les comportements des pirates

Contrairement à ce qu'on pourrait penser, la plupart des pirates ne sont pas des spécialistes très forts. Ils sont simplement des personnes et presque toujours de jeunes hommes bien informés sur les manières de pénétrer dans un système informatique. Ils sont justement plus obstinés que les autres dans ce domaine.

[34]. Sur la mise en place d'une défense d'un réseau, Jen-Louis MELIN, bâtir son réseau comme une forteresse, *Informatique magazine,* 11 juin 1999.

Certains pirates n'obtiennent pas normalement les informations dont ils ont besoin pour pénétrer dans les systèmes en sondant leur contenus avec zèle, puis en sautant pardessus les barrières électroniques. La plupart du temps, ils appellent un employé sans méfiance, et l'amènent à leur donner un mot de passe. Ou bien ils se font passer pour un nouvel employé qui a besoin d'aide pour se connecter sur le système, ou ils prétendent être un technicien qui a besoin de l'employé pour tester le système.

Si cette technique ne marche pas , ils vont fouiller dans les poubelles à la recherche de manuels d'informatique , de disquettes ou de morceaux de papier contenant des codes d'accès. Cette approche manifestement peu scientifique est une des sources productives d'information que les pirates et autres personnes de l'extérieur utilisent pour s'infiltrer dans un système.

Certains pirates essaient des centaines de combinaisons avant qu'une porte informatique s'ouvre. Le mode de réflexion des gens est également assez prévisible, et les pirates en ont conscience. Ils savent que la plupart vont choisir un mot de passe qui leur rappelle une personne, un endroit, un animal, ou un centre d'intérêt personnel, de façon à pouvoir s'en souvenir facilement. La manière la plus classique employée par un hacker pour essayer d'obtenir un mot de passe consiste à utiliser un dictionnaire. Dans ce genre d'attaque, le hacker utilise un dictionnaire de mots et de noms propres, et il les essaie un à un pour vérifier si le mot de passe est valide. Bien évidemment, ces attaques ont recours à des programmes qui peuvent essayer des centaines voir des milliers de mots de passe à la seconde. Ce procédé est d'autant plus facile, qu'il lui permet de tester des variations sur ces mots : mots écrits à l'envers, majuscules et minuscules dans le mot, ajout de chiffres à la fin du mot, etc...De plus la communauté des hackers a construit de gros dictionnaires spécialement conçus pour casser les mots de passe.

Les données voyagent par « paquets » sur Internet. Il s'appellent paquets d'informations (information packets, IP). Chaque paquet est inséré dans une enveloppe électronique et comme toute enveloppe, comprend une adresse « destinataire » et une adresse « expéditeur ». L'adresse IP d'un ordinateur est l'adresse qui est utilisée pour reconnaître un ordinateur sur Internet. Elle est présumée valide lorsqu'elle est certifiée par les services TCP et UDP. Si une machine se connecte sur une autre machine, les deux machines établissent un système de confiance. Les pirates peuvent profiter de ce type de relation de confiance pour pénétrer sur une machine. Ils créent des paquets avec l'adresse d'une machine connue et les envoient sur une autre machine de confiance, qui pense qu'il s'agit d'un ordinateur certifié , alors elle accepte la connexion.

Les pirates se maintiennent au courant des derniers progrès dans les domaines et ils ont de bon outils. Ils ont des besoins important afin d'obtenir et d'échanger de l'information sur la manière de trouver les mots de passe des ordinateurs, la construction d' une boîte permettant de passer des appels téléphoniques gratuitement, le moyens de se faire passer pour quelqu'un d'autre en envoyant des messages sur Internet, ...

Au royaume des pirates, l'information est une monnaie négociable. Pour jeter un coup d'oeil sur certains des meilleurs fichiers se trouvant sur un BBS fréquenté par les pirates et traitant de la manière de faire sauter un système informatique, il se peut que l'on vous demande de préalablement payer avec une carte de crédit . Ils fréquente « alt.2600 [35]», une conférence sur Internet où pullulent les pirates ,les reporters du secteur informatique, et tout ce qui gravite autour de ce sujet. On y trouve toute sortes de discussions sur la manière de pénétrer dans divers systèmes, de phreaker les systèmes de téléphone, de faire sauter le dispositif anti-copie des logiciels protégés et on vous indique également où aller pour se procurer les derniers outils en manière de piratage. Un bon endroit pour le débutant est **FAQ** (Frequenly Asked Questions) sur **alt.2600**. C'est une riche encyclopédie de conseils et techniques de piratage.

5.1.2. les outils utilisés par les pirates

Les mots de passe sont très important parce que c'est la première ligne de défense contre les attaques sur un système. Ceci peut être établit simplement : si un hacker ne peut pas interagir sur un système distant et qu'il ne peut pas ni lire ni écrire dans le fichier des mots de passe alors il n'a quasiment aucune chance de développer une attaque couronnée de succès sur ce système. c'est également pourquoi, si un hacker peut au moins lire le fichier des mots de passe sur un ordinateur distant, il aura aussi la possibilité de cracker un des mots de passe contenu dans ce fichier. S' il en parvient, alors on peut penser qu'il pourra se connecter sur ce système et qu'il pourra s'introduire en tant qu'administrateur en passant par un trou de sécurité dans le système d'exploitation.

La plupart des outils utilisés par les pirates pour s'infiltrer dans les systèmes informatiques étaient à l'origine des outils de dépannage, d'amélioration de la performance, et d'évaluation de la sécurité. Ainsi, pour évaluer les performances d'un réseau local, on utilise un « renifleur ». Pendant qu'il vérifie, par exemple, le flot de paquet sur un réseau local, le renifleur ramasse également des mots de passe. Il y a aussi les programmes comme **Cracker jack** pour les machine sous MS-DOS et **Crack** pour les stations UNIX, qui sont conçus uniquement pour trouver les mots de passe et qui sont largement disponibles sur Internet et les BBS clandestins.

Les programmes les plus populaires (au moins auprès des pirates) pour deviner les mots de passe contiennent des minidictionnaires des mots les plus communément utilisés comme mots de passe. Ils envoient ces mots à l'ordinateur un par un jusqu'à ce que l'un d'entre eux corresponde au véritable mot de passe. Il suffit de quelques secondes pour trouver un mot de passe ayant un seul caractère, de quelques minutes pour un mot de passe en composant deux et de quelques heures pour un mot de passe qui en a trois. Ce procédé est d'autant plus facile, qu'il lui permet de tester des variations sur ces mots : mots écrits à l'envers, majuscules et minuscules dans le mot, ajout de chiffres à la fin du

[35]. voir *le Guide clandestin de la sécurité des ordinateurs* écrit par Michael Alexander, International Thomson Publishing France, Paris, 1997, p.12.

mot, etc...De plus la communauté des hackers a construit de gros dictionnaires spécialement conçus pour cracker les mots de passe. La plus connu des programmes utilisé pour cracker les mots de passe est « **Crak 4.1** » avec son dictionnaire de 50 000 mots.

Le « sniffing » de mots de passe est aussi une façon assez populaire des pirates pour obtenir un mot de passe. la plupart des réseaux utilisent la technologie de « broadcasting » ce qui signifie que chaque message (ou paquet) qu'un ordinateur transmet sur un réseau peut être lu par n'importe quel ordinateur situé sur le réseau. En pratique, tous les ordinateurs sauf le destinataire du message vont s'apercevoir que le message ne leur est pas destiné et vont donc l'ignorer. Mais par contre, beaucoup d'ordinateurs peuvent être programmés pour regarder chaque message qui traverse le réseau. Si une personne mal intentionnée fait ceci, alors elle pourra regarder les messages qui ne lui sont pas destinés. Les hackers ont des programmes qui utilisent ce procédé et qui scannent tous les messages qui circulent sur le réseau en repérant les mots de passe avec les programmes de sniffing. Les programmes de sniffing les plus connus sont : **Esniff.c** et **TCPDump.**

Il faut se méfier des types d'outils qu'on utilise sur le système pour faire des diagnostics et des réparation, ils peuvent facilement se retourner contre le système qui les emploie.
un nouvel outil de sécurité informatique qui va encore faciliter la tâche, même aux plus novices d'entre eux, pour faire irruption dans des ordinateurs ou des systèmes. C'est outil s'appelle **Sesurity Administrator Tool for Analyzing Networks** (SATAN en abrégé), et ses concepteurs pensent que cela va aider les responsables de la sécurité à sonder leur ordinateurs pour en détecter les points faibles. Le problème est que **SATAN** est facilement accessible à toute personne qui veut l'obtenir, y compris aux pirates qui vont l'utiliser pour tenter de s'infiltrer dans les ordinateurs. Et en plus, c'est gratuit.

War Dialers est un programme qui compose à répétition des numéros de téléphone pour détecter la tonalité identifiant un ordinateur. Les pirates peuvent composer le numéros trouver de quel type d'ordinateur il s'agit, et si possible , s'y infiltrer. Actuellement le meilleur *war dialer* disponible pour les utilisateurs PC-DOS est **ToneLoc** de Minor Threat and MuchoMeas. Ce moyen de tester les numéros est illégal dans certains pays, mais il est difficile d'empêcher un pirate de l'utiliser.

5.1.3. Protection par mot de passe contre les pirates

Une des manières principales de limiter ou de contrôler l'accès à une machine est d'utiliser des mots de passe, mais tous les utilisateurs d'ordinateurs n'en saisissent pas réellement l'importance.

5.1.3.1. Les dispositifs de protection par mot de passe

Une nombre croissant de programmes , économiseurs d'écran, traitements de texte, base de données, utilitaires d'installation de disque dur, etc. sont dotés des fonctions optionnelle de protection par mot de passe.

- L'économiseur d'écran de l'ordinateur est doté d'une fonction de sécurité pour reserver son accès aux personnes autorisée. Il suffit d'aller dans le panneau de contrôle et de créer un mot de passe, puis écrire un message dans le style : « Ce PC est protégé . Accès restreint !» etc.

- De nombreux traitements de textes, tableurs, et autre applications courantes sont maintenant fournis avec une option mot de passe. Pour illustration, on peut protéger un document sous Microsoft Word ou Excel en sélectionnant Option dans le menu Outils puis en tapant un mot de passe. Mettre un mot de passe sur un document de façon à ce que personne ne puisse le regarder ou le changer donne une sereine impression de sécurité.

- Les programmes d'installation fournis avec les disques durs offrent généralement une fonction de protection par mot de passe. Une option permet de diviser le disque en partitions ou volumes et de les protéger par un mot de passe. On peut stocker les données sensibles dans une partition et la protéger.

- Les PC récents permettent de protéger la machine par un mot de passe en créant un mot de passe sur l'écran d'installation CMOS. La manière de le faire varie selon les machines, mais dans de nombreux cas, il faut appuyer sur les touches F1 ou Suppr au démarrage ou utiliser la disquette d'installation fournie avec l'ordinateur.

- Plusieurs programmes de base de protection par mots de passe comme **DikLock** de Symantec disponibles sur le marché et conçus pour empêcher les intrus de venir sur la machine le font principalement en verrouillant le disque dur. Certains offrent davantage qu'un simple verrouillage du disque dur comme, par exemple, une fonction d'alerte en cas de tentative de violation de la sécurité.

5.1.3.2. La création des mots de passe inviolables

- Bien sûr les longs mots de passe sont manifestement plus sûrs que. Mais il faut garder à l'esprit que certains systèmes ne permettent pas d'utiliser par exemple, un mot de passe de 12 caractères. Selon la plupart experts ,normalement en choisissant un mot de passe d'au moins sept caractères, on doit être correctement couvert.

- Il est préférable de mélanger des caractères majuscules et minuscules, chiffres et des symboles en créant un mot de passe comme $ & % pour ajouter un niveau de protection supplémentaire.

- pour se rappeler facilement d'un mot de passe, qui soit cependant difficile à deviner, On peut utiliser un signe ou une expression. Il est par exemple facile de se remémorer aisément IYA50MDV si on sait que cela signifie : « Il y a 50 manières de vivre ».

- Changer le mot de passe au moins tout les deux mois.

- Ne pas utiliser le même mot de passe pour tous les systèmes informatiques que ce soit la carte de distributeur de billets de banque, le compte en ligne, l'ordinateur de bureau, ou le portable.

- il est proposé d'installer un programme qui n'autorise pas un nombre illimité de tentatives de saisie d'un mot de passe, après quelques tentatives se bloque automatiquement.

- Ne pas noter le mot de passe par écrit, mais si c'est nécessaire , ne pas le mettre sur une note bien en vue sur l'ordinateur.

5.1.4. Le cryptage : une arme contre le piratage informatique

La protection par simple mot de passe n'est quelques fois pas suffisante. Pour éviter les risques d'insécurité informatique, établir des barrières de sécurité et combattre les dangers, les experts estiment qu'un meilleur moyen est vraiment efficace : le cryptage[36] Cette opération consiste à rendre les fichiers informatiques d'un utilisateur illisibles pour un autre utilisateur.

Le cryptage est le processus qui consiste à coder un message de façon à ce que seules les personnes en possession de la clé de décryptage puissent le lire. L'armée et les banques sont, pour des raisons évidentes, les utilisateurs les plus assidus du cryptage. Le cryptage est également utile pour protéger les informations privées ou confidentielles contenues sur l'ordinateur ou sur le système. Avec le cryptage les fichiers ne pourront pas être lus directement, même si quelqu'un contourne les contrôles de sécurité et parvient à voir les fichiers.

Les experts cryptologie définissent le sujet comme le processus de prendre du « texte simple » et de le coder en « texte chiffré ». Le décryptage est l'opération inverse : transformer du « texte chiffré » en « texte simple ».Le texte simple est comme son nom l'indique le texte original, également appelé « texte clair » parce qu'il est transmis en clair ; et le texte chiffré ne suit aucune logique apparente.

Le texte simple est codé en texte chiffré soit en transposant ou en changeant l'ordre des caractères du texte simple, soit en substituant des caractères chiffrés ou des symboles aux caractères du texte simple. une formule, ou algorithme, est utilisée pour coder le message, généralement en traduisant les messages en une série de chiffre.

[36]. Sur la cryptographie, Philip ZIMMERMANN, Cryptographie et réseau, *Pour la science*, juin 1999.

Deux type de base de schémas de cryptage sont utilisés dans des produits disponibles auprès du public : symétriques et asymétriques. Avec le cryptage symétrique, une clé est utilisée pour coder et décoder les messages. Avec le cryptage asymétrique (appelé aussi cryptage à clé publique), deux clés dont utilisées, l'une (clé publique) pour coder, et l'autre (clé privé) pour décoder les messages. Par exemple : Jean veut envoyer un message confidentiel à Paul, il utilise la clé publique de Paul, pour crypter son message. Ensuite Paul utilise sa clé privée pour le décrypter. Une fois que les messages sont codés, il n'y a que la personne ayant la clé privée correspondante, qui puissent les lire. Même la personne qui écrit le message ne peut le lire une fois qu'il a été crypté avec la clé publique de son destinataire. Les programmes de cryptage les plus avancés actuellement sont asymétriques.

Mais le cryptage est tellement redoutable que la plupart des gouvernements réglementent son emploi pour des applications civiles et, dans certains cas- les Etats-Unis-, contrôlaient les exportations de produits cryptés. Redoutant que les criminels ne la détournent à leur profit, ils souhaitaient être les seuls à en conserver l'usage pour des raisons policières et militaires. Mais en fait, les produits de cryptage sont largement disponible à l'étranger, parce que de nombreuses sociétés européennes fabriquent des produits de cryptage. Restreindre les exportations ne fait que freiner la compétition et donner l'avantage aux autres.

Avant le milieu des années 1970, l'Agence de sécurité américaine (NSA pour National Security Agency) avait le quasi-monopole de la cryptographie américaine ; les méthodes étaient confidentielles, connues seulement de quelques « hommes de chiffre ». En 1976, un article intitulé De nouvelles voies pour la cryptographie, a ouvert la cryptographie au monde de la recherche. Le développement du réseau Internet et le souci de confidentialité de ses utilisateurs ont intensifié les études de cryptographie civile. Aujourd'hui, les meilleurs algorithmes de chiffrement et les meilleurs systèmes cryptographiques sont mis au point hors de la communauté militaire[37].

Actuellement les systèmes de cryptage en usage les plus courants sont DES, PGP et RSA. Le DES est un dispositif de cryptage élaboré par IBM et officiellement approuvé par le gouvernement des Etas-Unis. Il est un système à une clé (symétrique). C'est le standard de cryptage numéro un depuis 1977, et aussi une Norme de cryptage des données. DES n'a jamais été pénétrée, bien que de nombreuses personnes aient essayé . Plusieurs programmes complets de contrôle d'accès utilisent le **Data Encryption Standard** (DES), le **Triple DES**, ou d'autre cryptages aussi sûrs.

Ces programmes peuvent également crypter les mots de passe afin qu'ils ne puissent pas être utilisés au cas où ils seraient interceptés lors d'une transmission sur réseau. Quelle que soit l'intelligence pour créer un mot de passe, si on le transmette sur un réseau, il peut être intercepté par un « renifleur », un analyseur de réseau, ou tout autre outil conçus pour dépanner les réseaux. Les renifleurs et autres programmes de ce type

[37]. Ronald Rivest, Pour la libération de la cryptographie, *pour la science* juin 1999.

peuvent aussi être utilisés pour collecter des mots de passe quand les utilisateurs se connectent sur le système. Donc crypter les mots de passe avant de les transmettre limite les conséquences s'ils sont interceptés.

5.1.5. L'installation d'une paroi antifeu (*firewall*)

La paroi antifeu , en anglais *firewall* fournit une protection digitale associée à la rapide croissance des réseaux et de la commercialisation de l'Internet. Beaucoup de gens ont entendu parler des *firewalls,* mais peu de personnes les utilisent. De plus, le nombre d'incidents de sécurité grandissant sur Internet laisse suggérer très fortement que trop peu de personnes les utilisent correctement.

La paroi antifeu est une sorte de technologie de contrôle d'accès qui empêche les accès non autorisés aux ressources d'information en plaçant une barrière entre le réseau de l'entreprise et le réseau non-sécurisé (Internet , par exemple). Une paroi antifeu est aussi utilisé pour empêcher les transferts d'information propriétaire du réseau de l'entreprise. ces caractéristiques principales sont d'isoler un réseau d'Internet et de se comporter comme un gardien, surveillant le débit de données entrant et sortant du système. En d'autres mots, une paroi antifeu fonctionne comme une passerelle contrôlant le trafic dans les deux directions.

les parois antifeu les plus courantes sont , par ordre d'efficacité croissante : les routeurs de filtrage de paquets, les portes aux niveau des applications, et les portes au niveau des circuits.

Comme toute solution technique, la paroi antifeu donne une impression de sécurité et établit un climat de confiance propice aux inattentions. Une vigilance constante est nécessaire.

5.2. Eradiquer les virus informatiques

Il y a toutes sortes de programmes informatiques capables de détruire des données ou des systèmes : les virus, les Chevaux de Troie, les bombes logiques, etc. Il ne faut pas les sous-estimer.

5.2.1. Le mécanisme des virus informatiques

Les virus informatiques sont des programmes qui peuvent infecter d'autres programmes en les modifiant par insertion d'une version d'eux-mêmes. Ils s'accrochent sur les programmes comme des sangsues et se reproduisent très vite . Tout virus comprend trois parties de base : un mécanisme qui lui permet d'avancer et de se multiplier, un déclencheur qui lui permet de s'activer, et une cargaison, parfois inoffensive, mais pas toujours.

Les virus ne sont pas des programmes au sens qu'ils sont capables de faire des choses d'eux-mêmes comme les vrais programmes, les virus informatiques travaillent de la même manière que leurs homologues biologiques, par exemple, le virus de la grippe a besoin d'un hôte (les cellules de corps) pour se développer. Il en va de même pour les virus informatiques : il leur faut un hôte, en l'occurrence un programme, pour commettre leurs dégâts.

Les experts en virus estimaient en 1997 qu'il existait près de 6500 virus et que chaque jour il en apparaissait deux ou trois. Typiquement, les virus se clonent en s'attaquant au programme qu'ils utilisent comme des rampes de lancement pour se reproduire. Certains virus comme des parasites s'accrochent à des fichiers ayant une extension en **.EXE** , **.SYS** ou **.COM** ; certains virus attaquent le secteur *boot* (contenant les instuction de démarrage d'un PC) d'un disque dur ou d'une disquette. Certains virus nommés « virus multiples » attaquent à la fois les fichiers et le secteur *boot*. Mais la plupart des virus entrent dans une de ces deux catégories : ceux qui infectent les fichiers, et ceux qui infectent le secteur *boot* d'un disque dur.

Les rédacteurs de virus et les créateurs de logiciels antivirus sont enfermés dans une version d'espion contre espion. A chaque virus créé il convient de trouver une manière de l'exterminer. Les virus et les méthodes pour les détecter et s'en débarrasser deviennent de plus en plus élaborées. Les scanners représentent le type courant de logiciel antivirus. Les virus ont une série de codes uniques qui peut être utilisée pour identifier tout nouveau virus, ainsi les scanners sont conçus pour rechercher les signatures des virus , mais les rédacteurs de virus ont concocter deux types de virus particulièrement insidieux, car ils sont tout deux conçus pour échapper à la détection des scanners, et qui donnent du fil à retordre aux créateurs de logiciels antivirus. Le premier est le virus furtif qui dissimule ses traces au fur et à mesure qu'il se déplace, infectant un programme un après l'autre. Normalement les virus s'accrochent aux programmes et

changent la taille de leurs fichiers, mais une forme du virus intercepte les tentatives effectuées par les programmes antivirus de détection des changement de taille des fichiers et renvoie au scanner la taille originale du fichier de façon à ce que le fichier apparaisse sain. Une autre catégorie désactive totalement les scanners de virus de façon à ce qu'ils ne fonctionnent plus. La seconde est le virus polymorphe, plutôt que de faire des clones identiques à lui-même, ce type de virus peut produire des copies toutes un peu différentes ; une autre brouille ses codes de façon à rendre l'identification plus difficile. Donc les scanners de virus peuvent détecter quelques variantes de chacun de ces cas, mais certainement pas toutes.

La manière la plus fréquente dont les virus pénètrent dans les PC est par l'intermédiaire d'une disquette, mais il est également possible de télécharger un programme contenant un virus, à partir d'un BBS ou même d'un serveur commercial connu. Ce qui se produit généralement est qu'un des programmes sur la disquette a été infecté, la disquette est insérée dans le PC , le programme infecté est ouvert, et le virus peut alors infecter les programmes qui résident sur le disque dur du PC, même une disquette vierge peut aussi contenir un virus. Tout disque qui a été correctement formaté contient un programme exécutable dans le secteur *boot, là où* il y a un programme exécutable, il peut y avoir un virus.

D'où proviennent les noms de virus « Joshi », « 4096 », « Jesusalem », « WIN95 », « Spanska », « Happy99 » ? Les noms de virus ont été attribués en fonction de l'endroit où ils ont été découverts ; de la date à la quelle ils sont programmés pour se déclencher ; d'une ligne de code du virus suggérant son objectif ; du message qu'ils délivrent ; de ce qu'ils font. Il n'y a aucune convention pour donner un nom. Ainsi lorsqu'on utilise un logiciel antivirus, il se peut que deux vendeurs différents aient attribué deux noms différents.

5.2.2. Les signes révélant le virus

Les rédacteurs de virus veulent que leurs créations soit diffusées le plus largement possible avant d'être identifiées. Par conséquent , il se peut que l'ordinateur ait déjà été infectée depuis longtemps avant qu'on puisse s' apercevoir qu'un code malfaisant a envahi la machine.

S'il arrive que les choses étranges se produisent, quand on est en train de taper sur le clavier, la première chose qu'on doit faire est de vérifier que le système ne contient pas de virus. Voici des signes révélant la présence d'un virus.

- La taille des programmes augmente de manière sensible, sans qu'on ait fait quoi que ce soit pour les changer.

- Il faut plus de temps que d'habitude pour charger et faire tourner les programmes, ou ils refusent tout simplement de fonctionner.

- Le disque dur ou la disquette se met à tourner, alors qu'on n'a pas touché au clavier depuis un moment.
- On n'a plus autant d'espace sur le disque dur, ni de mémoire qu'on avait auparavant.
- Des messages d'erreurs inattendus s'affichent sur l'écran, ou tout au moins plus souvent que d'habitude.
- Des événements inhabituels apparaissent sur l'écran, comme une balle de ping-pong qui rebondit, un message sans rapport avec les tâches en cours s'affiche....
- On ne peut pas imprimer.
- l'ordinateur *reboot* sans raison.

Donc quand de tels signes appairaient il faut surveiller l'ordinateur, regarder s'il y a des changement de configuration, et analyser les fichiers présents sur le système d'exploitation afin de détecter la présence éventuelle de virus.

5.2.3. Les antidotes aux virus

La seule manière d'être sûr qu'un virus est la cause des problèmes passe par l'utilisation d'un logiciel antivirus. En général il y a quatre procédés qui permettent la détection et l'éradication des virus: le scanner, le détecteur de changement des fichiers, le détecteur d'activité des virus, et le désinfectant. La plupart des logiciels antivirus vendus offrent une combinaison de ces procédés.

5.2.3.1. Le scanner

Les scanners sont conçus pour regarder dans les fichiers, les secteurs *boot,* et autres endroits où les virus sont connus pour dissimuler les séries de codes ou signatures propres à chaque virus. Certains scanners peuvent ramasser ces signatures même si le fichier contenant le virus a été compressé.

L'avantage des scanners est qu'ils sont capables de dire exactement à l'utilisateur quel virus a envahi le système généralement avant que le virus ait la possibilité de livrer sa cargaison.

L'inconvénient est que si le virus est inconnu, le scanner n'aura pas dans ces archives les codes numériques typiques du virus permettant de l'identifier. L'autre problème est que un scanner ne peut pas facilement détecter les virus polymorphes. Parce qu'ils passent leur temps à contrefaire leur signatures ; Pour contourner ce problème, les créateurs des logiciels antivirus sont en train de développer des scanners qui utilisent

l'heuristique, une sorte d'intelligence artificielle pour détecter le virus polymorphes. Un autre problème est que de nos jours ,bon nombre de logiciels sont compressés afin de faire entrer les gros programmes sur de petites disquettes, si le programme est infecté avant d 'être compressé, il se peut que le scanner ne détecte pas le virus.

5.2.3.2. Le détecteur de changement des fichiers

Le détecteur de changement des fichiers prend un instantané du contenu des fichier à l'aide soit de la *checksum* unique ou des caractère de vérification par redondance dans le code de fichier. Le détecteur vérifie périodiquement si le *checksum* ou la *CRC* a changé, ce qui indiquerait qu'un virus s'est probablement accroché au fichier. Le détecteur de changement des fichiers a pour rayon d'action le disque entier et il vérifie chaque programme lors du chargement de celui-ci ou juste les fichiers qu'on a spécialisés.

L'avantage du détecteur de changements des fichiers est qu'il peut être utilisé pour révéler la présence de virus inconnus.

5.2.3.3. Le détecteur d'activité de virus

Les détecteurs d'activité de virus permettent de signaler la présence d'un virus en activité.. Ces détecteurs restent en mémoire après exécution , ce qui signifie qu'ils résident en mémoire et vérifient les fichiers avant qu'ils ne soient ouverts et alertent immédiatement l'utilisateur quand des fichiers exécutables sont modifiés. Les détecteurs d'activités de virus ne sont pas forcément très efficace contre les virus inconnus. .

5.2.3.4. Le destructeur de virus

Malgré toutes les précautions, un virus parvient quand même à pénétrer dans l'ordinateur et à l'infecter, à ce moment il est obligé d'utiliser des destructeurs de virus.

Le destructeur détecte tous les virus connus, ils répare aussi les fichier infectés. Mais le destructeur n'agit que les virus connus, pas les inconnus. Il est donc nécessaire de mettre à jour régulièrement son logiciel antivirus afin de pouvoir bénéficier de fonctionnalité applicables à un large spectre de virus.

6. La prévention et la répression juridiques

Les solutions techniques ne sont pas une solution universelle aux problèmes de sécurité informatique. Les mots de passe, les logiciels et le chiffrement ne sont qu'une solution ponctuelle pour un certain type de problèmes mais ne permettent pas d'établir un plan global de sécurisation. Cela revient à mettre une porte blindée sur une cabine en bois. Donc il est indispensable de renforcer les mesures judiciaires, dans ce domaine.

6.1. Des approches mondiales contre la criminalité informatique

6.1.1. Le droit pénal national face à la nouvelle criminalité

Le débuts de la protection pénale des informations (criminal information law) qui ont fait l'objet de recherches plus détaillés ces derniers temps, trouvent leur origine dans les années 1960[38], quand les premiers exposés concernant la dite « délinquance informatique » ont été débattus dans la presse et dans la littérature scientifique. Ces cas traitaient pour la plupart de la manipulation d'ordinateurs. Etant donné que beaucoup de ces exposés se fondaient notamment sur des rapports de presse, il était très difficile de savoir si le nouveau phénomène de la criminalité informatique était du domaine de la « réalité ».

A partir du milieu des années 1970, de sérieuses recherches scientifiques et criminologiques ont été faites. A la suite de ces recherches une quantité restreinte des délits informatiques pouvaient être prouvés mais en même temps, apparaissait un chiffre noir important de délits.

Dans les années 1980, la conception publique et scientifique de la criminalité informatique a profondément changé. Il est alors apparu pour la première fois que non seulement le domaine de la criminalité économique était affecté par la criminalité informatique, mais qu'il y avait aussi des atteintes à d'autres biens comme par exemple la manipulation d'un ordinateur dans un hôpital ou des violations des droits de la vie privée d'une personne à l'aide d'un ordinateur. Du fait de la vaste diffusion du piratage de logiciels, de la manipulation des guichets automatiques bancaires et de l'abus des systèmes de télécommunication, qui en outre rendaient publique la vulnérabilité d'une société d'information, il paraissait indispensable de créer de nouvelles stratégie de contrôle de la sécurité dans le domaine de l'informatique et de sa prévention criminelle.

Pour faire face à cette nouvelle forme de délinquance, un arsenal pénal étatique a été développé, principalement dans les pays industrialisés, et a été peu à peu ajusté.

[38]. Dr. Ulrich Sieber, Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique : Commentaire et questions préparatoires pour le colloque de l'AIDP à Wurzbourg publié *dans revue internationale de droit pénal*, vol 64, n°1-2,1993.

Pendant ces dernières décennies, l'évolution d'une société industrielle vers une société post industrielle, la valeur croissante des informations pour l'économie, la société et la politique, ainsi que l'importance grandissante de l'informatique ont mené à de nouvelles exigences, celles pour le droit pénal de créer un « droit pénal de l'information ». Le résultat d'un changement de paradigme des objets corporels en objets incoporels a atteint le droit pénal en plusieurs « vagues » de révision du droit Code pénal.

Dans plusieurs ordres juridiques occidentaux, la première vague de révision des années 1970-1980 a concerné la protection de la vie privée. Cette législation au début de ces années fut une réaction aux nouvelles menaces de l'intimité, qui a été causée par les nouvelles possibilités de collecter, stocker et transférer des données au moyen de l'informatique.

Une seconde vague de révision du droit pénal, à partir des années 1980, résulte de la lutte contre la délinquance économique spécifique à l'informatique. Ces amendements législatifs devenaient nécessaires parce que les nouvelles formes de la délinquances informatique portaient atteinte non seulement aux biens qui étaient protégés jusqu'ici par le droit pénal, mais aussi à des biens immatériels (comme les programmes informatiques) et parce que de nouvelles méthodes de perpétration de l'infraction (par exemple : la manipulation d'ordinateurs au lieu d'escroquer une personne) ont été employées. Au lieu d'étendre excessivement la définition des éléments constitutifs de l'infraction, beaucoup d'Etats ont adopté des lois de lutte contre la criminalité économique spécifiquement informatique.

Au cours des années 1980, une troisième vague d'amendements législatifs a amélioré la sauvegarde de la propriété intellectuelle dans le domaine de l'informatique. Plusieurs Etats ont promulgué des lois garantissant la protection du droit d'auteur sur les programmes informatiques. En même temps, les peines concernant les délits contre le droit d'auteur ont été durcies dans plusieurs ordres juridiques. Depuis 1984 beaucoup d'Etats adoptaient des lois de protection des produits semi-conducteurs

Actuellement, une quatrième vague de réformes législatives est en train d'introduire des innovations dans le domaine du droit procédural. Ces nouvelles dispositions répondent aux nouvelles nécessités de la police judiciaire pour les enquêtes dans le domaine de la criminalité informatique.

La Suisse est l'un des premiers pays d'Europe à avoir introduit dans sa législation pénale une disposition particulière concernant les virus informatiques[39]. Depuis 1er janvier 1995 , le code pénal suisse s'est doté d'une disposition spéciale contre les virus informatiques. Utilisation de virus informatiques dans le but de détériorer des données est désormais passible de sanctions pénales. Mais selon cette disposition, il est aussi devenu illégal de fabriquer, d'offrir, d'importer, de mettre en circulation, de promouvoir ou de rendre accessibles des logiciels conçus pour détériorer des données, et de fournir des indications en vue de leur fabrication.

[39]. Cf. Claudio G. FRIGERIO, la nouvel article du code pénal suisse sur les virus informatiques, Revue internationale de police criminelle, n°464, 1997.

Ces dernières années, des services de police spécialisés dans la lutte contre la criminalité informatique ou des services équivalants ont été créés dans de nombreux pays. Tel que aux USA, au Royaume Unis, à la France, à l'Australie, au Japon et en Chine.

6.1.2. L'harmonisation et la coopération internationale

La nécessité d'une étroite harmonisation internationale dans ce domaine résulte surtout de la grande mobilité des informations dans les systèmes informatiques. Cette mobilité des données rend possible la perpétration d'une infraction au moyen d'un ordinateur dans un pays pendant que le succès de cet acte criminel se réalise dans un autre pays. Ainsi de tels délits demandent une coopération internationale effective qui est aussi essentielle pour une protection effective des systèmes de télécommunication traversant plusieurs pays. L'exportation des programmes informatiques à l'étranger justifie aussi la nécessité d'une réglementation juridique internationale.

L'harmonisation internationale dans le droit de l'information a jusqu'à aujourd'hui acquis un haut niveau, grâce aux initiatives de diverses organisations internationales dont le Conseil de l'Europe, l'Organisation de Coopération et de Développement Economique (OCDE) et les Nations Unies[40] qui ont cherché à fournir des remèdes à ce phénomène sur le plan international. Les organisations susmentionnées ont surtout beaucoup contribué au haut standard d'harmonisation dans le domaine de la protection de la vie privée par le droit public et le droit civil ainsi que dans celui des dispositions pénales contre la délinquance informatique. Le nombre de leurs réalisations dans ce domaine(études, rapports, mais aussi instruments internationaux) leur font honneur.

De nombreux groupes d'experts ont fourni d'importantes contributions en la matière, notamment le Groupe d'Experts du Conseil de l'Europe sur la criminalité informatique, qui a dressé dès 1989 deux listes d'infractions informatiques : une Liste minimale des infractions qui devrait être adoptée par tous les pays européens, et une Liste facultative d'infractions à examiner. Les travaux de ce groupe ont donné lieu le 11 septembre 1995 à une Recommandation du Comité des ministres du Conseil de l'Europe. Cette Recommandation a identifié les principes de la lutte efficace contre la criminalité informatique.

Réunis à Washington en décembre 1997, les ministres de l'intérieur et de la justice des sept pays les plus industrialisés ainsi que de la Russie ont adopté un plan d'action contre la criminalité informatique. le plan adopté prévoit, notamment , la révision des textes répressifs, la formation de personnels spécialisés, un renforcement de la coopération avec les industriels. Les pays G8 partageaient une même certitude : face à la montée de la criminalité transnationale engendrée par le développement rapide des nouvelles technologies de la communication, telles Internet, la téléphonie cellulaire ou satellitaire,

[40]. Nations Unies a publié un manuel des Nations Unies sur la prévention et la répression de la criminalité informatique, dans *Revue internationale de politique criminelle*, n°43/44, 1994.

une coopération internationale est indispensable. Ce plan d'action [41]est censé apporter une première réponse au défi de la criminalité informatique. Parce que les criminels qui s'attaquent ou se servent des systèmes informatiques se moquent des frontières, que leurs méfaits s'accomplissent en quelques secondes, souvent sans laisser de traces, les Etats sont désarmés pour trouver la parade.

Le sujet a encore une fois été évoqué par Bill Clinton au sommet du G8 de Birmingham en juin 1998. Et le programme contre le crime informatique a été évolués lors du sommet. Un groupe de travail, composé de hauts responsables policiers est réuni le 24 juin 1998 à Rome, pour tenter de définir une stratégie mondiale de défense contre la délinquance de haute technologie, car pour l'instant, les réponses restent trop souvent nationales.

La politique d'interception légale de communication internationale sur Internet a été décidées le 17 janvier 1995 par la résolution du Conseil de l'Union européenne. Cette politique a élargi le cadre juridique en ce qui concerne les interceptions de correspondances émises par la voie des télécommunications. L'enquêteur disposait alors du cadre juridique nécessaire à ces investigations. L'interception de communications sur Internet peut servir à rassembler des informations criminelles entretiennent les unes avec les autres.

L'interception sur Internet a déjà été réalisée par la police judiciaire, avec des résultats prometteurs comme par exemple le démantèlement d'un réseau de pédophilie par une section de recherches en décembre 1997.

6.2. Interpol et la criminalité informatique

Interpol travaille depuis plus de 13 ans dans le domaine de la criminalité informatique. Le dossier le plus ancien remonte à février 1985[42]. les archives criminelles d'Interpol témoignent de l'existence, dès 1995, de nombreux dossiers de détournements de fonds par des moyens informatiques, de contrefaçons de cartes de crédit, de piratage téléphonique, etc., et fournissent la description des modus operandi de ces infractions[43]. Les statistiques des pays membres d'Interpol font état d'une augmentation considérable du nombre global des crimes informatiques. La criminalité informatique est un phénomène mondial, qui requiert une approche internationale ,donc il est nécessaire de coopérer sur le plan international entre les services de préventions de répression, les échanges d'information, l'utilisation des méthodes et de procédures uniformes lors des enquêtes , la conception et l'organisation de formations spécifiques.

[41]. L. ZECCHINI, les ministres du G8 adoptent un plan d'action contre la criminalité informatique, *Le Monde*, 12 décembre 1997.
[42]. Wolfgang SCHREIBER, la délinquance assistée par ordinateur publié dans *Revue internationale de police criminelle*, n°464, 1997.
[43]. Souheil EL ZEIN, précité.

6.2.1. La constitution du Groupe de travail d'Interpol

Les bureaux centraux nationaux européens d'Interpol ont pris en compte les évolutions et pris des mesures appropriées dans le domaine de la criminalité informatique. Ainsi, en mars 1990, La 19ème Conférence régionale européenne d'Interpol qui s'est tenue à Budapest a demandé au Comité technique sur la coopération en Europe d'étudier la criminalité informatique et la contamination des systèmes informatiques et de créer un groupe de travail européen au Secrétariat général d'Interpol.

En janvier 1991, ce groupe de travail européen sur la criminalité informatique a été constitué. Il s'agit d'un groupe d'experts composé d'un représentant du Secrétariat général et de spécialistes venant de huit pays européens (l'Allemagne, la Belgique, la Finlande, la France, l'Espagne, l'Italie, les Pays-Bas , le Royaume -Unis et la Suède).

Le Groupe de travail européen sur la criminalité informatique s'est réuni pour la première fois au Secrétariat général à Lyon en janvier 1991. Trois sous-groupes ont été constitués pour examiner certains aspects de la criminalité informatique et trouver des solutions aux problèmes rencontrés. L'un de ces sous-groupes s'occupe entre autres des questions relatives au piratage, notamment les dispositions législatives et la jurisprudence en matière.

Depuis janvier 1990, ce groupe de travail s'est réuni trois fois par an. Il s'est efforcé de trouver des solutions concrètes aux problèmes liés à l'utilisation des ordinateurs à des fins illicites, tant au niveau national qu'au niveau international. Les travaux du groupe portent essentiellement sur les aspects répressifs, mais aussi sur la prévention, la formation et les aspects administratifs.

Depuis sa création, le groupe de travail sur la criminalité informatique a élaboré un message type « criminalité informatique » distribué aux bureaux centraux nationaux (BCN) d'Interpol dans le monde entier, afin de faciliter l'échange d'informations en ce domaine, a rédigé un manuel relatif à la criminalité informatique recensant les diverses infractions et indiquant les moyens d'identifier leurs auteurs. Ce groupes a organisé aussi de cours de formation sur la criminalité informatique.

La création des groupes de travail régionaux sur la criminalité informatique sur le modèle du groupe de travail européen existant et d'un comité directeur composé de membres des groupes de travail régionaux a été discutée en avril 1995, lors de la 1ère Conférence internationale sur la criminalité informatique et recommandée en octobre 1995 par l'Assemblée générale d'Interpol lors de sa 64e session. En 1996, Ces groupes de travail régionaux ont été constitués et à la fin de l'année 1996, un comité directeur s'est réuni à Lyon.

6.2.2. Message « criminalité informatique »

La criminalité informatique requiert des connaissances spécialisées de haut niveau et nécessite l'emploi d'une technologie complexe. Les malfaiteurs utilisent de plus en plus les équipements de télécommunications les plus récents : les effets du piratage informatique et les virus peuvent se propager sur les réseaux à la vitesse de la lumière, et il est possible de commettre une infraction des milliers de kilomètres en une fraction de seconde. C'est pourquoi les informations concernant ce type d'infractions doivent circuler tout aussi rapidement, afin d'éviter que d'autres préjudices soient causés, ou de permettre que des mesures soient prises immédiatement.

Compte tenu de tous ces éléments, il importe d'améliorer l'échange d'informations dans le cadre d'Interpol en mettant au point un système de transmission rapide. Donc le Secrétariat Général d'Interpol a élaboré en collaboration avec le groupe de travail un message type « criminalité informatique » normalisé[44]. Il s'agit d'un « canevas » destiné à aider les bureaux centraux nationaux d'Interpol du monde entier à vérifier qu'ils ont bien communiqué tous les éléments nécessaires ou souhaitables lorsqu'ils transmettent ou demandent des informations concernant des infractions liées à l'informatique.

Le message « Criminalité informatique » a été expérimenté par les membres du groupe de travail pendant deux ans, au cours desquels il a démontré son efficacité. Compte tenu des résultats, le Secrétariat général d'Intepol a demandé de présenter le message type à tous les pays membres d'Interpol en 1996. Il leur a vivement recommandé de l'utiliser pour communiquer ou demander des informations sur la criminalité informatique.

6.2.3. La Conférence Internationale sur la criminalité informatique

La criminalité informatique requiert des connaissances de haut niveau, nécessite l'emploi d'une technologie complexe et une spécialisation au sein des structures policières nationales. Celles-ci sont encore peu équipées pour s'occuper de ce nouveau monde sans frontières ou en décalage par rapport à lui .En complément de la coopération régionale et internationale habituelle et de l'échange quotidien d'information, il est indispensable d'organiser des réunions et des conférences internationales sur la criminalité informatique.

La 1ère Conférence internationale sur la criminalité informatique, organisée par le Secrétariat général d'Interpol, a eu lieu à Lyon les 19 et 20 avril 1995 . Plus de 125 délégués de quelque 50 pays y ont participé.

Des exposés ont été présentés sur les travaux et les réalisations du Groupe de travail européen sur la criminalité informatique, ainsi que sur divers problèmes juridiques ayant trait aux technologies de l'information, au piratage téléphonique, au piratage informatique, aux virus et aux différentes approches nationales du problème de la

[44]. Pour savoir le contenu de ce message type voir : la délinquance assistée par ordinateur de Wolfgang SCHREIBER publié dans *Revur internationale de police criminelle*, n°464,1997.

criminalité liée à l'informatique. Deux tables rondes ont permis de débattre des tendances et des problèmes actuels.

Les participants ont exprimé leur préoccupation quant à l'évolution rapide de la criminalité liée aux technologies de l'information, et ont reconnu la nécessité d'une action coordonnée pour lutter contre ce type de criminalité au niveau national et international. Ils ont rendu hommage à l'initiative européenne ainsi qu'à la contribution du Groupe de travail européen sur la criminalité informatique. Il a été proposé que le problème de la criminalité informatique soit traité de la même façon en Afrique, en Amérique et en Asie, ainsi que dans chaque Etat membre d'Interpol dans ces régions. En outre, il a été jugé opportun de mettre en place un comité directeur composé d'un petit nombre d'experts représentant les différentes régions, en vue de promouvoir et coordonner toutes les initiatives régionales et d'encourager l'adoption de méthodes d'enquête normalisées, définies d'un commun accord, dans le domaine de la criminalité informatique.

Le Secrétariat général d'Interpol a organisé les 9 et 10 mai 1996 la 2ème Conférence internationale sur la criminalité informatique, à laquelle ont assisté une centaine de personnes représentant des services répressifs et observateurs d'une quarantaine de pays, dont plus . Les exposés ont abordé entre autres les éléments de preuve de nature informatique, les initiatives régionales dans le domaine de la criminalité informatique, les escroqueries aux télécommunication, les réseaux à longue distance et la criminalité liée à l'informatique et à Internet.

La 3ème Conférence internationale sur la criminalité informatique s'est tenue du 1er au 3 septembre 1998 au Secrétariat général d'Interpol à Lyon. Elle a réuni 108 participants représentant 36 pays. Les exposés qui ont été présentés dans cette conférence concernent Les rapports d'activité des groupes de travail régionaux d'Interpol sur la criminalité liée aux technologies de l'information, les projets du Groupe de travail européen d'Interpol sur la criminalité informatique, les techniques et la politique en matière de chiffrement, la sécurité des paiements électronique, les techniques d'enquêtes nécessitant l'utilisation d'Internet et la coopération entre les services chargés de l'application de la loi.

Les participants à la 3ème Conférence internationale sur la criminalité informatique sont arrivés à l'approbation à l'unanimité de la recommandation suivante :

- De soutenir l'action des groupes de travail d'Interpol et du Comité directeur,
- De renforcer la coopération avec les autres organisations, nationales et internationales engagées dans la lutte contre la criminalité liée aux technologies de l'information,
- d'établir une coopération avec le secteur privé, par exemple avec le secteur bancaire, les laboratoires de police scientifique et les fournisseurs de services Internet, et de développer cette coopération,

- D'axer cette coopération sur l'obtention d'une efficacité maximum, en évitant les doubles emplois qui entraînent un gaspillage de compétences, de temps et de moyens en général.

Le principal résultat de la Conférence internationale sur la criminalité informatique a été la création de groupes de travail régionaux, sur le modèle du groupe de travail européen existant. Dans chacune des régions Interpol, un bureau central national s'est porté volontaire pour organiser une première réunion du groupe de travail de sa région vers le mois de septembre 1996. A la fin de l'année 1996, un comité directeur composé de membres des groupes de travail régionaux s'est réuni à Lyon pour échanger des expériences, développer et coordonner toute les initiatives régionales .

6.2.4. Les deux outils documentaire d'Interpol

Avec la multiplication des ordinateurs dans la société moderne, les fonctionnaires de police sont de plus en plus souvent confrontés à cette technologie dans l'exercice de leurs fonction. Il est de plus en plus courant que des malfaiteurs enregistrent des informations sur ordinateur, informations qui peuvent parfois servir d'éléments de preuve dans le cadre de poursuites judiciaires. Il est donc impératif que ces éléments soient préservés afin de pouvoir être présentés devant un tribunal pénal. La technologie informatique est un domaine dynamique en évolution constante, avec l'arrivée fréquente sur le marché de nouveaux ordinateurs et de différents systèmes. Cette situation est source de problèmes pour les services de répression, pour répondre aux questions, il convient d'examiner la pratique et les méthodes à adopter dans le domaine de la criminalité informatique.

Pour être en mesure d'enquêter dans cet environnement, les services de répression doivent disposer d'informations précises et à jour. Des données techniques de base et un cadre définissant des méthodes et des procédures éprouvées sont donc indispensables à l'efficacité et à la réussite de leurs actions. Dans ce contexte le Secrétariat général d'Interpol a publié deux ouvrages.

Le premier brochure c'est la Guide sur la criminalité informatique. Cette brochure, intitulée « Informatique et criminalité - Ordinateur et élément de preuve », est un guide général destiné à aider les fonctionnaires de police susceptibles de se trouver en présence d'ordinateurs au cours de leurs enquêtes. Elle a été diffusée à tous les Bureaux centraux nationaux d'Interpol. Dans cette brochure, on examine certaines pratiques et méthodes en rappelant quelque notions élémentaires d'informatique, en expliquant certains termes, en établissant une liste de règles à appliquer sur les lieux d'une infractions informatique.

A près le guide « Informatique et criminalité », qui fournit des informations de base sur l'informatique et la criminalité liée à l'informatique, le Secrétariat général a décidé de

publier un manuel plus élaboré sur la criminalité informatique intitulée « Interpol manual of standards and procedures - computers and crime », destiné aux spécialistes de la criminalité informatique et aux enquêteurs travaillant dans ce domaine. Ce manuel recensent les diverses infractions pouvant être commises et indiquant les moyens d'identifier leur auteurs. Il contient des informations plus détaillées sur la criminalité informatique, sa prévention, sa détection, la législation applicable et la formation. On y trouve aussi le message « Criminalité informatique » et la liste des points de contact centraux nationaux. Il comporte également des chapitres sur les technologies de l'information, les matériels techniques et les télécommunications. Ce manuel est constitué de feuillets mobiles. Il est d'abord diffusé à tous les Bureaux centraux nationaux européens, puis , par la suite ou sur demande, aux autres Bureaux centraux nationaux d'Interpol.

6.3. Le système informatique et les réseaux d'Interpol

La criminalité informatique est un phénomènes sans frontière, il est possible de commettre une infraction à des milliers de kilomètres en une fraction de seconde. Donc les informations concernant ce type d'infractions doivent circuler tout aussi rapidement, le réseau Interpol assure un haut niveau de rapidité et surtout, de sécurité.

Le fonctionnement du réseau d'Interpol est parfaitement illustré par la lutte contre la criminalité informatique. Compte tenu du caractère technique de la criminalité informatique du caractère technique de al criminalité informatique, des service spécialisés dans la lutte contre ce crime ont été créés dans de nombreux pays. Ils peuvent coopérer par le canal d'Interpol, ils peuvent coopérer avec les Bureaux Centraux Nationaux pour instituer une « autoroute centrale » afin de coordonner rapidement les demandes. Afin que les informations échangées par l'intermédiaire d'Interpol parviennent sans retard aux services spécialisés, Interpol a établi une liste de points de contact centraux nationaux pour la criminalité informatique. Ces points de contact sont particulièrement importants pour la mise en place d'un système d'alerte.

Assurer l'échange d'informations de façon permanente, rapide, fiable et sûr entre les Etats membres d'une part, et entre les Bureaux Centraux Nationaux et le Secrétariat général d'Interpol est un des objectifs fondamentaux assignés à Interpol. Ainsi Interpol dispose déjà d'un système moderne et très efficace de transmission rapide des informations.

Le réseau Interpol est un réseau fermé permettant l'échange de données informatisées entre le Secrétariat général d'Interpol et ses Bureaux centraux nationaux du monde entier. Ces informations se présente non seulement sous les formes de textes avec graphiques, schémas, tableaux, mais aussi sous les formes des images avec photographies , empreintes digitales et échantillons des faux billets.

6.3.1.L'architecture du Réseau d'Interpol

Interpol compte actuellement 177 pays membres qui présentent des degrés de développement technologique très diversifiés. Leurs besoins en matière de traitement et de communication des informations de police à caractère international sont très dissemblables.

le réseau de télécommunications d'Interpol est structuré en trois niveaux hiérarchiques :

- Premier niveau : Les Bureaux Centraux Nationaux. C'est l'interface entre les autorités de chaque pays et l'Organisation. Il y a 177 Bureaux Centraux Nationaux et 11 sous- bureaux.

- Deuxièmes niveau : Les stations régionales. Ces stations ont pour mission, d'une part d'assurer le trafic intrarégional entre les Bureaux Centraux Nationaux qui leur sont reliés et , d'autre part , de concentrer et de faire transiter le trafic entre la région et le reste du réseau de l'Organisation. Elles sont actuellement au nombre de sept : La station de Lyon (Secrétariat général d'Interpol) qui couvre zone Europe - Méditerranée / Amérique du Nord / Moyen- Orient ; La station de Nairobi qui couvre l'Afrique de l'Est ; La station d'Abidjan qui couvre l'Afrique de l'Ouest ; Ma station de Buenos Aires qui couvre l'Amérique du Sud ; la station de Tokyo qui couvre l'Asie ; la station de Porto Rico qui couvre les Caraïbes et Amérique Centrale et la station de Canberra qui couvre la région pacifique.

- Troisième niveau : la station centrale (au Secrétariat général d'Interpol). Elle assure les communications entre les régions à travers les stations régionales. En outre, la station centrale joue le rôle de station régionale pour la zone Europe - Méditerranée : Amérique du Nord / Moyen-Orient qui comprend 66 Bureaux Centraux Nationaux.

6.3.2. La situation actuelle du réseau d'Interpol

Le 31 décembre 1993, la station d'émission radio d'Interpol cessait d'émettre ; le commutateur automatique de messages du Secrétariat général, plus connu sous le nom d'AMSS, était arrêté ; puis le réseau de communication d'Interpol a fonctionné sur le réseau X-400. Cela signifie une nouvelle ère pour les télécommunications de police[45].

La norme X-400 est le standard international en matière de messagerie, défini par une série de recommandations du Comité consultatif international télégraphique et téléphonique (CCITT). Les offres de services de messagerie, tant publique que privé, se conforment de plus en plus à ce standard. Les administrations et la plupart des grands constructeurs offrent aujourd'hui des passerelles, des services ou des serveurs privés au standard X-400.

[45]. Dominic SUC, une nouvelle ère pour les télécommunications de police, *Revue internationale de police criminelle*, n°469, 1998.

Actuellement la plupart des pays européens et nord-américains ont mis en place des équipements X-400. Fin 1998, 162 pays étaient équipés ainsi que 7 stations régionales. l'intégralité du trafic transitant maintenant par le serveur X-400 du Secrétariat général d'Interpol.

Le plan de modernisation régionale prévoit d'équiper progressivement par régions entières 130 Bureaux Centraux Nationaux d'équipements X-400. Cette stratégie de grande envergure vise à aider les Bureaux Centraux Nationaux qui ne pourraient le faire rapidement à accéder à la nouvelle technologie et à avoir un égal niveau d'équipement dans toutes les régions du monde. En quelques minutes, un message pourra ainsi être retransmis dans le monde entier.

Ces projets s'appuieront sur le réseau mondial X-25 utilisé par les compagnies aériennes (SITA). La présence de cet opérateur dans tous les pays permettra aussi une maintenance et un support locaux très importants.

6.3.3. Le système ASF (Automated Search Facility)

Le système ASF est un système téléinformatique qui permet aux Bureaux Centraux Nationaux d'Interpol du monde entier et aux services officiels ayant une mission de police d'effectuer des recherches de façon automatique et instantanée et à distance dans une base de données criminelles sélectionnées.

Cette base de données se trouve sur un serveur au Secrétariat général. tous les jours, les informations envoyées par les Bureaux Centraux nationaux sont introduites dans cette base de données, avec l'autorisation préalable du pays expéditeur.

La mise en service opérationnel de ce système a eu lieu au mois de juin 1992, actuellement les sources suivants sont disponibles dans cette base de données :

- fugitifs et suspects internationaux (en total 260,000 paronymes et environ 50, 000 images)

- oeuvres d'art volés avec image en couleur.

- véhicules volées (en total 10 million de véhicules)

Les recherches sur l'identité d'un suspect peuvent être effectuées en utilisant entre autres critères la phonétique et permettent l'accès à des informations de différents types, tels que nom, prénom, date de naissance, nationalité. On dispose de ses alias connus, ses passeports ou pièces d'identité.

Il est également possible d'obtenir le transfert de la photo et des empreintes de cet individu avec sa notice internationale en anglais, français, espagnol ou arabe.

Pour accéder au serveur ASF central, différentes lignes peuvent être utilisées, comme le réseau téléphonique, le réseau de commutation par paquets (type X.25) ou le réseau numérique à intégration de services .

L'ASF peut également faire l'objet de copies installées auprès de chaque Bureau Central National, ce qui favorise plus encore l'accès à l'information. Ces copies font l'objet de mises à jour, par vois électronique, sur une base régulière.

Avec la mise en place des équipements X-400, du système de chiffrement des communications, du système ASF, Interpol dispose des base de données nécessaires au développement d'un réseau mondial à la pointe des technologies et très complet , capable de transmettre les textes et images cryptés.

6.3.4. Les systèmes informatiques

L'informatisation du Secrétariat général d'Interpol a permis de créer l'assistance technique et professionnelle demandée par les Etats membres et nécessaires à la mise en place du système de recherche automatique (ASF) indispensable à la lutte contre la criminalité internationale dans les années 90.

La modernisation par l'apport et l'utilisation de technologies de pointe au Secrétariat général d'Interpol s'est traduite dans deux secteurs principaux :

- L'extension du système informatique de documentation criminelle d'Interpol (ICIS) dans le but d'améliorer les méthodes de stockage et de recherche des informations relatives aux infractions, de réduire aux maximum les délais de réponse aux Bureaux Centraux Nationaux, de doter la Division de Liaison et de l'Information criminelle d'un accès rapide aux données transmises par les Etats membres .

- La mise en place d'un système électronique de bureautique, de messagerie et d'archivage. Ce système permet notamment de travailler dans les quatre langues de l'Organisation et de faciliter la communication interne.

6.3.5. Le système ICIS (Interpol Criminal information Systèm)

Le système ICIS comprend les archives criminelles de l'Organisation. Cette base de données globale est installée au siège du Secrétariat général dInterpol et géré par le personnel du Secrétariat général. Conformément à la réglementation adoptée par l'Assemblée générale d'Interpol, aucune autorité ou personne extérieure au Secrétariat général ne peut accéder directement aux informations contenues dans la base ICIS. L'accès s'exerce par l'intermédiaire de fonctionnaires du Secrétariat général habilités à examiner les motifs de la demande d'accès.

l'objet essentiel de la base est en effet de recueillir des informations sur les biens ayant fait l'objet d'une infraction pénale et surtout, sur les personnes recherchées, sur la base d'un mandat d'arrêt ou d'une décision de condamnation exécutoire, en vue d'une extradition ultérieure.

6.3.6. L'archivage électronique

Au Secrétariat général, Interpol dispose de différents fichiers sur l'information criminelle. tous ces fichiers sont conservés sous la forme électronique. Ils comprennent :

- un fichier informatisé des noms et des alias des individus impliqués dans des infractions internationales.
- un fichier informatisé des infractions classées par type, lieu de perpétration et modus operandi (ICIS).
- un fichier informatisé des saisies de drogues (ICIS).
- un fichier informatisé des saisies de fausse monnaie (ICIS).
- un fichier informatisé des vols d'oeuvres d'art (ASF).
- un fichier informatisé des véhicules volées (ASF).
- un fichier informatisé des numéros d'identification relevés lors d'enquêtes de police (ICIS).
- un fichier décadactylaire qui contient une collection d'empreintes digitales de malfaiteurs internationaux classée selon le système de Galton-Henry et dont l'exploitation permet soit de découvrir l'identité d'un malfaiteur usant de plusieurs états civils, soit d'établir celle d'un cadavre ou bien d'une personne amnésique.
- un fichier photographique groupant les portraits de malfaiteurs spécialisés, de récidivistes ou de personnes disparues.

6.3.7. Les mesures de sécurité d'Interpol pour protéger son réseau

6.3.7.1. Le cryptage des communication

Il ne suffit pas pour Interpol d'échanger des messages de façon permanente, rapide et fiable ; il faut aussi les échanger de façon sûre.

Le réseau Interpol comprend de nombreux types d'équipements terminaux et des messageries qui seront fournies par des constructeurs différents. Les fonctions de base à assurer en matière de sécurité des échanges sont donc :

- L'authentification de l'expéditeur, afin qu'un tiers ne puisse pas se connecter sur le réseau et envoyer des messages perturbateurs.

- La sécurité de l'échange lui-même, pour assurer la non-interception ou la non-identification d'un message donné.

Le système de cryptage retenu est adapté à tous les équipements basés sur des micro-ordinateurs et permet le chiffrement de bout en bout des communications établies entre micro-ordinateurs équipés de logiciels X-400, ainsi que l'authentification de l'expéditeur par la signature électronique par carte à mémoire, tous cela sans entraîner de modification sur le serveur X-400. Ces options évitent notamment des modifications coûteuses au niveau de la station centrale et assurent une grande sécurité aux moyens de transmission de l'avenir .

6.3.7.2.Le réseau séparé Internet / Intranet

Le réseau Intepol est un réseau fermé permettant l'échange de données informatisées seulement entre le Secrétariat général d'Interpol et ses Bureaux centraux nationaux du monde entier. Le réseau du Secrétariat général est strictement séparé entre système intérieur et systèmes extérieur. Les ordinateurs mis en place du Secrétariat général n'autorisent pas les accès depuis l'extérieur. Seule la messagerie électronique X-400 exploitée par la Sous-direction des télécommunications permet la communication avec les Bureaux Centraux Nationaux. Cette Organisation ne met jamais en relation directe et de façon interactive des personnes extérieures au Secrétariat général avec leurs serveur .

6.3.7.3. Renouvellement régulièrement du mot de passe

Selon les règles de sécurité du Secrétariat général, les mots de passe des postes doivent être renouvelé régulièrement toutes les 4 semaines. Et il est formellement interdit de communiquer le mot de passe pour permettre à un tiers d'accéder à son compte en son absence.

6.3.7.4. La mise en place de l'alarme signalant toute tentative d'ouverture du boîtier de l'unité centrale

Il est formellement interdit d'ouvrir une station de travail pour y installer du matériel supplémentaire. une alarme est envoyée au Département Informatique signalant toute

tentative d'ouvrir l'unité central du poste. Même toute demande de déplacement de matériel, débranchement et /ou branchement de clavier, écran ou souris doit être transmise au Département Informatique qui coordonnera les actions avec les services concernés (service généraux ou télécommunications).

6.3.7.5. La désactivation des lecteurs de disquette

Afin de garantir une sécurité maximum des systèmes informatiques de l'Organisation, les lecteurs de disquette de toutes les stations de travail ont été désactivés. Cette mesure a pour objet de prémunir :

- **des virus informatiques** extrêmement populaires dans l'environnement micro-ordinateurs et dont la disquette est le vecteur principal, et ceci malgré l'installation de logiciel antivirus.

- **du piratage informatique** en introduisant au Secrétariat général des logiciels non référencés, non licenciés et non maintenus par l'équipe d'exploitation. Il est totalement exclu que tout un chacun puisse introduire dans son micro-ordinateur un logiciel non certifié. Le Département Informatique est capable à tout moment, grâce un logiciel de gestion de parc, de connaître quels sont les logiciels installés et cela sans avoir à se déplacer.

- **de la fuite d'informations** dont le Secrétariat général est propriétaire et/ou dépositaire. Le Secrétariat général prend les précautions nécessaires afin de préserver le secret et la sécurité des informations de police et d'empêcher que ces informations ne soient traitées ou communiquées d'une façon illicite ou abusive. Et les personnels du Secrétariat général sont tenus au secret professionnel.

Conclusions

Les problèmes qui sont évoqués travers la criminalité informatique sont loin d'avoir trouvé une solution. En guise de conclusions, j'essaies de mettre en valeur les éventuelles obstacles et difficultés que rencontrent les professionnels concernés dans la lutte contre la criminalité informatique et de soulever certaines questions. Mais je ne proposera pas ici d'interprétation ou de réponses.

Jusqu'à présent , dans la plupart des pays seuls les objets corporels et visibles sont protégés par les lois. Bien que la sauvegarde des informations et des autres biens immatériels existait aussi depuis quelques temps dans quelque pays, mais elle était moins importante. Cette situation a complètement changé pendant les dernières décennies : L'importance grandissante de l'informatique a, entre-temps , mené à de nouvelles exigences du droit pénal de l'information. Dans tous les pays, il manque une théorie générale de la protection pénale des informations. Et la nouvelle théorie de la protection pénale de l'information devrait donc être fondée sur le « droit de l'information et le droit de l'informatique » qui se développe actuellement dans quelques pays.

A l'exception de quelques pays, la plupart des pays ne disposent pas d'une loi spécifique sur les délits informatiques. A défaut de cette loi il faut donc cantonner ces délits dans la 'trame' du code pénal traditionnel, les poursuites en sont rendues très difficiles.

Le problème majeur que pose Internet est celui de savoir quel est le régime juridique applicable. Selon certains, Internet se trouve 'en état d'apesanteur ' au sein d'un vide juridique. Tout y est réalisable. La liberté y est la règle. Aucune contrainte, des contrôles difficiles à réaliser, étant donné notamment l'espace mondial dans le quel ce système se déploie, tout cela ne pouvant que générer des abus.

Une course de vitesse est donc engagée dans ce domaine. Mais les technologies progressent souvent plus vite que les cadres législatifs utilisables par les autorités chargées de l'application des lois. Et c'est dans ces vides juridiques que s'engouffrent les cybercriminels.

Il n'y pas d'impunité totale dans le cyberespace ; Mais les particularités de l'informatique et du réseau ont apporté d'indéniables atouts aux criminels informatiques : la fugacité extrême des contenus apparaissant et disparaissant à la vitesse électronique, la diffusion internationales des infractions, l'anonymat renforcé des criminels, ont placé les policiers et les magistrats devant des complications à la fois juridiques et pratiques.

La question la plus délicate du point de vue juridique est la compétence judiciaire. Le développement de l'interconnexion de banque de données grâce aux réseaux internationaux de télécommunications entraîne l'internationalisation de la criminalité informatiques, alors que les informations en elles-mêmes sont des données régies par le droit local. Ainsi, les flux d'information parcourent librement les réseaux informatiques qui ne connaissent pas les frontières alors que les autorités chargées de l'enquête sont, elles, strictement liées par leur compétence territoriale nationale et par le principe de souveraineté.

Plusieurs cas de figures peuvent se présenter. une personne peut, à partir d'un ordinateur situé dans un pays **A** manipuler un programme ou entrer dans une mémoire d'ordinateur dans un pays **B**, acte qui affectera les intérêts d'une personne située dans un pays **C**. Dès lors se pose la question de la compétence des tribunaux de ces divers pays et de l'application de leur droit national.

Des inquiétudes ont été ainsi soulevées relativement au type d'information diffusée sur Internet et à la capacité de la société de réglementer le réseau qui constitue à la fois un avantage et un inconvénient pour la police judiciaire. Quiconque souhaite diffuser des messages de haine ou des matériels pornographiques peut le faire impunément en établissant un site web dans un pays où les lois sont moins contraignantes. Par l'exemple un canadien peut télécharger des matériels pornographiques transmis depuis la Grande- Bretagne sur un ordinateur situé aux Etats - Unis, puis sur un autre ordinateur situé en Europe, où ce matériel peut être toléré par les lois. Dans un tel cas, la police canadienne pourrait demander l'aide des autorités judiciaires du pays concerné, mais cette aide pourrait lui être refusée, étant donné qu'aucune loi n'a été enfreinte ou parce que les autorités jugent que le sujet est sans importance dans leur pays.

Il existe entre les pays non seulement des différences d'ordre juridique, mais également des différences d'ordre pratique.

Un officier de police judiciaire française s'était bien posé une question[46]en interrogeant : « A l'occasion d'une perquisition au domicile d'un homme soupçonné de pédophilie, avons-nous le droit d'accéder au serveur, installé aux Etats-Unis, sur lequel cet homme soupçonné s'est connecté ? ». Vraiment la perquisition et les saisies transfrontières effectuées sur d'autres systèmes informatiques localisés à l'étranger sont une question controversée à cet égard. Les autorités chargées de l'enquête n'ont pas la possibilité légale d'accéder aux données contenues sur d'autres systèmes informatiques étrangers liés par Internet, car pour les Nations Unies de tels actes, par le biais des systèmes de télécommunication internationaux, portent atteinte à la souveraineté de l'Etat où les données sont stockées. Mais les auteurs de crimes informatiques stockent de plus en plus de données aux pays étrangers, afin d'entraver les poursuites.

[46]. voir « dossier délinquance » publié sur *Le Monde*, 22/09/1998.

Le désire de réduire les obstacles à la coopération internationale dans la domaine de la lutte contre la criminalité informatique a donné naissance à des structures et à des systèmes régionaux[47] et la multiplication des structures internationale et régionales suppose en effet une harmonisation des procédures, une normalisation de l'utilisation de la nouvelle technologie, particulièrement Interpol a établi une procédure rapide d'échange d'informations . Malgré cela , la procédure et les structures de la coopération internationale et régionales sont insuffisantes, et il s'avère urgent d'y remédier, à cet égard on a beaucoup plus d'obstacles à surmonter.

[47]. Par exemple, en 1995, le Conseil de l'Union européenne a prouvé une politique d'interception légale des télécommunications dans l'Union européen. L'enquêteur disposait alors du cadre juridique nécessaire à ses investigations.

Bibliographie

Ouvrages

ALEXANDER, M., *Le guide clandestin de la sécurité des ordinateurs*, Paris : International Thomson Publishing France, 1997, 244p., ISBN : 2-84180-962-5.

CHAMPY, G., *La fraude informatique: Tome I*, Aix-en-Provence : Presses Universitaires d'Aix-Marseille, 1992. - 370p., ISBN : 2-903089-31-4.

CHAMPY, G., *La fraude informatique: Tome II*, Aix-en-Provence : Presses Universitaires d'Aix-Marseille, 1992, p.372-820, ISBN : 2-903089-31-4.

CLOUGH, B., MUNGO P., *La délinquance assistée par ordinateur: la saga des hackers*, nouveaux flibustiers high tech, Paris : Dunod, 1993, 220p., ISBN : 2-10-002013-7

FOMBONNE, J., *La criminalistique*, Paris : Presses universitaires de France, 1996, 127p., (Que sais-je? ; 370), ISBN : 2-13-047630-9.

GUISNEL, J, *Guerres dans le cyberespace: services secrets et Internet*, Paris : La Découverte, 1995, 251p. (Enquêtes), ISBN : 2-7071-2502-4.

HRUSKA, J, *Virus informatiques et systèmes anti-virus*, Paris : Masson, 1992, 149p., ISBN : 2-225-82523-8.

LE DORAN, S. ROSE P., *Cyber thrillers: 35 histoires vraies de délinquance informatique*, Paris : Albin Michel, 1996, 349p., ISBN : 2-226-08530-0

MARTIN D., *La criminalite informatique*, Paris : Presses universitaires de France, 1997. - 196p., (Criminalite internationale), ISBN : 2-13-048488-3

MEILLAN, E., *La sécurité des systèmes d'information: les aspects juridiques*, Paris : Hermès, 1993, 204p. (Systèmes d'information), ISBN : 2-86601-358-1

ROSE P., *La criminalité informatique à l'horizon 2005: analyse prospective*, Paris : I.H.E.S.I., 1991, 153p.

Articles des Périodiques

NATIONS UNIES., Centre pour le développement social et les affaires humanitaires, *United Nations manual on the prevention and control of computer related crime= Manuel des Nations Unies sur la prévention et la répression de la criminalité* informatique, INTERNATIONAL REVIEW OF CRIMINAL POLICY = REVUE INTERNATIONALE DE POLITIQUE CRIMINELLE, No.43/44, 1994, 47p. = 52p.

O.C.D.E., Comité de la politique de l'information, de l'informatique et des communications / BRIAT M., SIEBER U, Computer related crime: Analyse of legal policy= *La fraude liée à l'informatique: analyse des politiques juridiques*, Paris: O.C.D.E., 1986, 70p. = 79p.

DELSOUC C., *La sécurité des données informatiques*, FACE AU RISQUE, No.270, 02/1991, pp.30-33

DEVEZE, J., *La fraude informatique: aspects juridiques*, LA SEMAINE JURIDIQUE, No.25, 1987, p.3289

FORD G.D., *Computer related crime = Les délits informatiques*, ROYAL CANADIAN MOUNTED POLICE GAZETTE = LA GAZETTE DE LA GENDARMERIE ROYALE DU CANADA, No.7/8, 1990, pp.19-21 = pp.19-21

FRIGERIO C.G., *Le nouvel article du code pénal suisse sur les virus informatiques*, REVUE INTERNATIONALE DE POLICE CRIMINELLE, Vol.51, No.464, 1997, pp.19-26.

HANNAFORD, C., *Crime on the information highway = La criminalité perpétrée sur l'autoroute de l'information.* - ROYAL CANADIAN MOUNTED POLICE GAZETTE = LA GAZETTE DE LA GENDARMERIE ROYALE DU CANADA, Vol.57, No.10, 10/1995, pp.22-24 = pp.22-24

HETIER L.G., *Fraudes, détournements, sabotages*, FACE AU RISQUE, No.260, 02/1990, pp.63-67.

SCHREIBER.W., *La délinquance assistée par ordinateur*, REVUE INTERNATIONALE DE POLICE CRIMINELLE, Vol.51, No.464, 1997, pp.9-14.

SZABO D., *Crime et justice en l'an 2000*, REVUE INTERNATIONALE DE CRIMINOLOGIE ET DE POLICE TECHNIQUE, Vol.44, No.3, 1991, pp.279-298.

VAN ACHTER M., *Les perquisitions sur le réseau*, VIGILES: REVUE DU DROIT DE POLICE, No.1, 03/1997, pp.41-44.

MARTIN,D., *Cyber-terrorisme : le nouveau péril*, POLITIQUE NTERNATIONALE, No.77, 09/1997, pp.299-312.

MCGOVERN, R., *La fraude aux télécommunications*, REVUE INTERNATIONALE DE POLICE CRIMINELLE, Vol.51, No.464, 1997. - pp.15-18

PADOIN, D. , *La police judiciaire contre les crimes sur les systèmes d'information = La policía judicial contra los delitos informáticos,* REVUE INTERNATIONALE DE POLICE CRIMINELLE, Vol.51, No.457, 1996, pp.5-8.

PRADEL J. , *Les infractions relatives à l'informatique*, REVUE INTERNATIONALE DE DROIT COMPARE, No.2, 1990. - pp.815-828

ROSSI M. , *Confidentialité de l'information*, FACE AU RISQUE, No.295, 08/1993, pp.79-85.

PRADEL, J., *Les infractions relatives à l'informatique*, REVUE INTERNATIONALE DE DROIT COMPARE, n° 2, 1990, pp.5-8.

ROSSI, M. , *Confidentialité de l'information*, FACE AU RISQUE, N°295,08/1993, pp.79-85.

SZABO, D., *Crime et justice en l'an 2000*, REVUE INTERNATIONALE DE CRIMINOLOGIE ET DE POLICE TECHNIQUE, vol.44,n°3, 1991, pp.279-298.

Signets de sites Internet

Liens directs

Cybercrimes :
http ://cybercrimes.net

QuickLinks - Computer crime :
http ://www.qlinks.net/quicklinks/comcrime.htm

Computer Crime and Intellectual Property Section :
http ://www.usdoj.gov/criminal/cybercrime/

Computer crimes Criminal Justice Links :

http ://www.co.pinellas.fl.us/bcc/juscoord/ecomputer.htm

R.E.C.IF.-Recherches et Etudes sur la Criminalité informatique Française
http ://worldserver4.oleane.com/recif/

Documents en ligne

Dossier Criminalité informatique : analyse de l'avant-projet de la loi belge :
http ://www.froit-technologi.org/5_3_1.asp

Lenny Stripeikis. Computers and Crime :
http ://www.academic.marist.edu/papers/lenny/crime.htm

Bulletin sur la criminalité technologique :
http ://www.rcmp-grc.gc.ca/html/te-crimfx.htm

INTRINsec - Revue de Presse sur la criminalité informatique :
http ://www.intinsec.com/presse.html

Les résultats de l'analyse réalisée par le FBI et CSI sur Computer crime and Security 1997 :
http ://www.tla.ch/TLA/NEWS/etude97.html

Index

A

Accès et interception non autorisés 22
adresse IP 38
agressifs 28
amateurs 27
AMSS 11; 58
antidotes de virus 47
antivirus 45; 47
archivage électronique 61
ARPANET 34
ASF 12; 61

B

B.C.N. 10
BBS 39
BCN 53
Bombe logique 34
boot 45; 46; 47
Bureau Central National 10

C

casseurs de systèmes 27
cheese box 31
chevaux de Troie 28
CMOS 41
compétence judiciaire 65
Conférence Internationale 54; 55
Contre façon informatique 23
coopération international 13
Cracker jack 39
Crak 4.1 40
crime organisé 27
Criminalité informatique 16
cryptage 42; 43; 62
CSI (Computer Security Institue), ... 20

D

Data Encryption Standard (DES) 43
DES 43
destructeurs 28

E

Excel 41

F

FAQ (Frequenly Asked Questions 39
FBI (Federal Bureau of Investigation) 20
firewalls 44
formes de criminalité informatique 22
Fraude informatique 23
Fraude informatique concernant les jeux 24
Fraude informatique liée aux moyens de paiement 24

G

genèse de la criminalité informatique 16
Groupe de travail 53

H

hacking 29
hacker 30; 39; 40

I

ICIS 61
Informatique et criminalité 56
Infraction kiosque télématique (B.B.S.) 25
Internet 17; 26; 29; 35; 37; 64
Interpol 9

M

Matériels délictueux 25
mémoire criminelle mondiale 12
Message « criminalité informatique 54
mesures de sécurité 61
Microsoft Word 41
minidictionnaires 39
Modification de logiciels ou de données 23
mot de passe 40
motivations 27

N

NASA 16
National Security Agency 43
newsgroups 35
notice bleue 12
notice jaune 12
notice rouge 12
notice verte 12
notice noir 12
NSA 43

O

OCDE 18; 51
OIPC 9

P

paroi antifeu 44
PC-DOS 40
pédophile 29; 35
perquisition 65
phreaker 39
phreaking 31
Piratage informatique 29; 31; 63
Piratage téléphonique 31
pirate 39

R

renifleur 43
répression juridiques 49
Reproduction illicite 24
réseau d'Interpol 58

S

Sabotage informatique 24
Sabotage logiciel informatique 25
Sabotage matériel informatique 24
Saint-Cloud 13
SATAN 40
scanner 47
Secrétariat général d'Interpol 9
service des notices internationales d'Interpol . 12
Sesurity Administrator Tool for Analyzing Networks 40
SITA 59
sniffing 40
système ASF 59
système ICIS 60

T

Type d'infractions informatiques 22; 26
typologie des criminels 27

U

UNIX 39
utilitaristes 28

V

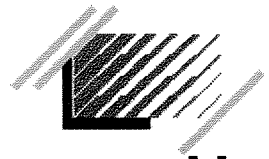
veille de la criminalité 11
Ver informatique 23
vers 34
virus 45
virus informatiques 32; 33; 45; 63
vol secret de fabrique par voie informatique ..25

W

War Dialers 40
weekly intelligence message 11

X

X400 58



Ecole
Nationale Supérieure
des Sciences
de l'information
et des Bibliothèques

17-21
bd. du 11 novembre 1918
69632 VILLEURBANNE
Cedex France

Téléphone : 0033 4
72444343
Télécopie : 0033 4
72442788
Web :
http ://www .enssib.fr