UNIVERSITÉ PAUL VERLAINE – METZ
École doctorale
« Perspectives interculturelles : écrits, médias, espaces, sociétés »
Centre de recherche sur les médiations (ÉA 3476)

LES MONDES DE LA CYBERDÉLINQUANCE ET IMAGES SOCIALES DU PIRATE INFORMATIQUE

Thèse pour le doctorat
en sciences de l'information et de la communication

présentée et soutenue publiquement le 26 octobre 2007
par

Jean-Philippe HUMBERT

Directeur de thèse : M. Jacques WALTER
Professeur à l'université Paul Verlaine – Metz

UNIVERSITÉ PAUL VERLAINE – METZ
École doctorale
« Perspectives interculturelles : écrits, médias, espaces, sociétés »
Centre de recherche sur les médiations (ÉA 3476)

LES MONDES DE LA CYBERDÉLINQUANCE ET IMAGES SOCIALES DU PIRATE INFORMATIQUE

Thèse pour le doctorat
en sciences de l'information et de la communication

présentée et soutenue publiquement le 26 octobre 2007 par
Jean-Philippe HUMBERT

devant le jury composé de :

M. Arnaud Mercier, Professeur en sciences de l'information et de la communication, Université Paul Verlaine – Metz
M. Eric Dacheux, Professeur en sciences de l'information et de la communication, Université Clermont-Ferrand 2, rapporteur
M. Gino Gramaccia, Professeur en sciences de l'information et de la communication, Université Bordeaux 1, rapporteur
M. Robert Longeon, Chargé de mission Sécurité des Systèmes d'Information, Centre National de la Recherche Scientifique (Paris)
M. Jacques Walter, Professeur en sciences de l'information et de la communication, Université Paul Verlaine – Metz, directeur de thèse

Remerciements

Ce travail n'aurait pu être réalisé sans la collaboration de plusieurs personnes. Mes pensées vont en premier lieu à ma famille, particulièrement à mon épouse et à ma fille ayant patiemment partagé mon travail au jour le jour.

J’adresse également mes vifs remerciements à mon directeur de recherche, M. le Pr. Jacques Walter, pour son aide, ses conseils et l’attention apportée à mon travail.

Ma reconnaissance va aussi vers M. Jeannot Krecké, Ministre de l’Économie et du Commerce extérieur du Grand-Duché de Luxembourg, M. Etienne Schneider, chargé de la direction générale de l’Energie et des Communications, ainsi que mes collègues du Ministère de l’Économie et du Commerce extérieur, compagnons de route indissociables de ce travail : MM. Raymond Faber, François Thill, Pascal Steichen, Jean-Marie Reiff et Dominique Ferrand.

Je tiens aussi à remercier, MM. Eric Dubois, Jean-Paul Michel, ainsi que Nicolas Mayer du Centre de Recherche Public Henri Tudor (Grand-Duché de Luxembourg), pour nos nombreuses interactions de recherche pertinentes, et enfin, tous ceux qui, d’une manière ou d’une autre, ont participé à ce mémoire.

Sommaire

Introduction 15

Titre I - Représentation sociale de la cyberdélinquance : illégalité et contexte statistico-démonstratif pour base structurante des significations sociales du pirate informatique 43

I – L'évidence des menaces numériques 44

1) La société numérique du risque 45
2) Types d'actions cybercriminelles 53

II – Le cadre sémantique de la cyberdélinquance 67

1) Etat d'éléments pertinents de recherche en matière de cyberdélinquance 67
2) Définitions d'une activité illégale 81
3) Historique de la cyberdélinquance 93

III – Identification des cadres de construction et de renforcement de l'image statistico-démonstrative et illégale de la cyberdélinquance 104

1) Les « entrepreneurs » de la sécurité de l'information 105
2) Des statistiques éprouvées 114
3) Représentation sociale et cyberdélinquance 126

Titre II - Approche communicationnelle du contexte social de la cyberdélinquance : reflet médiatique dominant du pirate informatique 134

I – Contexte et images sociales de la cyberdélinquance 136

1) Le contexte social du pirate informatique 137
2) Sondage public de l'image sociale dominante du pirate informatique 144
3) L'image médiatique « dominante » du pirate informatique 158

II – Rapport des médias à la construction de l'image sociale du pirate informatique 162

1) Veille médiatique – Internet : 162
2) Veille médiatique – Presse écrite : 175
3) Veille médiatique – Monde du journalisme : 187

III – D'autres mondes « bâtisseurs » d'images du pirate informatique 195

1) La sécurité de l'information et de la communication pour domaine d'expertise . 195

2) Les acteurs principaux de la cyberdélinquance 208

Titre III - Approche intégrée des significations du pirate informatique : un ensemble d'images sociales 221

I – Significations du pirate informatique du point de vue de l'expertise sécurité 222

1) Construction des significations des acteurs de la répression en France 223

2) Immersion et retour d'expérience au cœur du réseau « sécurité de l'information » luxembourgeois 232

II – Construction de l'auto-signification du « pirate informatique » 248

1) L'impossible pénétration sociologique du milieu 248

2) Modes d'organisation de la mouvance « *underground* » 259

III – Exemple de cas concret d'application de l'intégration des significations : le Grand-Duché de Luxembourg 281

1) Le besoin identifié d'une struture nationale d'observation des menaces IT 281

2) Le domaine de la réponse sur incidents (recherche et veille) 284

3) Perception du cybercrime au G-D de Luxembourg 288

Conclusion 305

Bibliographie 330

Annexes 339

Annexe 1 - Références (WEB) 339

Annexe 2 – Statistiques CSI/FBI 2005 341

Annexe 3 – Statistiques Panorama Cybercrime Clusif 2005 357

Annexe 4 - Liste des membres du CAP PFI Sécurité (Liste à jour 11 décembre 2006). 366

Annexe 5 – Exemples de techniques de piratage informatique 367

Annexe 6 – Questionnaire sondage (Version 1) 370

Annexe 7 – Questionnaire sondage (Version 2) 373

Annexe 8 – Roadmap des acteurs de la répression informatique en France..... 377

Annexe 9 - Corpus d'articles de la presse écrite française (1995-2003) 378

Annexe 10 – Listes des relevés « Google » à partir des mots-clés « cybercrime » et « pirate informatique » (janvier-juin 2006) 380

Annexe 11 – Veille documentaire du domaine de la réponse sur incidents 385

Annexe 12 – « Panorama Cybercrime Luxembourg – Partie I » (2005-2006)..... 387

Annexe 13 – Bilan individuel de recherche : Jean-Philippe Humbert..... 398

Liste des figures

- Figure 1. Modélisation graphique des représentations sociales de la cyberdélinquance 132

- Figure 2. Modélisation graphique de la représentation médiatique du pirate informatique 194

- Figure 3. La démarche d'analyse de risques EBIOS 240

- Figure 4. Modélisation graphique de la représentation du pirate informatique par le monde de la sécurité des systèmes d'information..... 247

- Figure 5. *What the Hack*, 28 au 31 juilllet 2005..... 260

- Figure 6. *What the Hack*, 28 au 31 juilllet 2005..... 261

- Figure 7. *What the Hack*, 28 au 31 juilllet 2005..... 262

- Figure 8. *Hack.lu*, 19 au 21 octobre 2006 263

- Figure 9. *Hack.lu*, 19 au 21 octobre 2006 264

- Figure 10. *Hack.lu*, 19 au 21 octobre 2006 265

- Figure 11. Badge d'accès à la conférence *DefCon*..... 267

- Figure 12. Bannière *DefCon (sticker)*..... 268

- Figures 13, 14 et 15. *What the Hack*, 28 au 31 juilllet 2005 – *CCC Camp*..... 270

- Figure 16. *What the Hack*, 28 au 31 juilllet 2005..... 276

- Figures 17, 18, 19 et 20. *What the Hack*, 28 au 31 juilllet 2005 279

- Figure 21. Modélisation graphique de la représentation du pirate informatique par le monde des pirates informatiques 280

- Figure 22. Modélisation graphique de l'objet de recherche « pirate informatique » en construction *via* les mondes de la cyberdélinquance 329

- Figure 23. Rapport CSI/FBI 2005 – Réponses par secteur industriel 343

- Figure 24. Rapport CSI/FBI 2005 – Usage illégal d'ordinateurs /12 derniers mois 346

- Figure 25. Rapport CSI/FBI 2005 – Type d'attaques ou mauvaise manipulation /12 derniers mois 349

- Figure 26. Rapport CSI/FBI 2005 – Relevés d'expérience d'incidents sur site web ... 351

- Figure 27. Rapport CSI/FBI 2005 – Montant des pertes par type d'attaques 352

- Figure 28. Rapport CSI/FBI 2005 – Technologies de sécurité utilisées 354

- Figure 29. Roadmap des acteurs de la repression en France 377

Liste des tableaux

- Tableau 1. Questionnaire cyberdélinquance – Résultats question N°1 149

- Tableau 2. Questionnaire cyberdélinquance – Résultats question N°2 150

- Tableau 3. Questionnaire cyberdélinquance – Résultats question N°3 150

- Tableau 4. Questionnaire cyberdélinquance – Résultats question N°4 150

- Tableau 5. Questionnaire cyberdélinquance – Résultats question N°5 151

- Tableau 6. Questionnaire cyberdélinquance – Résultats question N°6 151

- Tableau 7. Questionnaire cyberdélinquance – Résultats question N°7 151

- Tableau 8. Questionnaire cyberdélinquance – Résultats question N°8 152

- Tableau 9. Questionnaire cyberdélinquance – Résultats question N°9 152

- Tableau 10. Questionnaire cyberdélinquance – Résultats question N°10 153

- Tableau 11. Questionnaire cyberdélinquance – Résultats question N°11 153

- Tableau 12. Questionnaire cyberdélinquance – Résultats question N°12 153

- Tableau 13. Questionnaire cyberdélinquance – Résultats question N°13 154

- Tableau 14. Questionnaire cyberdélinquance – Résultats question N°14 155

- Tableau 15. Classement des alertes Google (mots clés « pirates » et « cybercrime ») 164

- Tableau 16. Répartition des articles de presse portant sur le domaine de la cybercriminalité 178

- Tableau 17. Tableau récapitulatif des menaces à la SSIC 246

- Tableau 18. Rapport CSI/FBI 2005 – Répartition des incidents internes/externes 347

Liste des acronymes

ACK – “ACKnowledge”

AFNOR - Agence Française de NORmalisation

ANSIL - Association de Normalisation pour la Société de l’Information Luxembourg

AOL - American On Line

APSI – Association des Professionnels de la Société de l’Information

APWG - Anti-Phishing Working Group

ASBL – Association Sans But Lucratif

ASCII – American Standard Code for Information Interchange

AVI – Audio Video Interleave

BBS – Bulletin Board System

BCG - Boston Consulting Group

BCRCI - Brigade Centrale de Répression contre le Crime Informatique

BRIC – Brésil, Russie, Inde, Chine

BSA - Business Software Alliance

CAP - Comité d’Accompagnement - PFI Sécurité

CASES - Cyberworld Awareness & Security Enhancement Structure

CCC - Chaos Computer Club

CCRC - Computer Crime Research Center

CERT-A - Centre d’Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques

CERT-CC - Computer Emergency & Response Team – Coordination Center

CESCTI – Centre d’Etudes Stratégiques sur la Convergence des Technologies de l’Information

CEVECS – Centre de Veille, de Conduite et de Synthèse

CFSSI - Centre de Formation Sécurité des Systèmes d’Information

CIA – Central Intelligence Agency

CIRET – AVT - Centre International de Recherches et d’Etudes sur le Terrorisme & l’Aide aux Victimes du Terrorisme

CIRT - Computer Incident Response Team

CLUSIF – CLUb de la Sécurité de l'Information Française

CLUSSIL - CLUb de la Sécurité des Systèmes d'Information Luxembourg

CNIL - Commission Nationale de l'Informatique et des Libertés

CNLSI - Comité de Normalisation Luxembourg pour la Sécurité de l'Information

CNSSI - Commission de Normalisation pour la Sécurité des Systèmes d'Information

COSSI – Centre Opérationnel de la SSI

CRP-HT - Centre de Recherche Public Henri Tudor

CSI - Computer Security Institute

CSIRT - Computer Security Incident Response Team

CSIRT-LU - Computer Security Incident and Response Team Luxembourg

CSRRT - Computer Security Research & Response Team

DADVSI - Droit d'Auteur et Droits Voisins dans la Société de l'Information

DARPA - Defense Advanced Research Projects Agency

DCSSI - Direction Centrale de la Sécurité des Systèmes d'Information

DdoS - Distributed DoS

DGCCRF - Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes

DGSE – Direction Générale de la Sécurité Extérieure

DNS - Domain Name Server

DoS - Denial of Service

DSI – Direction des Systèmes Informatiques

DST – Direction de la Surveillance du Territoire

EBIOS - Expression des Besoins et Identification des Objectifs de Sécurité

EEMA – European Electronic Messaging Association

ENISA - European Network & Information Security Agency

EPITA - École Pour l'Informatique et les Technologies Avancées

ETSI - European Telecommunications Standards Institute

FBI - Federal Bureau of Investigation

FCCU - Federal Computer Crime Unit

FSSI – Fonctionnaire de la Sécurité des Systèmes d'Information

HFD – Haut Fonctionnaire de Défense

HIDS - Host-based Intrusion Detection System

IBM – International Business Machines Corporation

IDS - Intrusion Detection System

IEC - Institut Européen de Cyndiniques

IEEE – Institute of Electrical and Electronics Engineers

IETF - Internet Engineering Task Force

INHES - Institut National des Hautes Etudes de Sécurité

IOS - Internetwork Operating System

IP – Internet Protocol

IRC – Internet Relay Chat

IRT - Incident Response Team

ISIQ - Institut de Sécurité de l'Information du Québec

ISP – Internet Service Provider

ISO - International Standardization Organization

ISO/JTC1/SC27 - IT Security Techniques - Joint Technical Committee 1 - International Standardization Organization

ISP - Internet Service Provider

ISS - Internet Security Systems

IT – Information Technology

KGB – Komitet Gossoudarstvennoï Bezopasnosti

LCEN – Loi pour la Confiance dans l'Economie Numérique

MARION – Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux

MEECES - Money, Entertainment, Ego, Cause, Entrance, Status

MEHARI – MEthode Harmonisée d'Analyse de RIsques

MELISA – Méthode d'Evaluation de la Vulnérabilité résiduelle des systèmes

MIT - Massachusetts Institute of Technology

MSN – Microsoft Network

MSSI - Management de la Sécurité des Systèmes d'Information

MX - Mail Exchange

NASA – National Aeronautics and Space Administration

NFS - Network File System

NIPC - National Infrastructure Protection Center

NIST - National Institute of Standardization Technology

NTIC – Nouvelles Technologie de l'Information et de la Communication

OCLCTIC - Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information

OTAN – Organisation du Traité de l'Atlantique Nord

PC - Personal Computer

PFI - Plate-Forme d'Innovation

PIB – Produit Intérieur Brut

PIN – Personal Identification Number

PJ – Police Judiciaire

R2SIC - Recherche pour la Sécurité des Systèmes d'Information et de la Communication

RG – Renseignements Généraux

RSSI – Responsable de la Sécurité des Systèmes d'Information

SAM – Security Account Manager

SCSSI - Service Central de la Sécurité des Systèmes d'Information

SERT - Security Emergency Response Team

SGDN – Secrétariat Général de la Défense Nationale

SI - Système d'Information

SMTP – Simple Mail Transfert Protocol

SPIRAL – Réseaux des professionnels de l'IT au Grand-Duché de Luxembourg

SSI - Sécurité des Systèmes d'Information

SSIC - Sécurité des Systèmes d'Information et de la Communication

SYN – « SYNchronisation »

TAZ - Temporary Autonomous Zone

TCP - Transmission Control Protocol

TCP/IP - Transmission Control Protocol/Internet Protocol

TF-CSIRT – Task Force - Computer Security Incident Response Team

TIC – Technologie de l'Information et de la Communication

TTL - Time To Live

VoIP - Voice Over IP

Introduction

La croissance des réseaux d'information et de communication, à l'échelle internationale, s'est corrélativement accompagnée d'une aggravation des risques et des menaces associées. En effet, ces réseaux reposent sur des systèmes informatiques qui n'ont pas été développés, de manière intrinsèque, avec des critères formels de sécurité, entraînant, de fait, l'exploitation possible de faiblesses nombreuses (les vulnérabilités). Ces dernières constituent les vecteurs de la réalisation du risque de sécurité, lorsqu'elles sont exploitées par ce qu'il est commun de dénommer les « menaces ». Ces menaces appliquées aux systèmes d'information et de communication peuvent être classifiées selon deux axes principaux : les agents techniques et les agents humains.

Les agents techniques peuvent être compris comme l'outil final utilisé pour attaquer un système informatique, ou encore la méthodologie « technique » particulière associée à l'attaque (exemple : le *social engineering* - ingénierie sociale - visant à profiter de la naïveté d'un utilisateur, par pression morale, pour en obtenir des données confidentielles). Ces agents techniques peuvent être également doués d'une certaine autonomie, pouvant se développer seuls sur les réseaux (exemple : les vers[1] Internet). Les agents humains sont ceux qui développent et/ou exploitent cet outil et/ou méthodologie associés au piratage informatique. Cette dichotomie formalise la différence entre deux objets de recherche possible : le premier d'ordre technique, le second de nature humaine.

Les premiers sont certainement les plus connus et les mieux appréhendés. Il convient de constater l'existence de nombreux dispositifs de protection de réseau informatique, que ce soit en entreprise avec le « *firewall* » (mur pare-feu) par exemple, ou encore avec l'anti-virus pour le particulier. La pénétration et le développement de ces outils de contre-mesures techniques sont de plus en plus prononcés en regard de la multiplication des menaces de sécurité sur les réseaux informatiques, et en réponse à leur forte médiatisation ; en corrélation les messages de sensibilisation à la sécurité de l'information sont aussi toujours remis à jour et véhiculés continuellement, ce que la

[1] *Un ver est un logiciel très similaire à un virus. Cependant et contrairement au virus, un ver n'a ni besoin de l'intervention humaine, ni d'un programme hôte pour infecter une machine. Il dispose de son propre moteur, un automatisme qui lui permet de délivrer et d'exécuter automatiquement son code, comme par exemple un mini serveur de mail lui permettant de transmettre une copie de son code par e-mail, puis, par la suite, de chercher des nouvelles cibles à infecter.*

Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI France) nomme : la « *marteau-thérapie* » (*sic*)[2].

Notre travail de recherche s'intéressera au second objet possible annoncé *infra* et relatif aux menaces des systèmes d'information et de communication. En effet, notre recherche visera surtout à étudier la réalité sociale des agents humains de la menace numérique, à savoir l' « attaquant d'ordinateurs », qui, *via* ses actions, a formalisé un nouveau cadre de loi et de répression adapté au numérique. Mais, la connaissance de cet acteur n'est pas actuellement véritablement maîtrisée par l'opinion publique, notamment par absence de mise en relation directe ou encore par ignorance de son contexte social. Ainsi le citoyen, (tout individu, en fait, au sein de la société pris dans son acception la plus large) ne peut finalement que se représenter notre objet de recherche, dans le meilleur des cas (sauf si ce dernier fréquente des réseaux ou bien des personnes coutumières du fait, ce qui demeure rare), ou bien, tout simplement ignorer cet acteur « dangereux ». Nous nous intéresserons donc principalement à ceux que nous nommerons les « pirates informatiques », constitutifs d'un concept né avec les réseaux et ses multiples attaques relevées, à savoir : la cyberdélinquance (nous ne ferons pas de différence entre les termes « cyberdélinquance » et « cybercriminalité », par mesure de simplification compréhensive, bien que le terme « cyberdélinquance » nous semble le plus juste aujourd'hui, car moins restrictif). La notion de pirate informatique se confond aussi souvent avec celle de *hacker*, qui s'affiche ou est affichée parfois comme démarquée de tout acte illicite, mais aussi avec celle de cyberdélinquant ou encore de cybercriminel. Nous montrerons que cette distinction des appellations devrait pourtant permettre de qualifier correctement le risque engendré, mais, que, dans tous les cas, elle prête surtout à confusion et ne facilite pas véritablement le jugement de valeur de l'acteur concerné. Objet menaçant et élément de risque de sécurité, le pirate informatique nous laisse finalement une interrogation en terme de compréhension et de connaissance générale. En effet, le fait que ce personnage reste d'appropriation floue au sein de la société constitue pour nous un véritable questionnement, une question de communication

[2] Réunion DCSSI du 23/01/2007 « *Conception du portail d'information sur la sécurité des systèmes d'information pour tout public* » (« *Développer la sensibilisation et promouvoir les réseaux d'alertes* » – CISI – Comité interministériel pour la Société de l'Information du 11 juillet 2006).

face à cet objet de recherche, et qui cadrera ainsi notre travail de réflexion. Nous poserons donc le pirate informatique en tant qu'objet de notre recherche (et nommé ainsi dans la suite du document), afin d'interroger qualitativement ses significations associées (au sens des valeurs sociales accordées) au sein de la société. Pour ce faire, nous nous attacherons à étudier cet objet à la lumière du concept de l'image sociale.

Méthodologie

De façon à justifier nos choix méthodologiques pour guider notre travail, nous détaillerons notre parcours professionnel qui constitue un véritable pré-requis ayant mené à cette réflexion de recherche. Nous travaillons depuis 1994 sur des problématiques relatives au pirate informatique. Le point de départ de notre carrière professionnelle a commencé au cœur de la première unité de lutte dédiée au cybercrime, au ministère de l'Intérieur en France (75 – Paris). Nous avons pu ainsi observer de près les pirates informatiques de 1994 à 2001, en tant que Lieutenant de Police veillant à la répression du cybercrime en France. Nous avons été très impliqués sur cette matière, dès les premières enquêtes judiciaires de cybercrime d'envergure, au niveau national et international. Le pirate informatique est devenu, dès lors, une de nos préoccupations majeures. Notre implication s'est renforcée de 2001 à 2007, avec un changement professionnel, en devenant ingénieur de recherche spécialisé dans le domaine de la sécurité de l'information. Nous avons ainsi pu participer au développement de nombreux concepts visant l'amélioration constante des principes de protection numérique pour tout type d'organisation, notamment en tant que chargé de missions pour le ministère de l'Économie et du Commerce extérieur du Grand-Duché de Luxembourg. Encore une fois durant cette période, le pirate informatique était présent dans nos réflexions, en tant que « menace avérée ». Récemment encore, nos nouvelles fonctions en tant qu'employé d'État au ministère de l'Économie et du Commerce extérieur au Grand-Duché de Luxembourg, où nous sommes en charge de l'accréditation des systèmes d'infrastructure à clés publiques, visant la confiance numérique nationale, sont accompagnées de même, d'implications fortes en termes de sécurité de l'information, reconnaissant l'aspect

menaçant des pirates informatiques. Enfin, notre travail de DEA[3] (2003) nous a aussi permis de mesurer l'importance de la recherche relative au pirate informatique, alors posé comme interconnecté avec la notion de risque au cœur de la société de l'information. *Via* le présent travail de recherche, nous capitaliserons donc huit ans d'expérience directe envers le phénomène de la cyberdélinquance, ainsi que six ans spécifiquement dans le champ de la sécurité de l'information. De fait, de manière naturelle nos deux terrains de recherche seront constitués de la France et du Grand-Duché de Luxembourg, en regard de notre expérience professionnelle (Cf. *supra*).

De manière parallèle à notre parcours professionnel, les statistiques montrent, depuis plusieurs années, au niveau international, une augmentation exponentielle des incidents de sécurité au sein des réseaux d'information et de communication, dont les causes sont multiples. En 2004, l'étude « *e-crime watch* », menée par le centre de coordination des équipes de réponse et d'urgence informatique[4] (Etats-Unis) a, par exemple, relevé, auprès des organismes ayant répondu à l'enquête, un préjudice total de 666 millions $. Sans aucun doute, depuis l'interconnexion croissante des réseaux d'information et de communication vers l'extérieur, les menaces externes se sont multipliées d'autant. La société de l'information ne semble, à ce titre, qu'une transposition de la société traditionnelle. Cependant, les menaces au cœur de la société de l'information existent réellement 24/24 heures et 7/7 jours, sans connaître de frontière physique ou temporelle. Les menaces ne se limitent plus à un périmètre particulier, elle concerne tout ordinateur interconnecté, que ce soit celui d'un particulier, d'un enfant, d'un employé, d'un directeur d'entreprise, ou encore d'un dirigeant, pour autant qu'il soit vulnérable. La capacité de réplication d'une attaque numérique est désormais infinie, ce qui rend ce phénomène aussi dangereux. Bien que le premier délit informatique identifié ait été commis aux Etats-Unis en 1966 (il s'agissait alors d'une altération des comptes d'une banque de Minneapolis – Etats-Unis), la criminalité des réseaux est globalement un phénomène plus récent (en témoigne sa médiatisation), en expansion constante depuis le début des années 1980. Elle s'est généralisée en France, depuis l'avènement d'Internet, fin 1994. « *L'évolution de ce phénomène cybercriminel est constante et a suivi, au cours*

[3] *La cyberdélinquance, un risque pour Internet ?* (Humbert, 2003).
[4] Usuellement dénommé *CERT-CC* soit *Computer Emergency and Response Team- Coordination Center.*

des vingt dernières années, celui de la démocratisation de l'accès à l'informatique et de la globalisation des réseaux. L'internet lui offre depuis peu une nouvelle plate-forme de développement »[5]. Ces menaces diverses se doivent d'être analysées et comprises pour agir en conséquence et connaissance de cause. En effet, au cœur du processus de la gestion des risques de la sécurité de l'information, la méthodologie de l'évaluation des risques prévoit spécifiquement l'identification et l'étude des menaces (mettant à disposition des bases complètes de références).[6] Ainsi, afin de mieux formaliser l'identification des menaces, il convient aussi de replacer ce concept au cœur de la théorie du risque. L'interconnexion des réseaux et des systèmes imposant désormais la nécessité de penser ce phénomène de manière globale. La société traditionnelle dans laquelle nous vivons présente de nombreuses menaces auxquelles nous prêtons attention et contre lesquelles nous nous protégeons consciemment ou par réflexe. La protection est soit préventive ou réactive, en fonction d'une perception particulière de la menace au sein de l'espace public. La cyberdélinquance, ainsi identifiée au sein de la société de l'information et de la communication, correspond, nous le verrons, à une menace caractérisée, généralisée sur les réseaux d'information et de communication, et notamment sur Internet. En 1994, en France, les enquêtes de cybercrime étaient principalement relatives à des actes de cyberdélinquance sur les réseaux de type X25 (réseau Transpac de France Télécom), *via* des pénétrations véhiculées par des pirates se réunissant *via* des systèmes de communication partagée en ligne[7] (*BBS*). Cette communauté particulière, de la génération Minitel, était le point de ralliement et de « *challenges* » numériques pour attaquer des sites informatiques « atteignables » *via* le réseau public X25. Puis, rapidement, les premiers fournisseurs d'accès Internet[8] (*ISP*) sont apparus en France, après les *BBS*, les points de ralliement à la mode devenaient les systèmes de communication partagée en ligne sur Internet[9] (*IRC*) ; et depuis le mouvement a grandi, avec la croissance des facilités de communication numérique.

[5] *La criminalité sur l'Internet* (Pansier, Jez, 2000).
[6] *ISO/IEC 27005 : « Information technology - Security techniques - Information security risk management »* (référence mondiale en matière de gestion des risques de sécurité de l'information).
[7] Usuellement dénommées *BBS* soit *Bulletin Board System.*
[8] Usuellement dénommés *ISP* soit *Internet Service Provider.*
[9] Usuellement dénommés *IRC* soit *Internet Relay Chat.*

Aujourd'hui, les cibles potentielles sont désormais tous les ordinateurs qui sont interconnectés *via* le jeu de protocoles réseau utilisé sur Internet : TCP/IP[10], c'est-à-dire la quasi-majorité absolue du parc informatique et/ou de tout appareil informatisé au niveau mondial.

L'information et la communication relative à cette menace « *underground* » sont prolixes au niveau international, et notamment *via* Internet. Cependant, les pratiques d'attaques étant de plus en plus élaborées, et la technologie parfois difficile d'appréhension, ce sont désormais les protagonistes mêmes qui demeurent véritablement à un niveau d'accès et de compréhension très opaque, justifiant le terme qui caractérise leur monde social, à savoir l'« *underground* » (mouvement souterrain, clandestin). En regard, le pirate informatique demeure un objet de recherche complexe, sujet à de nombreuses interprétations, faisant l'objet de multiples significations, voire des mélanges de genre, plus ou moins bien agrégés au niveau international. Ainsi, de par son existence même, et surtout face à des actes formalisés très préjudiciables, notamment via les médias, l'objet est très présent en termes d'information et de communication et, de facto, son contexte semble socialement représenté. Un dixième de seconde suffit, sur Internet, *via* un moteur de recherche (données de juin 2007, http://www.google.fr), pour obtenir plus de 1,5 millions de résultats pour la requête « pirate informatique », de même, plus de 3 millions de résultats sont disponibles pour la requête « cybercrime ». L'information produite et véhiculée demeurant le vecteur principal de diffusion de connaissance de l'objet de recherche, il nous importe, par notre étude, de tenter d'en dégager la réalité sociale. La caractérisation sous forme d'image sociale est désormais devenue de mise face à cet objet de recherche, en effet, la majorité des citoyens ne rencontrera jamais sciemment et physiquement un pirate informatique. Souvent reconnu, parfois perçu ou inconnu, quasiment jamais rencontré, il nous semble déterminant d'établir le cadrage social de l'image produite de cet acteur à l'origine de ces nombreux dysfonctionnements numériques. « *Comme les représentations sociales, les images sociales seraient attachées à un objet, et fonderaient, pour une bonne part, le jugement porté sur cet objet (attitudes d'attraction ou de rejet, ou bien évaluation normative). Ainsi, les images sociales*

[10] *Transmission Control Protocol/Internet Protocol.*

orientent non seulement la cognition sociale, mais également les conduites et positions à l'égard de l'objet qui devient, de la sorte, accepté ou refusé, préféré ou dénigré, élu ou banni (Moscovici, 1961, 1976) »[11]. Ainsi définies, les images sociales semblent, en effet, des effecteurs non négligeables du rendu des significations de notre objet de recherche au cœur de la société.

Lors du 17ème Congrès international des sociologues de la langue française[12], Hélène Jeannin[13] rend compte du déficit d'image dont souffre le pirate informatique, depuis l'année 2000, évoquant « *un processus de déconstruction de la figure de ce personnage des réseaux, popularisé dès les années quatre-vingt par le film Wargames* ». Cette dernière montre l'importance des médias dans la qualification du pirate informatique, qui finalement semblent s'être appropriés son image du « héros moderne » (sic), avec pour traduction une caractérisation « dangereuse » non maîtrisable par les puissances publiques, entraînant, de facto, le déclin du « personnage » et le développement d'un arsenal répressif conséquent en réponse. Ces images médiatiques semblent répondre aux mêmes caractéristiques que le concept des images sociales, décliné *supra*, qui permettent d'affecter des valeurs de jugement vis-à-vis de l'objet, pouvant alors entraîner des conséquences sur sa représentation sociale. Ces images « qualificatives » déterminent la clé de compréhension pour expliquer la pensée sociale qui affecte le pirate informatique. Cependant, « *les images sociales ne sont pas des représentations, elles en sont le produit (Molinier, 1996)* »[14]. De ce fait, l'identification et la caractérisation de l'objet initial représenté socialement, comme producteur majeur des images sociales du pirate informatique, demeure la première étape de notre recherche. Pour cadre de référence, entourant le pirate informatique, nous déterminerons, la cyberdélinquance, en tant qu'objet social constitué pouvant alors être considérée comme génératrice des qualifications et des jugements affectés au pirate informatique. Bien qu'il paraisse important de déterminer s'il existe plusieurs images sociales du pirate

[11] *Les représentations sociales* (Mannoni, 2001).
[12] 17ème Congrès international des sociologues de la langue française, Tours, France, du 6 au 8 juillet 2004.
[13] *Du pirate informatique au cybercriminel : Grandeur et décadence d'une figure de héros contemporain* (Jeannin, 2004).
[14] *Les représentations sociales* (Mannoni, 2001).

informatique, il demeure primordial d'étudier les processus de construction de ses images sociales, alors en inter-relation avec la représentation sociale de la cyberdélinquance.

Pour ce faire, nous nous engagerons vers une démarche compréhensive en suivant une « ficelle » prônée par H.S. Becker[15] : « *Ne demandez pas « Pourquoi ? » ; demandez « Comment ?* » ». « *Quant aux composantes des images sociales, elles regroupent l'ensemble des caractéristiques et des propriétés physiques, psychologiques ou sociales que les individus attribuent aux objets avec lesquels elles sont en rapport. Tous les membres d'un groupe sont concernés et adoptent, à l'égard des objets en question, la même attitude et le même type de jugement. De cette manière, ils sont intégrés dans l'univers cognitifs du groupe et deviennent pour lui, des objets sociaux (investis ou évités) (Molinier, 1996)* »[16]. Le processus de construction de l'image sociale se lie donc, par dépendance, à des dispositifs d'où émergent les significations (les images produites), déterminant le contexte social dans lequel elle est générée. Nous nommerons ce dispositif (le groupe en question) : un monde social. De plus, « *Deux conditions président à l'émergence d'une image sociale : que les individus aient des informations et des expériences comparables, et qu'ils mettent en œuvre des savoirs préalables communs à type de représentations sociales (Molinier, 1996)* »[17]. Nous pouvons donc identifier et étudier en regard de l'objet de recherche des groupes constitués en tant que mondes sociaux, et nous considèrerons en l'espèce la possibilité de plusieurs de ces groupes sociaux. Pour l'objet de recherche, l'image médiatique joue et a joué un rôle déterminant, dans son processus de construction « positif » ou « négatif », et à ce titre, il conviendra d'étudier aussi plus finement sa production et son discours. En effet, en absence de contexte social « direct et palpable » du pirate informatique, l'image médiatique peut jouer, à part entière, et par défaut le rôle d'une image sociale de fait, voire dominante, car appropriée par l'ensemble en tant que tel, comme produit majeur de la représentation sociale de la cyberdélinquance. Nous rendrons compte du fait que l'information produite, en regard de l'objet de recherche, se construit sur un ensemble de choix discursifs empruntant une forme écrite spécifique, et que ces partis pris discursifs peuvent oeuvrer

[15] *Les ficelles du métier* (Becker, 2001).
[16] *Les représentations sociales* (Mannoni, 2001).
[17] *Les représentations sociales* (Mannoni, 2001).

ainsi à la promotion, voire à la construction, chez les individus d'images se structurant de manière collective : « *Agissant comme des filtres interprétatifs, ces représentations constituent des instruments d'intelligibilité du réel, perçu à travers ces biais comme plus ou moins violent, plus ou moins rationnel…* »[18]. Il semble important, de ce fait, de vérifier cette force structurante des médias sur l'objet étudié et de déterminer si cela demeure suffisant pour interroger la génération des significations sociales de ce dernier. Pour ce faire, nous déterminerons plusieurs axes possibles d'approche médiatique de l'objet social, comme autant de marqueurs en montrant l'importance.

Pour accompagner notre réflexion, une multitude de travaux de recherche dans les champs de l'informatique ou des systèmes d'information s'oppose au manque de travaux de référence en sciences sociales. Ainsi, actuellement, la recherche s'intéresse plus fortement au moyen technique de lutte contre la cyberdélinquance qu'à sa compréhension sociale, à travers ses responsables principaux. Les ouvrages consacrés au pirate informatique sont très souvent d'ordre professionnel, et majoritairement d'outre-atlantique. A ce titre, nous pouvons constater le peu de travaux français relevant de cette discipline qui soit entièrement consacré à l'objet, de surcroît au cœur des sciences de l'information et de la communication. En regard, de ce constat, que nous détaillerons dans le premier temps de notre étude, notre méthodologie se décline naturellement afin de pallier aux absences de travaux de recherche pertinents permettant de relever de la réalité de l'objet social que constitue le pirate informatique, en étudiant sa construction sociale à travers une approche communicationnelle globale. À partir de l'observation de terrain, nous expliquerons, ainsi ce phénomène sous l'angle des sciences de l'information et de la communication, afin d'en percevoir les implications, notamment en déterminant clairement les responsables identifiés des aspects de déstabilisation de l'information et de la communication. Ainsi, nous interrogerons les lieux de discours spécifique relatifs au pirate informatique, comme lieux de construction de ses significations.

Via ces travaux, notre ambition vise à atteindre, en terme d'expérience personnelle, un besoin de « vérité » vis-à-vis de l'objet de recherche et doit permettre d'en rendre compte à partir d'une approche « terrain », aussi dans notre contexte,

[18] *La communication médiatique* (Lochard, Boyer, 1998).

majoritairement professionnel, et qualificatif de l'objet de recherche. En effet, chacun détient sa propre vérité, mais notre implication sur ce phénomène nous demande, désormais, d'aller plus loin que la simple subjectivité d'une image mentale : « *[…] comment existerait-il même la possibilité d'expliquer quand nous faisons d'abord de toute chose une image, notre image !* »[19], en posant alors notre réflexion plus en avant au niveau de l'existence possible de plusieurs images sociales du pirate informatique.

L'intérêt de notre travail repose, principalement, sur notre angle d'analyse de l'objet, en regard de notre expérience et de notre implication professionnelle actuelle en sécurité des systèmes d'information et de la communication (voir *supra*). Nous pensons pouvoir apporter un éclairage nécessaire aux sciences de l'information et de la communication, d'un objet qui, résolument, leur appartient, et qu'elles n'ont pas véritablement analysées, pour l'instant, sous l'angle de la problématique du processus de production des images sociales de ce dernier. Nous validerons particulièrement l'importance du champ d'études de la sécurité des systèmes d'information et de communication, en réponse à la problématique posée. L'intérêt des sciences de l'information et de la communication est double, tout d'abord elles ne peuvent occulter l'analyse de ce phénomène en s'appuyant nécessairement sur des théories appartenant à d'autres disciplines. De plus, il apparaît important que soit investigué le champ d'activités pouvant nuire au développement de l'information et de la communication, *via* les technologies de l'information et de la communication (TIC), précisément en déterminant la réalité de ces acteurs sociaux considérés comme « dangereux » et responsable du fait.

Notre sujet est traité de manière particulière et vise la mise en évidence d'une démarche compréhensive possible de l'objet de recherche, mais surtout, une concrétisation professionnelle, clairement, l'aboutissement d'une période de validation des acquis. Le résultat de ce travail de doctorat vise à établir l'état de connaissance transmissible et utile à la compréhension du phénomène, tout en respectant notre détachement vis-à-vis de l'objet de recherche, tout du moins d'en être et d'en rester conscient (en regard de nos connaissance acquises professionnellement). Nous nous

[19] *Le gai savoir* (Nietzche, 1950).

intéresserons globalement à l'objet de recherche en termes d'image(s) sociale(s) produite(s) et au déroulement de sa ou de leur construction. Nous mobiliserons les concepts de la théorie des représentations sociales pour comprendre les bases et les différents aspects relatifs à la construction et évolution d'une ou des image(s) sociale(s), mais également celle des représentations médiatiques de l'objet de recherche. Notre montage théorique repose donc sur l'importance des représentations sociales, véritables effecteurs de la pensée sociale, guidant notre réflexion afin de mener à bien, l'identification du processus de construction de(s) image(s) sociale(s) du pirate informatique. Les représentations sociales sont entendues comme des systèmes d'interprétation régissant notre relation au monde et aux autres qui orientent et organisent les conduites et les communications sociales. Elles demeurent donc d'importance pour la compréhension de notre objet. Les représentations sociales forment ainsi le cadre théorique de référence de notre recherche. Pour leur analyse, en regard de l'objet de recherche, nous croiserons une méthodologie fondée sur deux grand types d'approches : celle de l'anthropologie – étude et observation de terrain, recueil et analyses de témoignages, et observation participante, et celle fondée sur l'analyse formelle des données provenant de statistiques disponibles ou encore de sondage. Ces deux approches permettront d'analyser la cyberdélinquance à la lumière de sa représentation sociale, et les images sociales du pirate informatique sous l'éclairage des processus contextualisés de production de ses significations. « *On a tendance à négliger le fait que l'aspect processuel se trouve en amont et en aval du produit, et seule la prise en compte des contenus permet une étude systématique des aspects processuels (Abric, 1987 ; Flament, 1984*[20]*)* »[21]. Ainsi, nous nous intéresserons au rôle de la représentation « *déjà-là* », mais aussi à celle en devenir, à partir de l'existant disponible. Quant à la démarche méthodologique, « *L'idée que l'étude des représentations sociales ne peut se satisfaire d'une seule méthode n'est pas nouvelle. Etudier, comme le suggérait Moscovici, la connaissance que les individus possèdent au sujet d'un objet et la manière dont celle-ci est organisée et utilisée par les individus, les groupes, implique la perspective*

[20] *Coopération, Compétition et représentations sociales* (Abric, 1987)
From the bias of structural balance to the representation of the group (Flament, 1984)
[21] *Méthodes d'études des représentations sociales* (Abric, 2003).

incontournable de la pluri-méthodologie»[22]. Nous observerons, à ce titre, une démarche parallèle à celle de la triangulation, reposant sur un principe de validation des résultats par la combinaison des différentes méthodes visant à vérifier l'exactitude et la stabilité des observations, et des données obtenues, en nous aidant de notre expérience acquise. Nous ne découperons pas véritablement notre terrain de recherche sous la forme stricte de la triangulation, mais nous nous attacherons à rendre compte des données produites par les instruments, en relation avec l'objet de recherche, et de leur validation, par expérience de ce même terrain. La forme de base, en termes de stratégie d'analyse, rejoint finalement celle proposée par Denzin, quant à la « *triangulation méthodologique* »[23] (c'est-à-dire l'utilisation de différentes méthodes et techniques pour étudier un même phénomène particulier). « *Il est difficile de définir une démarche type de triangulation et de présenter les étapes et les opérations à entreprendre ; tant l'hétérogénéité et la non-superposition systématique des opérations de triangulation à partir d'un cadre défini sont revendiquées dans une posture non-positiviste, comme des prérogatives de la démarche et de la capacité du « chercheur-bricoleur » (Denzin et Lincoln, 1998)*[24] *à mobiliser de façon raisonnée et éclectique des outils propres à chaque situation pour étudier la complexité des phénomènes auxquels il est confronté* »[25]. Ainsi, pour reprendre cette analyse de J-C Abric, nous analyserons notre objet, dans ce sens, en nous donnant pour objectif général de construire un savoir pertinent et consistant sur le phénomène, à partir des différentes opérations de croisement sur les plans théoriques, méthodologiques et/ou de production de données cités *infra*. « *En l'état actuel de nos connaissances, cet aspect mérite que l'on s'y intéresse davantage pour montrer comment les différentes constructions de la pensée sociales (construits culturels, pré-savoirs, théories implicites) affectent le traitement de l'information et la connaissance des objets sociaux »*[26].

Pour rejoindre aussi les questionnements au sein des sciences de l'information et de la communication, en relation avec la communication interculturelle, nous formaliserons l'importance de cette dernière, en privilégiant l'analyse

[22] *Méthodes d'études des représentations sociales* (Abric, 2003).
[23] *The research act*. (Denzin, 1978).
[24] *Emerging the field of qualitative research* (Denzin et Lincoln, 1998).
[25] *Méthodes d'études des représentations sociales* (Abric, 2003).
[26] *Méthodes d'études des représentations sociales* (Abric, 2003).

communicationnelle sur les terrains de plusieurs mondes sociaux en regard du pirate informatique. Cette démarche permettant aussi de dépasser la seule approche médiatique pour comprendre l'objet de recherche. En ce sens, pour atteindre la pleine mesure des significations sociales de l'objet, l'analyse des instruments de terrain semble alors nécessaires pour combler le différentiel et atteindre sa connaissance ou du moins de sa pleine mesure. Ainsi, l'absence de mise en relation, entre plusieurs interactions culturelles touchant le même objet, réduit particulièrement l'approche communicationnelle large. De fait, cette dernière semble se réduire à l'avantage de la communication médiatique qui peut alors globaliser les significations sociales de l'objet. Notre étude vise donc aussi à témoigner et relever, au profit des sciences de l'information et de la communication, des interactions autres que l'approche médiatique relatives au pirate informatique. Nous montrerons ainsi une importance pour la connaissance de l'objet de recherche et la perspective grandissante du travail de terrain, ainsi que de l'attachement aux interactions des acteurs d'où émanent les significations, cela pouvant s'appliquer à tout objet de recherche en sciences de l'information et de la communication.

Notre « moteur » méthodologique sera fondé sur le paradigme de l'interactionnisme symbolique qui au lieu de traiter les faits sociaux comme des choses, renverse la perspective, pour en faire des activités sociales toujours en chantier (rejoignant notre notion de processus de construction des significations, voir *infra*). Notre approche s'inscrit ainsi dans une approche constructiviste qui permet de prolonger notre expérience acquise, d'en utiliser les résultats, tout en respectant engagement mais aussi détachement, avec pour confirmation finale ce travail de doctorat, tentant d'approcher la vérité « sociale » de l'objet étudié. Notre perspective vise l'analyse communicationnelle du pirate informatique, au-delà de sa représentation dans les médias traditionnels, et de rendre justement compte de l'existence et de la production relative d'autres instruments communicationnels dédiés. En référence, notre hypothèse de travail consiste à mettre en évidence l'existence de plusieurs images sociales de l'objet de recherche, provenant de différents mondes sociaux, dans le sens où la signification sociale de ce dernier ne peut se réduire uniquement à l'approche médiatique (ce qui peut sembler majoritairement le cas en l'espèce), et que l'intégration de l'ensemble des vues ou autres significations peut alors jouer un rôle déterminant pour atteindre la connaissance globale de l'objet, comme

socle de sa réalité sociale. Un des risques de la prégnance médiatique est de considérer le pirate informatique comme un objet déterminé, alors que justement il paraît opportun de l'interroger comme un objet en construction à travers différents mondes sociaux.

Notre travail de recherche vise donc à expliquer la signification sociale du pirate informatique, en la rendant moins complexe, par l'étude de sa construction. Notre volonté et notre expérience nous ont conduit à privilégier cette approche d'observation de terrain entourant le pirate informatique, et donc de traiter des processus sociaux (et médiatiques) de construction de ce dernier. Notre but sera d'éviter une vérité « toute faite » venant expliquer les données, mais de favoriser une compréhension des significations produites et mises en œuvre par les différentes parties en présence, autour de l'objet, que nous nommerons ainsi « les mondes de la cyberdélinquance ». Ces mondes pris en compte, à travers les démarches théorique et méthodologique présentées *supra*, permettront d'expliquer la complexité de la représentation sociale du pirate informatique. De fait, pour terrain, nous avons établi ces mondes sociaux de la cyberdélinquance comme étant ceux qui en traitent le plus, et qui permettent de relever alors de(s) image(s) sociale(s) du pirate informatique. Pour mener à bien notre travail de recherche, nous avons mené des investigations dans les mondes sociaux de la cyberdélinquance et communiqué constamment sur nos travaux réalisés (voir annexe 13).

Les agents sociaux menaçants sont généralement globalisés *via* le vocable commun de cyberdélinquants. D. L. Carter[27], professeur au département de justice pénale de l'Université de l'Etat du Michigan, établit une définition de la cyberdélinquance en fonction de l'utilisation faite du médium informatique. Soit l'instrument informatique est utilisé par le délinquant comme outil d'un crime conventionnel (escroquerie, menaces…etc), soit l'ordinateur est la cible visée par le délinquant (vol ou destructions de données…etc). Ainsi la cyberdélinquance constitue, à la fois, une forme de criminalité nouvelle, exploitant des situations socio-économiques inédites à des fins malveillantes, mais également la traduction d'une criminalité traditionnelle qui exploite le média représenté par le réseau informatique mondial, pour alors commettre des actes délictueux déjà connus et identifiés. Si la criminalité traditionnelle a aussi basculé vers le terrain

[27] *Computer Crime Categories : How Techno-Criminals Operate* (Carter, 1992).

virtuel, la cybercriminalité est aussi véritablement une notion pénale récente pour un nouveau type de délinquance qui a grandi avec Internet et qui concerne des faits propres aux systèmes informatiques. Il s'agit des attaques affectant directement le dispositif informatique. Le coût de cette activité n'est pas simplement financier, mais est aussi lié à la fragilisation des circuits de communication électroniques et informatiques, devenus des éléments essentiels de nos économies et échanges sociaux, à l'exploitation de leurs vulnérabilités intrinsèques, mais aussi à la fragilisation de la confiance numérique, élément clé du développement d'une réelle économie numérique. Notre objet de recherche concernera principalement les acteurs d'activités relatives au second niveau de la définition de D. L. Carter : le pirate informatique qui s'attaque aux ordinateurs *via* les réseaux de l'information et de la communication (spécifiquement Internet), à savoir celui qui a engendré cette nouvelle forme de délinquance numérique, expliquée *supra*. La détermination de sa réalité sociale devrait nous permettre de mieux comprendre les fondements de telles pratiques illégales. L'image sociale du pirate informatique, au sens de sa « représentation » au cœur de l'opinion publique, constitue ainsi l'axe de recherche important au regard du développement de la croissance exponentielle de la cyberdélinquance. En effet, l'identification du rapport du citoyen à l'objet de recherche peut permettre, par exemple, de déterminer le décalage possible entre l'état de la conscience publique de la cyberdélinquance, et les efforts de sensibilisation à la sécurité de l'information encore nécessaires à apporter, et/ou ceux à améliorer ou orienter (tant au niveau sociétal, économique ou industriel). Pour ce faire, nous caractériserons en profondeur les mondes sociaux attachés à l'objet de recherche comme un (ou des) univers d'interactions et de significations partagés possibles, comme un véritable contexte social posé comme un « laboratoire d'analyse » pour notre objet de recherche, en fait une « société » particulière au sens où G. Simmel[28] la décrit : « […] *La « société » n'est dans ce cas que le nom donné à un ensemble d'individus, liés entre eux par des actions réciproques* » (Simmel, 1981, 90). Notre recherche vise, finalement, à déterminer la réalité sociale du pirate informatique, à savoir la détermination des significations associées, mais aussi le processus de construction sociale de cet objet de recherche.

[28] *Sociologie et épistémologie* (Simmel, 1981)

Mais comment déterminer une image « véritable » ? En effet, une évidence n'est pas forcément une vérité. Nous examinerons, alors, pour ce faire, ces « mondes de la cyberdélinquance », définis *supra*, sous l'angle de l'information et de la communication (*via* leurs interactions et leurs significations).

Ainsi, nous guiderons nos articulations et progressions théoriques en procédant à un éclairage disciplinaire scientifique des termes de notre question générale de recherche : **Comment se construisent les significations sociales (ou encore images sociales) du pirate informatique ?** Notre étude consistera en une démonstration hypothético-déductive, choix effectué après avoir sciemment occulté une démarche inductive, eu égard à notre expérience dans le domaine de la sécurité des systèmes d'information, et cela afin de tenter de rester neutre. Comment, en effet, comprendre notre objet de recherche complexe ? Dans quelle mesure les mondes de la cyberdélinquance permettent-ils le développement de l'image ou des images sociale(s) du pirate informatique ? Pour ce faire, nous décomposerons ainsi notre question principale, afin de l'étudier d'un aspect général vers le particulier.

Articulation des axes de recherche

Afin d'atteindre une approche interculturelle du pirate informatique, en réponse à cet objet social complexe, nous suivrons notre méthodologie détaillée *supra* en développant notre travail selon trois axes de recherche permettant d'obtenir un cadrage social large. Afin de montrer que l'image sociale du pirate informatique ne correspond pas simplement à celle de son image médiatique, nous nous demanderons : quelle(s) image(s) est (sont) produite(s) par l'état établi de la cyberdélinquance ? Puis, via une approche communicationnelle, nous nous demanderons si le reflet médiatique du pirate informatique nous renvoie son image dominante ? Enfin, via une approche interculturelle, l'intégration des significations en provenance de différents mondes sociaux permet-elle finalement de mieux traduire la réalité sociale du pirate informatique ?

I – Quantitatif, statistiques et aspects légaux : la représentation sociale de la cyberdélinquance?

L'état quantitatif de la cyberdélinquance, fortement relayé par les médias, est un vecteur fort de son image. Ces derniers font toujours montre de statistiques exponentielles en regard de ce phénomène. Généralement, et par analogie, en rapport au danger affiché comme grandissant sur les réseaux publics, il devient facile d'associer à ces faits une image « toute faite » de l'acteur social responsable. Ainsi, une nouvelle forme de délinquance a progressé en corrélation avec le développement du réseau de réseaux, *via* la généralisation de l'interconnexion de l'outil informatique. Le terme « cybercriminalité » s'est peu à peu généralisé, confirmant cette qualification du doyen J. Carbonnier : « *L'évolution des mœurs et des techniques donne matière à de nouvelles formes de délinquances* »[29]. Afin de le vérifier, nous déclinerons le concept éprouvé de la société numérique du risque qui se détermine à travers l'équation du risque de sécurité, et apporte notamment la justification du concept de menace et d'agents menaçants, quant aux pirates informatiques. Nous nous appuierons et détaillerons nécessairement les approches statistiques, les plus connues et reconnues, comme une évidence indispensable à la quantification du phénomène, qui en rend compte et qui est notamment principalement véhiculée *via* les médias.

Nous décrirons également le champ sémantique de la cyberdélinquance, particulièrement ses définitions. En effet, nous nous apercevrons que le phénomène fait l'objet de définitions diverses, utilisées *via* des contextes différents, par de nombreux acteurs, avec des qualificatifs spécifiques, et non forcément pour expliquer des faits identiques, notamment *via* les médias. Nous procèderons tout d'abord à une analyse scientifique synthétique en rendant compte des éléments pertinents de recherche récents permettant de faciliter l'appréhension du domaine de la cybercriminalité et des pirates informatiques. De plus, les actes de piratages informatiques seront éclairés à travers des statistiques officielles internationales récentes relatives à ce phénomène (*CERT*, *Computer Security Institute*, et CLUb de la Sécurité de l'Information française

[29] S*ociologie Juridique* (Carbonnier, 1978).

(CLUSIF)…). Cela permettra de qualifier les pirates informatiques en tant que risque réel puisque ces derniers peuvent être poursuivis pénalement, en cas de passage à l'acte (notamment en cas de dépôt de plainte). Ce cadre législatif strictement prédominant au niveau international préfigure fortement de la représentation sociale formalisée de la cyberdélinquance. Afin de rejoindre notre problématique, et montrer plus en avant cette évidence de la cyberdélinquance, il importera donc d'en afficher le cadre de construction, qui sous-tend à sa réalité.

L'état relevé de la cyberdélinquance nous apporterait finalement une représentation sociale de type « statistico-démonstratif », fortement attachée à son caractère illégal. Un socle de production, pour les images sociales du pirate informatique, comme acteur principal de ce champ, qui peuvent, de fait, observer les mêmes valeurs et demeurer *de facto* résolument singulières. Ainsi, la représentation sociale de la cyberdélinquance semble effective et, par défaut, un effecteur non négligeable de l'image sociale du pirate informatique. Cependant, la définition même de l'acteur social responsable pouvant s'afficher ainsi « reliée » à la représentation sociale de la cyberdélinquance, nous choisirons alors de la considérer et de la traiter comme résolument complexe. Cette inter-relation avec la cyberdélinquance même pose d'ailleurs problème et n'est pas véritablement acquise par le citoyen, elle semble même évoluer en fonction de l'opinion publique, qui intègre plus ou moins facilement cette relation. De cette « caractérisation » sociale acquise ou inconnue, quelle image dominante du pirate informatique se dessine alors ? Quel rapport les médias jouent-ils avec cette représentation ? D'autres mondes peuvent-ils aussi participer à la construction de l'image sociale du pirate informatique ? Plus clairement, est-ce que plusieurs mondes sociaux différents peuvent être à l'origine de la formalisation de différentes significations ? L'investigation de la construction sociale de l'objet « pirate informatique » et des processus/instruments associés demeurent les clés essentielles de la réponse à notre problématique posée. Nous la développerons ainsi, au sein de notre deuxième partie, pour les médias semblant dominants à ce niveau de recherche, pour notre objet.

II – Quelle image nous renvoie une analyse du contexte médiatique entourant le pirate informatique ?

En termes de méthodologie, en amont d'une analyse médiatique, afin de « recueillir » une partie de l'opinion publique face à ces différents constats en regard de l'objet de recherche, nous rendrons compte d'un sondage que nous avons créé et mis en ligne sur Internet, relatif au pirate informatique. De ce sondage, formalisant de nombreuses réponses intéressées et intéressantes, nous analyserons plusieurs critères pertinents concernant notre objet de recherche, corroborant les informations des définitions apportées en première partie (notamment l'inter-relation forte entre la représentation sociale de la cyberdélinquance et l'image sociale du pirate informatique). De fait, nous mobiliserons la théorie des représentations sociales pour mieux comprendre, et tenter de déterminer et d'expliquer le processus de construction de l'image du pirate informatique, à partir de ces résultats de recherche obtenus.

Ce « sondage social » montre les possibles interprétations et images sociales diverses, pour un même objet. En effet, ce n'est pas une mais plusieurs images sociales qui s'affichent alors possibles. Cependant, notre sondage nous a révélé la dominance d'un monde favorisant l'image du pirate informatique, à savoir les médias (fait que nous pouvons aussi valider, d'expérience, avec pour preuve, le dossier de presse établi par nos propres soins, de manière empirique, de 1995 à 2002, relatif à l'objet de recherche et analysé dans cette même partie (voir annexe 9). Nous étudierons donc ce monde médiatique permettant de recueillir les informations nécessaires quant à notre problématique.

Les représentations médiatiques du phénomène marquent de leur importance la formalisation des significations sociales associées à notre objet étudié, notamment lorsque, majoritairement pour chaque citoyen, aucune confrontation directe n'est possible avec le milieu « *underground* » (clandestin, secret). Pour nos recherches, nous nous sommes concentrés sur l'information presse, avec l'analyse du discours relatif à l'objet de recherche. Dans le cadre d'une recherche précédente[30], nous avons été amenés à

[30] *La cyberdélinquance, un risque pour Internet ?* (Humbert, 2003).

effectuer le même type de démarche de mise en indexation et de veille des parutions dans la presse généraliste et spécialisée en informatique, des articles substantiels consacrés à la cybercriminalité, c'est-à-dire ceux présentant Internet comme porteur de menaces. C'est l'exploitation de ce corpus ainsi rassemblé (voir *infra*) qui est proposée ici. Nous avons également privilégié une recherche indexée sur les mots-clés « cybercriminalité » et « pirates informatiques », *via* un abonnement de type « *Google Search* » (http://www.google.com). Cette veille a été entreprise de début janvier 2006 à juin 2006.

Nous nous sommes attachés à relever, classer, annexer et analyser cette documentation. Enfin plusieurs rencontres avec différents journalistes sur le sujet du piratage informatique permettront aussi de renforcer l'étude de la construction médiatique des significations relatives à l'objet de recherche.

Cependant, l'image médiatique n'est pas identifiée comme la seule, et finalement plusieurs images seraient le fait des différents mondes traitant du phénomène, qui génèreraient alors principalement autant d'images singulières du pirate informatique, dans le cadre d'une confrontation d'idéologies bien prononcées. Des images différentielles apparaîtraient, alors, selon les mondes sociaux d'origine concernés. Les significations de chaque monde ouvrant vers des catégorisations particulières, selon le principe de « concurrence » idéologique, ou encore de frontières culturelles très marquées. Un monde pouvant alors aussi favoriser la production, en fonction de la force de la pénétration de ses significations vers le public, de l'image dominante du pirate informatique à travers la société, le cas en l'espèce du monde des médias, en effet, prédominant.

Nous avons donc posé comme postulat le fait que les images caractérisant les pirates informatiques peuvent être formalisées par plusieurs mondes sociaux. Ainsi, d'autres mondes choisis, mis à part les médias, formaliseraient aussi l'ingénierie de l'image du pirate informatique au sens de notre recherche. En regard, il n'existerait pas d'image unifiée, mais plutôt de multiples en fonction des mondes concernés ? Pour ce faire, nous posons alors les images du pirate informatique comme évoluant selon les significations de chaque monde considéré, comme autant de maîtres d'ouvrage de l'objet. En s'appuyant sur le paradigme de l'interactionnisme symbolique, nous considèrerons que les acteurs sociaux construisent la réalité sociale *via* les processus d'interaction,

notamment pour les deux autres mondes investigués, post-médias, afin de répondre à notre troisième question spécifique de recherche. D'expérience, les mondes des experts en sécurité de l'information et des pirates informatiques seront choisis comme participant également majoritairement à la construction des images sociales du pirate informatique.

III – La réalité sociale de l'objet provient-elle de plusieurs images construites *via* plusieurs mondes ?

En comparaison aux éléments recueillis en provenance du monde des médias, notre recherche se focalisera sur les experts du domaine de la sécurité de l'information et des protagonistes principaux des mondes de la cyberdélinquance, à savoir les pirates informatiques, particulièrement sur les significations qu'ils affectent à l'objet de recherche. Nous proposons alors de rendre compte d'une approche cognitive en considérant, « du point de vue de l'acteur », les représentations de ces deux mondes participant à l'ingénierie de l'objet. Afin de parfaire la compréhension des images provenant de ces mondes sociaux, notre méthodologie principale reposera sur l'observation participante, mettant notamment en évidence, durant la rédaction de cette thèse, des différents mandats du champ de la sécurité des systèmes d'information et de la communication (SSIC) que nous avons occupés, principalement au Grand-Duché de Luxembourg, pour cadre de travail : Responsable de la PFI (Plate-Forme d'Innovation) Sécurité du Centre de Recherche Public (CRP) Henri Tudor, Responsable du CAP (Comité d'Accompagnement) PFI Sécurité du CRP Henri Tudor, Président CNLSI (Comité de Normalisation Luxembourg pour la Sécurité de l'Information), Vice-Président ANSIL (Association de Normalisation pour la Société de l'Information), Chargé de Missions CASES (*Cyberworld Awareness & Security Enhancement Structure* – Structure d'amélioration de la sécurité & de la sensibilisation au monde numérique), Secrétaire Général du CLUSSIL (CLUb de la Sécurité des Systèmes d'Information Luxembourg), Chargé de cours pour le Master SSIC de l'Université Paul Verlaine - Metz et pour le Master MSSI (Management de la Sécurité des Systèmes d'Information) de l'Université de Luxembourg, principalement.

Encore une fois, le paradigme de l'interactionnisme symbolique nous permettra de mesurer plus facilement l'adéquation des interactions à l'intérieur des différents mondes choisis pour étudier notre objet de recherche. Au-delà de ce paradigme et afin de nourrir notre réflexion, nous prendrons aussi en compte les liens de notre objet de recherche avec les concepts de l'étiquetage social, de la catégorisation, de la déviance, de la délinquance, et de l'expertise principalement. La préoccupation de cette troisième partie repose principalement sur la participation de chaque monde quant à la construction d'un « imaginaire » du pirate informatique. En effet, pour chacun quelle ingénierie des significations y est associée ? Cette dernière est-elle singulière ou unifiée ? Ces images ne semblent, en effet, pas être formalisées de la même façon par des mondes différents, affectant *de facto* à l'objet des significations diverses.

Le monde des experts SSIC, sera observé de manière participante, en intégrant de nombreux comités, en organisant de nombreuses conférences et meeting, et en nous posant nous-mêmes comme expert de la matière (voir annexe 13). De cette observation, nous pourrons raffiner les résultats de significations et positionnement du monde des experts vis-à-vis de l'objet de recherche. Enfin, le monde des pirates informatiques sera étudié en regard de l' « auto-représentation » de cet acteur principal de la cybercriminalité. Son monde sera étudié de manière qualitative, privilégiant le travail de terrain (entretiens, investigations, échanges directs et indirects d'information, etc…) afin de développer une approche compréhensive et cognitive de cet acteur social, et qualifier plus particulièrement sa propre définition. L'ensemble de ces données nous amènera, enfin, à rendre compte d'un cas d'application concret de l'intégration des significations de notre objet de recherche, à savoir l'application de notre travail à la dimension d'un pays, en l'espèce le Grand-Duché de Luxembourg. Ainsi, dans le cadre du projet de recherche R2SIC[31] qui a « abrité » l'ensemble de notre travail de doctorat, nous avons mené l'étude de mise en place d'un observatoire des menaces IT pour le Grand-Duché de Luxembourg, en tenant compte de la problématique de la réalité sociale du pirate

[31] R2SIC : Recherche pour la Sécurité des Systèmes d'Information et de la Communication, projet de recherche conventionné entre le Ministère de l'Economie et du Commerce extérieur et le Centre de Recherche Public Henri Tudor – Grand-Duché de Luxembourg.

informatique, à partir des résultats de recherche de nos différents axes de recherche traités.

Cette étude a profité des évolutions et questionnements scientifiques divers posés par nos avancées, notamment en reprenant les bases du sondage établi pour notre question spécifique étudiée en deuxième partie (voir questionnaire en annexe 6). Les résultats ont été validés et transmis *via* le Comité d'accompagnement de la Plate-Forme d'Innovation Sécurité du CRP Henri Tudor. Ils ont permis de servir de base pour la réflexion de mise en place d'une équipe luxembourgeoise de réponse sur incidents et de sécurité informatique[32]. Ce projet correspond à la réalisation concrète du deuxième pilier du Plan Directeur National de la Sécurité des Réseaux (Luxembourg), à savoir la phase de « réponse » face aux menaces numériques. Cette étude a permis d'éclaircir le domaine et la perception des acteurs responsables. La mesure de l'importance des faits au niveau international a dirigé l'évolution en cours de la prise en compte du phénomène au Grand-Duché de Luxembourg, qui, à ce jour, ne dispose pas de structure de réponse sur incident au niveau national. Ainsi, l'importance de la réalité statistico-démonstrative, de l'illégalité des actes, a été analysée, tout autant que la dimension « nébuleuse » du cybercrime et de ses contours difficiles à définir, qui furent aussi spécifiés et reconnus durant l'étude. Il appert, par exemple, des résultats qu'il ne peut être retenu comme concevable qu'aucune statistique ne soit relevée quant au phénomène au niveau national luxembourgeois. En effet, un élément déterminant de la prospective quant au pirate informatique repose aussi sur la sensibilisation au personnage qui demeure la plupart du temps peu connu par le citoyen, mais aussi en entreprise, déterminant de fait la nécessaire implication au fait, en en facilitant l'accès à la connaissance, via aussi une quantification et une qualification de la réalité nationale des faits. Notre étude, à ce titre, propose un nouvel accès à celle-ci, en favorisant la vision de l'ensemble des mondes vis-à-vis de l'objet, afin de ne pas en restreindre la compréhension. Notre but étant de ne pas montrer une évidence, mais une vérité sociale.

Puis, à partir de ces différentes données obtenues, observons-nous finalement une bataille d'images créées ? Pouvons-nous vérifier l'existence de passerelles entre les

[32] Usuellement dénommés CSIRT-LU soit *Computer Security Incident and Response Team Luxembourg*.

frontières des significations émanant de chaque monde, un interactionnisme symbolique actif entre les mondes de la cyberdélinquance, et vérifier alors ce fait comme solution pour uniformiser l'image sociale du pirate informatique. Cela favoriserait ainsi la diffusion d'une image singulière à terme (et son lien avec une image considérée comme véritable : partagée)? Les points d'interaction entre les mondes permettent-ils de « lisser » les images, et permettent-ils un consensus, une classification unique?

Les mondes participeraient à l'image d'un même objet mais, pour résultat, ne formaliseraient pas la même image. Les processus d'ingénierie des significations ne seraient donc pas les mêmes. Les différences apparaissent surtout dès lors que le monde concerné considère l'objet comme un produit fini ou bien en construction, et traite finalement de l'objet *via* une approche processus ou bien via une approche état. L'absence d'une vision interactionniste symbolique entre les mondes empêcherait aussi une construction unifiée. Nous noterons les points de rupture dans la construction, en provenance des mondes, et de fait, une quasi impossible uniformité car les visions état et processus se mélangent et se confrontent. La tendance vers l'homogénéité, vers la catégorisation entraînerait alors la naissance d'une pyramide de la classification des pirates informatiques. Ainsi, de la catégorisation par consensus, des phases d'« objectivation » et d'« ancrage » des significations communes pourraient naître, et la représentation sociale du pirate informatique s'établir et devenir durable.

L'évolution continue de ce phénomène, au gré des acteurs et des changements technologiques, induit un axe de recherche plutôt orienté « processus », car supposé à l'opposé d'un état figé (développé en première partie pour la cyberdélinquance). Ainsi, selon notre analyse, autant de mondes participeraient à l'ingénierie des images sociales du pirate informatique. Si un monde social est défini comme un réseau d'acteurs coopérant dans l'accomplissement d'activités spécifiques, le chercheur est tenu d'identifier qui agit avec qui, pour produire quoi, selon quel degré de régularité, et sur la base de quelles conventions. Ainsi approchées, les activités coopératives peuvent être échelonnées sur un axe, depuis les plus routinières, formellement organisées et strictement répétées, jusqu'aux plus instables, rapidement changeantes. L'une des conséquences de ce mode d'analyse est de renoncer à la valeur opératoire des

descriptions qui établissent des distinctions strictes et des classifications étanches. H.S. Becker dans les *Mondes de l'art*[33] ne classifiera (typologie) pas, mais intégrera dans son chapitre huit, une distinction selon le degré d'intégration au monde de l'art. Le livre développe en réalité, et dans la ligne de mire de la théorie de l'étiquetage à laquelle Becker a attaché son nom, toute une réflexion sur la façon dont les acteurs s'accordent ou s'affrontent pour inventer des catégories et des classements, et tracer des frontières (notamment entre art et non-art). Dès lors qu'ils sont interprétés comme autant de processus mobilisant des acteurs, les faits, les valeurs et les significations qui en résultent peuvent changer graduellement ou radicalement comme se modifient les réseaux qui les ont produits. Les concepts de coordination et de coopération sont omniprésents dans l'interprétation beckerienne. Notre recherche convient de raisonner ainsi au cœur des mondes de la cyberdélinquance afin de déterminer les processus d'ingénierie appliqués aux images sociales du pirate informatique. Observer cette construction afin d'en déterminer une structuration permettra de répondre à notre problématique.

A ce titre, les sources d'informations formées par l'ensemble des médias français, notamment la presse écrite, précisent, depuis l'avènement d'Internet en France (fin 1994)[34], que le réseau de réseaux constitue également un tremplin pour de nouvelles activités criminelles qui s'attaquent soit directement au médium, soit l'utilise pour commettre des infractions de droit commun, fondues dans une dénomination commune : la cybercriminalité. Celui qui ne sait pas, s'en tient à de l'information relayée et formalise une image, une représentation de l'objet concerné. Il en va ainsi de la perception du pirate informatique au cœur de la société traditionnelle. En effet, combien d'entre nous les connaît véritablement, les rencontrent ou les ont rencontrés, discutés sur le sujet de leur vocation ?

Il convient donc de s'interroger, les points de ruptures de signification entre les mondes déterminent-ils un kaléidoscope d'images du pirate informatique ? Quels impacts traduisent ces diffusions de significations en provenance des différents mondes ? L'opinion publique jouit-elle de la vision croisée formalisée par l'ensemble des mondes ?

[33] *Les Mondes de l'art* (Becker, 1992).
[34] Correspond au développement des premiers abonnements disponibles pour le grand public en France.

Notre étude propose un « élan » de compréhension en prenant la mesure des différents registres permettant d'établir les images sociales du pirate informatique. Loin d'établir comme nécessaire cette mesure, notre travail vise à faire reconnaître l'existence de plusieurs réalités selon le point de vue de l'acteur social concerné, selon le monde qu'il représente, selon l'image qu'il défend. Nous avons pu, à travers notre expérience, être à la croisée des mondes que nous avons définis pour la cyberdélinquance. Il appert finalement, qu'aucun monde ne semble détenir la vérité, la véritable image, mais sa vérité, sa véritable image, ce qui « justifie » de l'existence propre de chaque monde et de l'univers même des mondes de la cyberdélinquance, comme un univers d'interactions, pas forcément partagés. Il s'agit d'une justification de l'intérêt d'avoir aussi posé notre étude tel que, comme base de compréhension, car souvent, l'image du pirate informatique apparaît de manière unilatérale, antagoniste, renvoyant les significations des uns aux autres… puisque *« L'homme est la mesure de toute chose* »[35] et le demeure face à l'objet.

Nous proposons donc une vérité de l'objet à travers et en tenant compte des différentes significations, en tout état de cause une matrice compréhensive pour y parvenir, que nous développerons en conclusion. Afin de mieux percevoir les attributs et fonctions de l'objet de recherche nous proposerons une prospective innovante permettant d'aller plus en avant dans la compréhension de l'objet de recherche. Nous déterminerons un pont supplémentaire et spécifique en terme de recherche. Ainsi, nous spécifierons comme important de « creuser » le monde des pirates informatiques, non en tentant de pénétrer les réunions opaques ou même de devenir délinquants, mais plutôt de rencontrer, à terme, *via* une matrice de recherche adaptée, les acteurs effectivement interpellés et condamnés pour des faits de piratage informatique. La prospective passe immanquablement par la meilleure compréhension directe de l'acteur social, « finement » écouté. Ainsi, au-delà des principales frontières entre les mondes sociaux, différents ponts apparaissent possibles et surtout non négligeables entre ces derniers. Il appert surtout que sans prospective sur l'objet de recherche, les classifications « exagérées » peuvent devenir possibles, ainsi que l'ouverture vers toutes sortes d'images sociales. La prospective s'affiche alors comme une ouverture vers l'homogénéité représentative entre

[35] Platon – *Protagoras.*

les mondes de l'objet de recherche. Aucune vérité n'est juste, et il est certainement plus juste de rendre compte de chaque vérité.

Enfin, les images sociales du pirate informatique sont souvent calquées sur les images médiatiques. La prédominance des médias masque une partie des significations sociales. Cependant, elles sont aussi une transcription de la réalité (ou parfois d'une partie seulement).

La réalité du pirate informatique se fond à travers le prisme des mondes qui en composent l'image, à savoir ceux qui lui affectent des propriétés, de manière constructive. Propriétés qui peuvent se rejoindre ou être antagonistes, ce qui forme des ponts ou des oppositions de représentation de l'objet social concerné. Pour exemple, l'image sociale du pirate informatique, à travers la représentation sociale de la cyberdélinquance, est souvent présentée comme un état et donc toute faite, notamment via les médias, avides de sensationnel. Cependant, cette image pour être réelle devrait s'attacher à prendre en compte les représentations des mondes qui en produisent l'image, le résultat n'étant plus un état mais un processus, continuellement en construction, mettant en évidence des ponts de connaissance, mais aussi des oppositions entre les mondes, une déclinaison « d'images sociales », avec souvent pour résultat direct, la difficile et mauvaise perception du citoyen vis-à-vis de l'objet social. Le processus engagé devrait tout de même évoluer, à très long terme, vers un objet représenté socialement. Cependant, pour cela, chaque monde doit pouvoir exprimer ses significations, se faire comprendre, et reconnaître, ensuite seulement les différentes images pourront alors se confronter entre elles, pour qu'à terme, il n'en reste qu'une ?

PREMIERE PARTIE

Titre I - Représentation sociale de la cyberdélinquance : illégalité et contexte statistico-démonstratif pour base structurante des significations sociales du pirate informatique

Cette première étape permettra de rendre compte de la réalité des faits quant au contexte entourant notre objet de recherche. Il importe dans un premier temps de mettre en évidence la réalité du risque que représente la cyberdélinquance, notamment dans son acception généralisée de menace préjudiciable. Ensuite, nous définirons de manière sémantique ce qu'englobe le terme cyberdélinquance, en présentant les derniers résultats de recherche en rapport, ainsi qu'un historique rapide. Nous montrerons, enfin, la structure des instances de prévention à la cyberdélinquance, les pratiques récentes d'attaques techniques, ainsi que leur pertinence statistique. Nous pourrons ainsi rendre compte d'un état de la cyberdélinquance, posée comme domaine spécifique dans lequel évolue le pirate informatique, et de facto les images sociales associées. Nous visons à déterminer si les résultats apparaissent comme suffisamment formalisés et, dans le même temps également partagés par un groupe de manière consensuelle. A ce titre, nous nous interrogerons sur cet espace propre, pour vérifier si ce dernier peut apparaître comme le lien structurant logique de lieux de production des significations sociales de notre objet de recherche. Notre approche comprend la prise en compte de la représentation sociale de la cyberdélinquance comme « producteur » des significations sociales (ou images sociales) du pirate informatique, via des dispositifs à déterminer.

I – L'évidence des menaces numériques

Nous rendrons compte, en amorce, de l'évidence du risque que représente la cyberdélinquance, notamment dans son sens généralisée de menace préjudiciable. Ce domaine est, en effet, principalement présenté comme fortement interconnecté avec le domaine du risque numérique. Nous exposerons la société numérique du risque, puis nous poserons le risque comme un objet social construit au cœur de la société, son indissociable lien avec la société de l'information, et enfin la réalité technique de ces menaces numériques. Nous détaillerons ainsi les différents types d'actions cybercrimelles, et les diverses pratiques d'attaques comme autant de marqueurs pour établir la représentation de la cyberdélinquance.

1) La société numérique du risque

Au fil du temps, le risque s'est imposé comme une entrée pertinente pour comprendre les sociétés contemporaines et surtout les défis auxquelles elles doivent faire face. Ces dernières années, la notion de risque a ainsi permis de qualifier de nombreux domaines, notamment pour mettre en avant des situations dangereuses qu'il convient d'éviter, par exemple pour la préservation de l'environnement ou encore de la santé publique. Depuis, cette notion de risque a été appréhendée par le citoyen et a généralement permis de mettre en place des outils ou solutions pratiques, telles que les assurances ou l'amélioration de diverses mesures et procédures de sécurité.

Parallèlement à cette qualification au sein de la société prise au sens traditionnel, où l'objet du risque apparaît socialement « construit », qu'en est-il pour la société de l'information, et l'usage des technologies associées? « *La société de l'information désigne une société dans laquelle les technologies de l'information jouent un rôle central. Elle est en général placée dans la continuité de la société industrielle* »[36]. A ce titre, est-il possible de tenir, pour cette dernière, les mêmes raisonnements et principes retenus pour la société traditionnelle ? De même, en conséquence de ce phénomène d'apparence complexe, quelle est la sensibilité de l'utilisateur des technologies numériques quant aux risques de sécurité ?

Les médias, les experts et les diverses statistiques font souvent état de risques exponentiels au cœur de la société de l'information, montrant notamment une progression alarmiste de la menace « *underground* », à caractère transnational. De fait, la lutte contre la cybercriminalité et la gestion des risques associés s'affichent, aujourd'hui, comme des enjeux majeurs pour la sécurité. Cependant, cette mouvance « *underground* » demeure délicate à appréhender, car imperméable et relativement peu loquace. Il s'agit pourtant de l'élément caractéristique et déclencheur de la formalisation du risque au cœur de la société de l'information. Ainsi, le plus souvent, cet « ennemi invisible » (du fait de son caractère confidentiel), fait de facto l'objet de représentations sociales. L'objet social ainsi caractérisé, est-il aussi solidement construit tel que le risque traditionnel au cœur de

[36] http://fr.wikipedia.org.

la société ou bien demeure-t-il en construction, cela au travers des différents mondes sociaux qui les caractérisent ?

Nous montrerons l'évolution du risque et de sa perception, aboutissant à l'omniprésence du risque dans la société actuelle. Il sera présenté comme un objet social pouvant prendre des formes multiples en fonction du domaine d'application, mais sera considéré par la suite comme un objet social construit et maîtrisé par les différents acteurs de la société. Dans un second temps, nous nous intéresserons plus spécifiquement aux risques liés aux TIC. Nous identifierons la transposition des risques « traditionnels » présentés aux spécificités du monde virtuel de la société de l'information.

Le risque, un objet social généralement construit *via* la société

- Définition du risque et origine

Le terme « risque » proviendrait de l'italien *risco* (ou de l'espagnol *riesgo*), mot dérivé du latin *resecum* (« ce qui coupe »), qui désignait en premier lieu l'écueil qui menaçait les navires, puis, plus généralement, tout danger encouru par les marchandises en mer. L'autre origine possible du terme « risque » est *rixicare* (« se quereller », qui a donné « rixe ») et qui évoque également le danger. Cependant, risque n'est pas simplement un synonyme de danger. La première étymologie l'associe à une volonté d'entreprendre tout en maîtrisant les coups du sort. De manière générale, on l'identifie de nos jours comme un « *danger éventuel plus ou moins prévisible* » ou, dans la sphère économique, comme « *la probabilité d'un événement négatif combiné avec l'impact chiffré qu'il peut avoir* ».

J. Bouyssou[37] précise qu'au XVIIIème siècle, le risque était peu évoqué. Puis ensuite, le calcul de probabilités s'est répandu et a permis ainsi de mieux percevoir le risque. Le concept de gestion des risques (ou *risk management*) a très certainement fait son apparition à la fin des années 50 aux États-Unis dans le domaine financier, en relation avec des questions d'assurance. Le risque était alors devenu calculable. En effet, pour

[37] *La théorie générale du risque* (Bouyssou, 1997).

qu'un assureur puisse accepter alors de garantir un aléa[38], il devait pouvoir tarifer le risque, c'est-à-dire calculer une prime d'assurance. Le risque était alors défini comme étant la probabilité d'apparition d'un événement indésirable multipliée par la perte économique résultant de cet événement.

La gestion des risques a ainsi longtemps été considérée comme la dimension probabiliste d'une perte financière au regard de la question d'assurance et ne jouait donc qu'un rôle périphérique dans la plupart des secteurs d'activité. A partir des années 90, les notions de risque et de gestion des risques ont commencé à s'étendre à de nombreux autres domaines, citons notamment l'environnement, la gestion de projet, le marketing ou encore la sécurité informatique, à tel point que l'on considère actuellement que la majorité des processus et activités des organisations peuvent être vues sous l'angle du risque, devenu ainsi un outil d'aide à la décision en contexte d'incertitude.

La notion de « risque » s'est donc progressivement transposée au sein de la société. Actuellement la notion de « sociologie du risque » est en plein essor. Selon le sociologue allemand Ulrich Beck, nous passons d'une société industrielle, où le problème central était la répartition des richesses, à une société centrée sur la répartition des risques, déterminant le concept de « *société du risque* ». Autrement dit, le risque n'est plus une menace extérieure, mais bien un élément constitutif de la société. J. Peretti-Watel[39] confirme cette émergence et met en avant le caractère paradoxal d'une société que l'on décrit comme de moins en moins dangereuse, mais de plus en plus risquée. Il considère que : « *le propre du risque est de proliférer* ». Pour lui, un monde plus sûr peut aussi s'avérer plus risqué. Il considère un risque comme un danger d'un type bien particulier : un danger aléatoire, sans cause. C'est un danger dont il s'agit moins d'imputer les occurrences passées à des fautifs que de prévoir les occurrences futures. Ces nombreuses recherches sociologiques, associées à ce domaine, pose le concept de risque comme étant de manière globale socialement représenté.

[38] Terme spécifique désignant un événement source de risque dans le domaine de l'assurance.
[39] *La société du risque* (Peretti-Watel, 2001).

- Le risque, un objet social construit au sein de la société

La société moderne est actuellement exposée de manière permanente à des risques conduisant à des décisions en lien avec ces derniers. Pour reprendre l'exemple de l'assurance, applicable à l'ensemble de la société, chaque assuré va donc appréhender les risques qu'il court et sélectionner une assurance en lien avec ses besoins. A noter que dans certains cas, cela peut même être réglementairement obligatoire.

Les risques sanitaires sont un autre exemple pertinent de l'omniprésence de risques au sein de la société. Ils font l'objet d'une médiatisation très forte, tant au niveau des journaux, de la télévision ou d'Internet, médium à qui l'on doit une démocratisation de l'accès aux connaissances en général. On y croise souvent, notamment sur des forums, des personnes contestant ouvertement les approches officielles en matière de prévention du risque. Par exemple, certains mettent en doute l'efficacité de programmes de prévention ou de dépistage de maladies graves en leur opposant, notamment, des approches offertes par les médecines alternatives.

L'écologie et l'environnement sont également des domaines où le risque constitue un des paramètres incontournables. Pour répondre à cette préoccupation dans ces domaines, la communauté scientifique a d'ailleurs développé le concept du « principe de précaution ». Qu'il s'agisse de ressources naturelles non renouvelables ou d'atteintes à l'environnement sous forme de pollutions, le débat se structure désormais autour de quatre questions clés[40] :

- Le caractère multidimensionnel des problèmes, qui ne permet plus de distinguer la sphère économique de la sphère naturelle et s'inscrit dans le phénomène général de mondialisation.
- Le souci de répartir avec équité le bien-être, non seulement entre les individus actuels mais aussi, ce qui est plus difficile encore, sans pénaliser les générations futures.
- Le caractère apparemment irréversible des conséquences de comportements ou de choix actuels.

[40] *Encyclopædia Universalis.*

- L'incertitude très large concernant la gravité réelle de ces choix ou comportements mais aussi les préférences des générations futures.

Ces quatre aspects, et notamment les deux derniers, donnent naissance au principe de précaution : même si le pire n'est pas certain (notion d'incertitude), la possibilité d'un risque majeur (irréversibilité) doit guider la démarche. Tout citoyen est concerné par les risques liés à l'environnement et se doit alors de respecter le principe de précaution.

La prégnance du concept de risque à l'ensemble de la société a même conduit à l'émergence récente d'une « science du risque » : les *cyndiniques*. Il s'agit d'une science plurielle qui revendique une approche « transdisciplinaire » (incluant toutes les sciences humaines, mais aussi celles de l'ingénieur) qui prétend s'appliquer à une très large gamme de risques, dont les risques technologiques. Les *cyndiniques* envisagent de constituer une véritable « *Encyclopédie du Danger* », illustrant de façon caricaturale un aspect du succès contemporain de la notion de risque, notamment la prolifération d'experts qui font des risques le « carburant » de nouvelles professions. Cette nouvelle science est née en 1980 et il existe notamment un institut européen de cyndiniques (IEC).

J. Peretti-Watel admet que l'homme est capable de se projeter dans l'avenir, qu'il a donc acquis une culture du risque. Or cette culture se heurte aujourd'hui aux risques technologiques majeurs, apparus dans la seconde moitié du XXe siècle : catastrophes nucléaires, pollution de l'air, de l'eau et des sols (auxquels nous pouvons adjoindre les entraves appliquées au réseau de réseaux Internet). Ces derniers font souvent l'objet de débats publics au cours desquels se confrontent experts et profanes, qui revendiquent de plus en plus une participation réelle aux décisions politiques sur ces questions, et souhaitent une démocratisation de la gestion de ces nouveaux risques majeurs. Ce phénomène semble également se vérifier *via* des articles de presse qui apportent le débat sur la place publique. Il met également en avant le concept de la prolifération du risque qui est d'abord verbal. Celle-ci résultant avant tout des efforts d'une profession : « *Les assureurs ne se contentent pas de constater passivement des risques, ils cherchent à étendre constamment leurs champs d'activité en créant des risques, c'est-à-dire en définissant comme tel des dangers et en proposant de les assurer* ».

Via ces exemples empiriques, le risque dans la société traditionnelle semble être devenu un objet socialement construit, à savoir « *socialement acquis dans la perspective*

d'un groupe, qui l'intègre ensuite à ses pratiques sociales ou à son système d'appréhension du monde, modélisant un cadre de vie déterminé »[41].

Corrélativement, le risque semble avoir aussi pour champ d'application la société de l'information. En effet, les médias présentent constamment les dangers du piratage informatique et ses conséquences néfastes, notamment pour l'entreprise, et tout utilisateur IT, qui doivent alors s'en protéger. Les assurances se sont d'ailleurs récemment positionnées pour proposer des polices répondant aux risques informatiques, notamment aux intrusions réseaux et aux risques de sécurité de l'information.

Quid du risque au sein de la société de l'information ?

La société de l'information, est une continuité de la société prise au sens traditionnel et usant des TIC. Cette définition permet de déterminer comme principal périmètre d'usage actuel : Internet, comme réseau de réseaux formalisant un vecteur de communication universel et en développement constant. Nous avons établi précédemment que la notion de risque paraît socialement acquise au cœur de la société traditionnelle, et que des solutions ont été identifiées et mises en œuvre pour s'en prémunir. Ce premier constat nous permet-il à présent de transposer cette analyse à la société de l'information et en particulier à Internet ?

Risque et société de l'information

Historiquement, Internet et ses multiples composants informatiques, n'ont pas été développés de manière sécurisée. Les supports logiciels et matériels étaient et sont restés empreints de nombreuses failles de sécurité, qui peuvent présenter en cas d'exploitation malveillante un danger de pérennité pour ces moyens de communication et d'information. Très tôt, la notion de risque « numérique » a été liée à l'incident de sécurité pouvant atteindre le système informatique.

1988 marque le point de départ d'une prise de conscience internationale lorsque Robert Morris, fils d'un des principaux scientifiques du *National Computer Security Center*, « lâche » le premier ver sur Internet. Conséquence : 6000 machines

[41] *Les représentations sociales* (Mannoni, 2001).

interconnectées sont infectées. Cet « évènement » constitue le premier déploiement majeur d'un ver au sein d'une infrastructure globale IT à la fin des années 80. « *Soudainement, les gens ont pris conscience d'un fort besoin de coopération et de coordination entre les administrateurs systèmes et les gestionnaires IT afin de traiter des cas comme ceux-ci. Et quelques jours après l'incident « Morris » l'Agence des Projets de Recherche Avancés de Défense*[42] *a mis en place le premier CSIRT : Centre de Coordination CERT (CERT/CC - (Computer Emergency & Response Team – Coordination Center)), établi à l'Université Carnegie Mellon à Pittsburgh (Pennsylvanie) »*[43].

Ainsi, l'incident du ver Morris fut le déclencheur de prise de conscience des risques numériques de sécurité présents au cœur de la société de l'information, et le point de départ de la mise en place des structures de réponse sur incidents en charge de recenser et de traiter ces derniers. Les premiers traitements d'incidents de sécurité numériques prévoyaient un rapport qui formalisait les faits, en s'attachant à décrire l'attaque, la détermination de l'exploitation de la faille de sécurité (la vulnérabilité), le préjudice subit et enfin, les contre-mesures prises ou à prendre. Depuis, avec l'explosion d'Internet et le développement du tout numérique à l'usage de tous les citoyens, les relevés d'incidents se sont multipliés de manière exponentielle (cf première partie – III - 2). Le monde des experts de la sécurité informatique a tenté de prévoir et de prévenir ce type d'incident numérique, à l'aide de ce que l'on nomme couramment « l'équation du risque », concept théorique très utilisé dans le monde des experts en sécurité de l'information :

« RISQUE = MENACE * VULNÉRABILITÉ * IMPACT ».

Bien que son expression s'apparente à une équation mathématique, elle signifie qu'un risque est la composition probabiliste d'une menace, d'une vulnérabilité et d'un impact. De façon plus détaillée, la menace, source du risque, se présente comme la possibilité d'attaque d'un élément menaçant externe au système (pirate informatique, virus…), le plus souvent totalement incontrôlable et sur lequel il est difficile d'agir

[42] Usuellement dénommée DARPA soit *Defense Advanced Research Projects Agency*.
[43] *Enisa ad hoc Working Group on Cert Cooperation and Support*, 2006.

directement. La menace est donc purement potentielle. Les mesures de sécurité à mettre en place ne relèvent pas de l'utilisateur des technologies de l'information, mais des pouvoirs publics qui ont les moyens de légiférer en cas de besoin face aux menaces IT. La vulnérabilité se caractérise par une faiblesse ou une faille dans la sécurité (absence de contrôle d'accès, anti-virus non mis à jour…) d'un Système d'Information (SI) maîtrisable. Cette vulnérabilité est propre au SI, ce qui la rend plus facile à identifier. Elle représente l'élément du risque sur lequel vont se concentrer les mesures de sécurité pour la corriger. Aujourd'hui, les mises à jour de sécurité des systèmes informatiques existent et sont largement diffusées pour améliorer les systèmes vulnérables. Enfin, l'impact représente la conséquence du risque sur l'utilisateur et ses objectifs. Il se caractérise par le préjudice subi, pouvant être de nature diverse : perte de données, rupture de communication, perte financière, de contrats, etc.

De nos jours, les systèmes d'information sont très rarement visés par erreur ou par simple challenge[44]. La cible des menaces est désormais le plus souvent l'information supportée, qui au travers de la criminalisation « galopante » d'Internet, est devenue très lucrative. Plusieurs indicateurs permettent d'en rendre compte et de dresser le bilan de ces faits (cf. première partie - III – 2).

Menaces numériques : une réalité technique

Les menaces, en tant que réalité technique, se mesurent souvent en terme d'impacts financiers. De nombreux marqueurs fournissent, en effet, des preuves tangibles de cette activité. Ainsi, les incidents de sécurité, formalisant l'exploitation d'une vulnérabilité par une menace (formant une attaque), sont largement diffusés et disponibles pour tout public sur Internet. Le *Federal Bureau of Investigation* (FBI - Etats-Unis) évalue, par exemple, le coût total du cybercrime pour la seule année 2005, à 67 milliards $. De même, le rapport du CERT-CC rend compte pour la même année, de 150 millions $ de pertes, *via* une enquête réalisée sur la base de 819 réponses. Afin de contextualiser ces chiffres, nous pouvons noter que le CERT-CC a enregistré de 1988 à 2003 près de 319 992 incidents de sécurité numérique, sachant qu'un incident peut

[44] Communément dénommé « *hacking* ».

impliquer un site ou plusieurs centaines, et que de plus, ce dernier peut apparaître de manière continue sur une grande période. Plus récemment (2006), le CERT-CC a produit un rapport nommé « *e-crime watch survey*» (cf. *supra*), validant ces faits : ainsi sur un échantillon de 434 entités aux Etats-Unis, globalement le nombre d'incidents de sécurité numérique par répondant baisse (136 en 2004, 86 en 2005, 34 en 2006), alors que dans le même temps, les préjudices financiers associés augmentent de façon significative (en moyenne par répondant 704.000 $ en 2006 contre 507.000 $ en 2005).

2) Types d'actions cybercriminelles

Afin de mieux anticiper la connaissance de la cybercriminalité et sa « sédimentation sociale », il convient de présenter la démarche des actes qualifiés comme tels. Nous tiendrons compte des différentes pratiques d'attaques, entre le médium informatique utilisé en tant qu' « outil » du crime informatique et celui qui est véritablement pris pour cible. Auparavant, nous procèderons à un *focus* sur les pratiques et techniques innovantes d'attaques déployées par les pirates informatiques réseaux, en termes de méthodologies d'attaques (de manière chronologique).

Méthodologie

- La prise d'empreinte

Généralement avant d'attaquer une cible particulière, le pirate informatique procède à un relevé de toute information pouvant mener à une cartographie de l'organisation qu'il vise. Par ce fait, il s'approprie l'objectif. Pour exemple, à Los Angeles, *Intense School* propose un séminaire intitulé : « le *hacking*, ou l'art de pénétrer les systèmes informatiques (« *Hacker College*»). Son Directeur précise : « *Le premier jour, les étudiants apprennent des techniques gratuites et légales pour trouver des informations sur des entreprises, leurs dirigeants et les systèmes informatiques qu'elles utilisent. Avec quelques efforts, ils ont par exemple découvert qu'un Directeur Général d'une grande entreprise possédait un site personnel sur les guitares et qu'une autre*

grande société utilisait encore des systèmes connus pour être particulièrement vulnérables aux attaques des hackers »[45].

Nous sommes en présence de relevés d'informations stratégiques pour le pirate, recherchant des angles d'attaques différents, lui permettant d'atteindre la cible par des chemins détournés. Cela lui évite un repérage direct en frontal de la cible en privilégiant une approche en spirale. Souvent, des pirates « professionnels » ne reculent devant rien, tel que faire les poubelles de la cible, envoyer des faux mails, ou encore prendre contact avec des proches de la cible par exemple (Notion de *social engineering* - Ingénierie sociale -). Le *social engineering* consiste en toute procédure de recherche de renseignement non technique. Il s'agit d'une approche sociale, généralement le pirate contacte alors la cible ou son environnement direct en frontal.

Le pirate cherche ainsi à établir un profil précis de la cible. Tout est bon à prendre au départ ; plusieurs petites informations peuvent finaliser un renseignement utile pour la suite des activités pirates. L'intérêt se porte au départ sur Internet. Quelle visibilité offre la cible : serveur web (nom de domaine), contact mail, organigramme, historique, localisation physique, recrutement en cours (peut permettre d'entrer au cœur de la cible), cartographie réseau (sous-réseau), services réseau (serveurs accessibles)…etc. Le premier jet du pirate doit permettre d'aller plus en avant en déterminant les systèmes d'exploitation utilisés et les vulnérabilités potentielles à exploiter. Le pirate tentera d'obtenir également les protocoles réseaux utilisés et des informations sur le matériel d'interconnexion réseau (routeurs, *switchs*, *firewalls,* etc…). Une attention particulière peut être portée sur les outils de connexion à distance (et notamment la recherche/exploitation de mots de passe faibles, ou laissés par défaut (de type constructeur)). Le pirate doit aussi, avant toute chose, déterminer le périmètre de l'empreinte souhaitée. Tout élargissement est possible, mais pas forcément réalisable. Ainsi, généralement le pirate se limite au site principal (correspondant au siège de l'organisation) ou à certains sites ciblés. En fonction de ses recherches sur la cible, le périmètre du pirate peut évoluer, notamment lors des recherches sur Internet. Le pirate se

[45] In Libération (24/06/04), Dave Kaufman.

focalisera notamment sur les informations centrales de la cible, par exemple le site web central qui affiche le plus d'informations utilisables.

Toute information nominative est généralement bonne à prendre pour le pirate, notamment les points de contacts (adresses, photos, mails, téléphones, etc…), les adresses physiques (siège, dépôts, filiales, etc…), les autres serveurs web ou autres services associés (serveurs ftp (*file transfert protocol*), wiki (interface *open source* de services de développement web), etc…). Toute visibilité offerte va alors l'intéresser. Ainsi, la rencontre physique de personnes ayant été identifiées par photo disponible, par exemple sur Internet, est parfois effectuée par le pirate afin de faciliter ensuite l'entrée au cœur de la cible. Souvent, le pirate cherchera plus en avant des commentaires particuliers en étudiant de près le code source du site web (configuration du site web). Les recherches *via* les moteurs ou méta-moteurs de recherche sont également légion. Il s'agit de l'utilisation des sources ouvertes ; ainsi par exemple un pirate pourra à loisir faire des recherches sur des personnes identifiées sur le site web de la cible et effectuer des recherches pour localiser par exemple une page personnelle ou une activité quelconque au sein d'un forum ou sur *Usenet*.

La recherche de type presse peut aussi constituer une source d'informations non négligeable. Parfois, le pirate brosse des sites d'informations économiques afin de vérifier la santé financière de la cible. Des mises en évidence de fusions ou acquisitions récentes peuvent renseigner sur de nouvelles infrastructures réseaux, voire permettre l'élargissement de la cible, ou encore permettre de pointer et de rencontrer de nouvelles ressources humaines.

- Identification réseau

En premier lieu, le pirate doit procéder à l'identification des noms de domaine qui représentent la présence de l'organisation ciblée sur Internet. Le but de l'identification est généralement la découverte des réseaux associés, mais aussi de déterminer si la cible est son propre hébergeur ou si le site est délocalisé (*outsourcing*). Des informations nominatives de personnes « de contacts » sont à ce titre des éléments intéressants pour le pirate informatique. Pour ce faire, les outils sont nombreux afin d'interroger les bases de données de type « *whois* » (déterminant l'identité d'une adresse IP ou d'un nom de

domaine). Les sources de ces identifications sont publiques et souvent bien renseignées. Les bases de données suivantes sont communément utilisées :

- www.ripe.net, (attribution adresses IP (Internet Protocol) pour l'Europe)
- www.apnic.net (attribution adresses IP pour Asie pacifique)
- www.arin.net (*American Registry for Internet Numbers*).

- Recherches DNS :

La pratique d'interrogation du serveur DNS (*Domain Name Server*) est courante après avoir identifié les domaines IP de la cible. Le serveur DNS permet une correspondance entre l'adresse IP et le nom du domaine. Un serveur DNS mal sécurisé peut fournir des informations privées de l'organisation. En effet, les pirates informatiques tentent dans la plupart des cas, d'exploiter (ou du moins tester) la faille d'autorisation des utilisateurs Internet non validés à exécuter un transfert de zone DNS. Un grand nombre de serveurs DNS sont encore mal configurés et fournissent une copie de la zone à quiconque la demande. Ainsi en récupérant les informations d'adresse IP internes, le pirate récupère ainsi une cartographie complète du réseau interne de la cible (utilisation de la commande « *nslookup* » par exemple).

- Recherches Mail Exchange (MX) :

En pratique le pirate cherchera également à déterminer la localisation du serveur mail (gestionnaire de courriels) de la cible. En effet, parfois le courrier électronique est géré sur le même système voire le même réseau que le pare-feu (« *firewall* »). (Utilisation de la commande « *host* » + nom de domaine, permettant de qualifier les services des machines par exemple).

- Cartographie de réseau :

Via cette méthodologie, le pirate recherche un diagnostic du réseau cible et à en cartographier les composants. Le programme généralement utilisé est « traceroute » (fourni, à l'origine, avec Unix et Windows (à partir de Windows : outil dénommé

« tracert »). C'est un outil de diagnostic permettant de visualiser le chemin parcouru par un paquet de type IP d'un hôte à un autre. Via « traceroute », chaque routeur qui manipule le paquet IP de diagnostic, « décrémente » le champ « TTL » (« *Time To Live* » ou encore « durée de vie »). « Traceroute » peut permettre de découvrir la topologie réseau de la cible et surtout d'identifier les mécanismes de contrôle d'accès (« *firewall* »)[46]. Des outils de type IDS (*Intrusion Detection System*) permettent aussi de relever ce type de cartographie réseau. Le programme « RotoRouter » (Groupe pirate « Rhino9 ») permet aussi de renvoyer de fausses informations, lorsque ce type de requêtes est enregistré.

- Balayage « systématique » de réseau :

La prise d'empreinte correspond à la recherche d'informations ciblées. Le balayage systématique correspond à la recherche d'informations au sens large (image consistant à clencher chaque porte pour déterminer celle qui peut s'ouvrir). Les pirates testent chaque système cible pour vérifier s'il est actif, et déterminer quels ports de communication peuvent être en veille. Les différentes catégories de balayage réseau (ainsi que les techniques de prise d'empreinte de pile TCP/IP) sont présentées, pour information, en annexe 5 de notre étude. Les techniques de recensement et d'exploitation de failles sont aussi généralement propres à chaque système d'exploitation.

- Le recensement :

Après la prise d'empreinte, le pirate va ensuite chercher à identifier des comptes d'utilisateurs valides ou des ressources partagées mal protégées. Ces opérations sont appelées les opérations de « recensement ». Il s'agit véritablement de passer à la phase active de pénétration et d'intrusions. Généralement, lorsqu'un nom d'utilisateur ou de ressource partagée est recensé, le délai est court avant que l'intrus ne parvienne à deviner le mot de passe correspondant ou à identifier une faille associée au protocole de partage de ressource.

[46] *Note : hors la détection de type ligne de commande, il est possible de déterminer ces chemins de manière visuelle, notamment via l'outil http://www.visualroute.com (ne convient pas au réseau de grande taille).*

Après avoir détaillé chronologiquement les différents types d'actions cybercriminelles, au sens méthodologique, nous proposons d'en développer les pratiques d'attaques associées.

Les pratiques d'attaques pour preuves

- L'ingénierie sociale

L'ingénierie sociale (ou encore « *social engineering* ») n'est pas véritablement une attaque de type technique. Il s'agit d'une méthode pour obtenir des informations sur un système ou des mots de passe, cela *via* une personne physique. La technique consiste à se faire passer pour quelqu'un que l'on n'est pas (en général un des administrateurs du serveur que l'on veut pirater), mais qui est identifié au cœur du site victime. Le but est de demander des informations personnelles (*login*, (identifiant)), mots de passe, accès, numéros, données, etc…) en inventant un quelconque motif (problème réseau, nécessité de modification sur celui-ci, etc…). Cette technique peut s'exécuter soit par une simple communication téléphonique, soit par mail.

- Pratiques d'attaques sous IP :

- Le *sniffing*

Cette attaque est utilisée par les pirates aux fins de récupération des logins/mots de passe de divers utilisateurs transitant *via* une machine piégée. Lorsque les réseaux utilisent la technique du *broadcasting*, toutes les données transitent *via* toutes les cartes réseau des ordinateurs connectés. En temps normal, les trames destinées aux autres machines sont ignorées, seules celles concernant la machine destinatrice sont lues. Cependant, un logiciel appelé *sniffer* est capable d'intercepter toutes les trames d'une carte même si elles ne lui sont pas destinées. Une connexion de type *telnet* (connexion à distance), qui transite en clair, va pouvoir être capturée par un logiciel de type *sniffer* et lue. De même, il est possible de déterminer quelles pages web sont visionnées, les

sessions *ftp* et les mails en envois/réception. Cette technique demeure limitée car le pirate doit se trouver sur le même réseau (ou sous-réseau) que la machine qu'il veut pirater.

- Le « *spoofing* » ou encore « *IP spoofing* »

Cette attaque consiste à usurper une adresse IP, en la falsifiant, de manière à se faire passer pour une autre. Le pirate doit choisir la machine cible et doit en obtenir le maximum de détails pour savoir quelles machines sont autorisées à se connecter (notamment avec des droits autres que la simple lecture)[47].

La machine victime est appelée machine de confiance car elle a une « relation de confiance » avec le serveur. Le pirate doit la rendre inopérante pour être sûr qu'elle ne réponde pas à sa place. Pour ce faire, une attaque de type déni de service est généralement utilisée. Le pirate va ensuite envoyer plusieurs trames, en regardant l' « incrémentation » des numéros de séquencement, il va essayer de prévoir le numéro suivant. Ainsi le pirate va falsifier son adresse IP en la remplaçant par celle de la machine invalidée. Il envoie alors une demande de connexion au serveur (*SYN* – pour synchronisation). Le serveur envoie une trame *SYN ACK* (*ACK* – pour *acknowledge* (reconnaissance)) à la machine qu'il pense être l'émettrice. Celle-ci ne peut répondre (déni de service actif) et le pirate doit acquitter cette connexion (par une trame *ACK*) avec le numéro de séquence prévu plus un. Si le numéro est le bon, la connexion est établie et la machine *spoofée* peut alors commencer à envoyer des données sur le serveur. Une fois connecté *via* ce mode, le pirate installe des outils pirates afin de conserver un accès de type « *backdoor* » (porte dérobée) plus simple à mettre en œuvre que cette attaque de type « *spoofing* ».

En résumé :

1 : récupération de données pour deviner les numéros de séquencement et trouver une machine de confiance

[47] Si aucune machine n'est autorisée à se connecter en mode *root* (super-utilisateur) sur la machine victime (serveur), l'attaque demeure impossible.

2 : mise hors d'état de la machine de confiance (déni de service)

3 : demande de connexion avec une adresse spoofée

4 : envoi de la trame SYN ACK à la machine de confiance (mais saturée)

5 : réponse de la machine spoofée qui a alors ouvert la connexion

Cette attaque demeure très difficile à réaliser. Il existe des variantes de *spoof* pour des adresses e-mail, des serveurs DNS ou NFS (*Network File System*).

Les courriers électroniques sont aussi falsifiables car toutes les commandes sont écrites en code ASCII. Il est donc très facile de les taper à la main à l'aide d'une commande *Telnet* (port 25 : SMTP – *Simple Mail Transfert Protocol*).

- DoS, « *Denial of Service* »

Le « *DoS* » ou « *Denial of Service* » est une attaque visant à bloquer des services et ainsi empêcher le bon fonctionnement d'un système. Cette attaque ne permet en aucun cas l'accès à des données. Il s'agit entre autre de techniques de *flooding*, de *TCP-SYN flooding*, du *smurf* et du débordement de tampon. Suite à ces attaques, la bande passante est saturée, ce fut le cas lors des attaques de *DdoS* (*Distributed DoS*) en 2001 (sites : yahoo, amazon, …). (Cf. première partie - II - 3 - « Historique de la cybercriminalité »).

- Le *flooding*

Cette attaque consiste à envoyer à une machine de nombreux paquets IP de grosse taille. La machine cible ne pourra pas tous les traiter et finira par se déconnecter du réseau. Pour que l'attaque fonctionne, le pirate doit pouvoir envoyer les données plus vite que la machine ne peut y répondre.

- Le *TCP-SYN flooding*

Il s'agit d'une variante du flooding qui s'appuie sur le protocole TCP. Un grand nombre de demandes de connexions (*SYN*) au serveur sont effectuées à partir de plusieurs machines (on parle de « DdoS » pour « *Distributed DoS* ») ou d'une seule avec falsification de l'adresse IP (méthodologie de *spoofing*). Le serveur va envoyer un grand nombre de paquet *SYN-ACK* et attendre une réponse *ACK* qui ne viendra jamais. Les

paquets envoyés plus rapidement que le « *timeout* » (hors temps) des connexions débutées à moitié, entraîne la saturation du serveur et sa déconnexion.

- Le « *smurf* »

Le « *smurf* » est une attaque s'appuyant sur « *ping* » (*Packet INternet Groper*) et les serveurs de « *broadcast* ». Le « jeu » consiste pour le pirate à falsifier son adresse IP afin de se faire passer pour la machine victime en tant qu'émetteur (« *spoofing* »). Un « *ping* » est envoyé sur un serveur de « *broadcast* ». Il le fera suivre à toutes les machines qui sont connectées qui renverront chacune un « *pong* » au serveur et qui fera suivre à la machine cible (dont l'adresse avait été falsifiée au départ). Celle-ci sera alors inondée sous les paquets et finira par se déconnecter.

- Le débordement de tampon

Le débordement de tampon est aussi connu sous la dénomination « *buffer overflow* ». Il s'agit d'une attaque visant la gestion des chaînes de caractère. Cette attaque consiste à envoyer à la machine cible des données d'une taille supérieure à la capacité d'un paquet. Celui-ci va alors être fractionné pour l'envoi et rassemblé par la machine cible. A ce moment, il y aura débordement des variables internes. Suite à ce débordement, soit la machine se bloque, redémarre ou engendre écriture sur le code en mémoire. Ainsi, il devient possible de modifier directement le code des programmes de la machine. Si le débordement est suffisamment important, il peut écraser diverses données cruciales pour le système. Souvent, un pirate peut profiter de la situation pour prendre le contrôle de l'exécution d'un programme et ainsi acquérir les privilèges de celui-ci.

Ce développement des pratiques de piratage informatique permet de mieux se rendre compte de la réalité des faits, *via* les contournements effectifs possibles de mesures techniques et/ou humaines en place. Nous proposons ensuite de distinguer les tendances des actes de cybercriminalité, de manière détaillée, *via* une approche quantitative.

Exemple de relevés des tendances des actes de cybercriminalité

Le phénomène connaît depuis 15 ans une progression exponentielle. Sur la période 1994-1995, 4752 incidents de sécurité ont été relevés par le CERT-CC. Sur la période 1996-2001 : 92 714 incidents (explosion de 1998 à 1999 passant de 3734 incidents relevés à 9859). En 2002 : 82 094, puis en 2003 : 137 529. Sur la période 1988-2003 : 319 992 incidents de sécurité ont été relevés en tout. À partir de 2004, le CERT a mis en production le rapport « *E-Crime Watch Survey Shows Significant Increase in Electronic Crimes »* (qui remplacera à terme les statistiques de type rapports d'incidents). Ce relevé permet d'offrir la vision experte quantitative du phénomène, *via* des approches statistiques. Cette étude est réalisée par CSO magazine, *United States Secret Service,* et *Carnegie Mellon University Software Engineering Institute's CERT-CC*. Les enquêtes sont menées auprès de professionnels de la lutte contre la cybercriminalité (« *e-crime »).* Pertes estimées, en globalité au niveau économique, de type « e-crime » pour 2003 : 666 millions de dollars.

D'après les statistiques fournies par le e-crime 2005, « *Watch Survey* : *Survey Results Details »*, les variations les plus notables par catégories de crimes électroniques (cf. http://www.cert.org) sont les suivantes :

– 35 % augmentent,

– 13 % décroissent,

– 30 % ne varient pas.

La part de ratio entre interne/externe pour le cybercrime est :

- 80 % externes,

- 20 % internes.

Les types de cybercrime sont :

– 92 % *Phishing,*

– 92 % *Web site defacement,*

– 89 % *Spyware.*

L'enquête s'est déroulée auprès des sources suivantes : 62 % Secteur privé, 23 % Gouvernement, 14 % Entités légales.

Corrélativement, dans le cadre international du *HoneyNet Project*[48], notre participation au projet « *HoneyLux* » du Grand-Duché de Luxembourg, a permis de dresser un inventaire des activités courantes de cybercriminalité. Ce projet de recherche est abrité par l'association *Computer Security Research & Response Team* (CSRRT) ayant pour but d'améliorer la sensibilisation à la sécurité de l'information, y compris à un niveau international : « *CSRRT est une association de recherche en sécurité informatique et de réponse sur incidents localisée au G-D de Luxembourg. CSRRT-LU se livre à des développements avancés en sécurité informatique et à des projets de recherche dans le but d'augmenter la promotion et la conscience de la sécurité, en particulier au G-D de Luxembourg, mais aussi à un niveau international. CSSRT-LU est en partenariat étroit avec les instituts de recherche, le secteur industriel, et les institutions gouvernementales* »[49]. CSRRT a organisé deux conférences de type international, auxquelles nous avons pu participé, avec de plus pour la seconde, notre engagement au comité de relecture.

Ce projet repose sur le volontariat des organisateurs, chercheurs et autres participants. Il est constitué de machines interconnectées sur Internet à partir du territoire luxembourgeois, elles apparaissent de manière anonyme (implantation confidentielle), telles des machines de production classiques. HoneyLux est actif depuis quatre ans au Grand-Duché de Luxembourg. Il vise à capturer les traces de piratages informatiques afin ensuite de les étudier et de tirer des enseignements sur les techniques utilisées par les pirates informatiques, traduisant *de facto* la menace du moment sur le réseau de réseaux Internet. A l'inverse d'une approche théorique, HoneyLux vise une approche purement pratique dans le but principal d'apprendre mieux sur le terrain, et de déceler les nouvelles attaques de manière à mieux s'en protéger.

---

[48] http://www.honeynet.org, HoneyNet est un projet de Recherche, reposant sur le volontariat, et qui fédère l'ensemble des *HoneyPots* disponibles sur Internet. Les *HoneyPots* (littéralement Pots de miel) visent à piéger des *crackers* pour étudier leurs techniques d'attaques. HoneyNet est littéralement un réseau d'*HoneyPots*. HoneyLux est un *HoneyPot* en place au G-D de Luxembourg. La plus forte présence se situe aux États-Unis.

[49] « *CSRRT-LU is a computer security research and response team association localized in the Grand-Duchy of Luxembourg. CSRRT-LU engages in highly advanced computer security development and research projects in order to increase security awareness and advancement especially in Luxembourg but also on an international level. CSRRT-LU is in close partnership with research institutes, the industrial sector and governmental institutions* ». http://www.csrrt.org.lu.

Le co-fondateur du projet HoneyLux nous a indiqué que la faille de sécurité « *SQL Server* » (serveur de gestion de bases de données) a été découverte, à l'époque, à partir d'une attaque sur une machine du *HoneyNet project*, permettant de prévenir rapidement les organismes de sécurité, tel que le CERT CC, qui ensuite se sont chargés d'alerter l'ensemble de la communauté Internet. Statistiquement, notre interlocuteur nous a précisé qu'un *HoneyPot* « voit » pratiquement toutes les catégories d'attaques réelles atteignant le réseau de réseaux Internet et ceci en direct.

L'intérêt réside aussi dans le fait que HoneyLux capte les attaques mais les stocke également, ce qui permet de les analyser plus en profondeur. Cela permet d'effectuer une analyse de type « légiste » de l'entrave à l'information et à la communication. En moyenne, une machine HoneyLux est attaquée dans la minute suivant sa mise en ligne sur Internet. L'activité pirate est très dense. Les membres du réseau HoneyLux souhaitent aussi héberger des projets de Recherche innovants. Récemment, un membre de ce réseau a présenté, lors d'un groupe de travail CLUSSIL (CLUb de la Sécurité des Systèmes d'Information Luxembourg[50]), le projet en cours d'analyse de la « *malware activity* » hébergé par le réseau HoneyLux. Un logiciel malveillant (*malware* en anglais) est un logiciel développé dans le but de nuire à un système informatique.

Cette activité est actuellement très forte, et les nouveaux *malwares* se comptent journellement par centaines (pour chaque empreinte différente). Le CSRRT confronte ces derniers aux anti-virus les plus avancés qui souvent ne reconnaissent pas ce type de nouvelles menaces. A ce titre, le travail du CSRRT est véritablement innovant. Une carte de la « *malware activity* » mondiale peut être consultée et analysée, sur le site web du CSRRT, statistiquement par pays, ainsi que les résultats d'analyses d'anti-virus face aux *malwares* captés, sur le site web du CSRRT. Les virus et les vers sont les deux exemples de logiciels malveillants les plus connus. Les logiciels malveillants peuvent être classés en fonction des trois mécanismes suivants :

- le mécanisme de propagation (par exemple, un *ver* se propage sur un réseau informatique en exploitant une faille applicative ou humaine) ;
- le mécanisme de déclenchement (par exemple, la *bombe logique* — comme la

[50] http://www.clussil.lu.

bombe logique surnommée *vendredi 13* — se déclenche lorsqu'un événement survient (cf. partie « historique de la cybercriminalité ») ;

- la charge utile (par exemple, le *virus* Tchernobyl tente de supprimer des parties importantes du BIOS, ce qui bloque le démarrage de l'ordinateur infecté).

Cette classification standard est actuellement la plus couramment adoptée dans les milieux de la sécurité informatique internationaux. Ils se déclinent ainsi :

- les virus et les vers sont deux grandes classes de logiciels malveillants. Leur caractéristique commune est qu'ils sont tous les deux capables de se répliquer eux-mêmes. Ils peuvent générer des copies d'eux-mêmes, parfois modifiées. Toutefois, tous les programmes qui se répliquent ne sont pas forcément des virus ou des vers. Pour être classifiées comme virus ou ver, il faut qu'au moins certaines de ces copies puissent se répliquer elles-mêmes aussi. La différence entre un virus et un ver est qu'un ver peut fonctionner plus ou moins indépendamment, tandis qu'un virus dépend des autres hôtes du réseau pour se propager.

- les vers (*worm*) se répandent dans le courrier électronique en profitant des failles des différents logiciels de messagerie (notamment Microsoft Outlook). Dès qu'ils ont infecté un ordinateur, ils s'envoient eux-mêmes à des adresses contenues dans tout le carnet d'adresses, ce qui fait que l'on reçoit ce virus de personnes connues. Certains d'entre eux ont connu une expansion fulgurante (comme le ver « *I Love You* »).

- les chevaux de Troie (*Trojan horses*) portent le nom de la célèbre ruse imaginée par Ulysse. Ces programmes prétendent être légitimes (souvent de petits jeux ou utilitaires), mais comportent des routines nuisibles exécutées sans l'autorisation de l'utilisateur. Les chevaux de Troie ne sont pas des virus car il leur manque la fonction de reproduction, essentielle pour qu'un programme puisse être considéré comme un virus.

- les *backdoors* (portes dérobées) qui prennent le contrôle de l'ordinateur et permettent à quelqu'un de l'extérieur de le contrôler par le biais d'Internet.

- les logiciels espion (*spyware*) peuvent accompagner certains logiciels et pilotes de périphériques ; ils s'installent discrètement sur l'ordinateur, sans prévenir l'utilisateur, collectent et envoient des informations personnelles à des organismes tiers.

- les canulars (*hoax* en anglais), que l'on classifie régulièrement à tort de virus ou logiciel malveillant, sont des courriers électroniques dont le contenu est souvent une

alerte sur un faux-virus ; ils n'ont pour conséquence indirecte que de saturer les serveurs de courriels de messages inutiles.

Voici différentes techniques de lutte contre les logiciels malveillants, celles-ci pouvant être cumulées car n'agissant pas sur les mêmes risques :

- prévention par la sensibilisation des utilisateurs aux problématiques de sécurité,
- mise à jour systématique (par exemple quotidiennement ou à chaque connexion sur Internet) du système d'exploitation et de tous les logiciels,
- utilisation d'un logiciel anti-virus, contre les virus, vers, et chevaux de Troie,
- utilisation d'un logiciel *anti-spyware*,
- utilisation d'un logiciel *anti-rootkit*,
- utilisation d'un HIDS (*Host-based Intrusion Detection System*), un système de détection d'intrusion sur l'hôte,
- utilisation d'un pare-feu, pour verrouiller toutes les communications (dans les deux sens) qui ne sont pas requises.

Ces systèmes ne sont pas parfaits (aucun logiciel anti-virus ne détecte tous les virus, ni les *malware* d'ailleurs), mais ils permettent de réduire considérablement les risques d'infection ou d'attaque de logiciel malveillant. L'utilisation conjointe de plusieurs méthodes du même type, mais ayant un fonctionnement différent peut aussi s'avérer utile.

Après avoir décliné les démarches d'attaques, il appert important de mettre en évidence, de manière plus spécifique le cadre sémantique de la cyberdélinquance. Pour ce faire, nous examinerons plus en avant un état d'éléments pertinents de recherche en la matière, puis les définitions d'une activité illégale, et enfin un historique de la cyberdélinquance. Ce cadre sémantique permettant de valider, en corrélation avec les éléments précédemment détaillés, des caractéristiques essentielles de la représentation sociale de la cyberdélinquance.

II – Le cadre sémantique de la cyberdélinquance

Avant de rendre compte de l'évidence statistico-démonstrative et de la caractérisation d'illégalité fortement prononcée pour la cyberdélinquance, nous analyserons l'état des éléments pertinents de recherche en la matière, puis ses différentes définitions, pour enfin caractériser un rapide historique. Ces éléments doivent nous permettre d'étudier la représentation sociale de la cyberdélinquance comme établie, et comme autant de marqueurs de son contenu et de sa structure. Une représentation sociale étant un ensemble organisé d'informations, d'opinions, d'attitudes et de croyances à propos d'un objet donné, les éléments étudiés en permettent une traduction concrète. Nous les considèrerons comme une connaissance sociale « sédimentée » exprimée délibérément de manière explicite, pédagogique, consensuelle, et directement analysable (via notre expérience professionnelle, en tant que filtre interprétatif). Il s'agit donc de la mise en évidence de constituants non négligeables de la cyberdélinquance socialement représentée.

1) Etat d'éléments pertinents de recherche en matière de cyberdélinquance

« *L'émergence de l'ère informatique a donné naissance à de nouveaux comportements délinquants, difficiles à appréhender et marqués du sceau de l'immatérialité* »[51]. En effet, le terrain d'expression de la délinquance au niveau du cyberespace détermine des possibilités infinies d'actes illégaux, pouvant se répéter à l'infini: « *L'automatisation du monde numérique rend plus dangereuses les attaques sur les services Internet que les attaques du monde réel […] Dans le monde réel, les attaques ne s'étendent pas aussi facilement, cependant au fur et à mesure que le monde physique se transpose en ligne, le monde « underground » peut potentiellement exploiter des vulnérabilités de manière automatisée et très approfondie* »[52]. Dans ce même ordre

[51] *La criminalité sur l'Internet* (Pansier, Jez, 2000).
[52] « *One of the things that makes attacks on Internet services more dangerous than attacks in the physical world is the automation that is possible in the world of computers […] The worry is that in the physical world, attacks do not scale very well, but as soon as a physical world process is moved online, malicious parties can potentially exploit vulnerabilities in an automated and exhaustive fashion* » .

d'idée et cadre d'application, D. Guinier définit la cybercriminalité, au sens large, comme « *tout ce qui regroupe les activités illégales et les actes directement commis à l'encontre ou à l'aide des technologies de l'information et de la communication (TIC), localement ou à distance, et qualifiables de délictueux ou criminels* »[53]. Ces menaces proviennent le plus souvent de l'exploitation d'outils à caractère malveillant disponibles gratuitement sur Internet, ou correspondent tout simplement à la transposition numérique de comportements délictueux de la société traditionnelle. Certains pirates informatiques développent, cependant, de manière personnelle, leur propre méthodologie et outils, de manière personnelle, qui demeurent par le fait difficilement saisissables.

Le principe d'une nouvelle délinquance s'est ainsi rapidement développé sur Internet : « *la croissance exceptionnelle de cet univers de communication s'accompagne évidemment de son cortège de méfaits : les nouvelles technologies de l'information et de la communication sont à la fois l'objet et l'outil de nouvelles délinquances. On peut classer ces délinquances en fonction de l'objet technologique concerné ou en fonction de l'usage qui en est fait : si c'est un outil utilisé par le criminel pour commettre son forfait ou s'il en est l'objet même* »[54]. De plus, aujourd'hui, ces cyberdélinquants ciblent et prennent l'habitude de camoufler leurs attaques pour plus d'efficacité, combinant *social engineering* (ingénierie sociale), technologies et codes malicieux…

Ainsi, à ce jour la cyberdélinquance se professionnalise et le crime organisé l'a également largement intégrée à ses pratiques. Pour exemple, le procureur antimafia italien, Pier Luigi Vigna, a récemment souligné que le crime organisé « *se sert de managers et de cols blancs pour gérer les affaires illégales à travers le système informatique* ». En effet, les différents types de criminels ne fonctionnent donc pas en autarcie, mais interagissent, multipliant les effets négatifs, illégaux et dangereux de la cyberdélinquance. Le récent rapport Symantec « *Le cybercrime s'organise pour vider les caisses* »[55] précise la généralisation de ce phénomène. Globalement ce rapport fait état d'une cyberdélinquance internationale de mieux en mieux organisée, les pirates

---

Defending Against an Internet-based Attack on the Physical World (Byers, Rubin, Kormann, 2002).

[53] *Les systèmes d'information – Arts et pratiques* (Guinier, 2002).

[54] *L'internet* (Capul, mars-avril 2000).

[55] *Pirates, phishing virus...le cybercrime s'organise pour vider les caisses,* guide de la sécurité informatique, (Symantec, 2006).

informatiques « pensant réseau » avant tout, et coordonnant leurs actions. La cyberdélinquance s'organise donc, avec par exemple des outils de type « *crimewares* » (programmes informatiques conçus spécialement à des fins malveillantes) qui se professionnalisent et perfectionnent tout type d'escroquerie comme le vol d'informations sur Internet.

Récemment, après en avoir délimité l'existence, la recherche scientifique s'est intéressée plus en avant à l'objet même de la « cyberdélinquance ». C'est son domaine technique qui fut principalement étudié ; ses perspectives sociales se développent depuis peu, mais timidement. Ainsi, la majorité des publications scientifiques relevant de l'objet a principalement pour origine le domaine de l'informatique et des technologies associées aux systèmes d'information. En effet, les principales recherches se sont attachées à définir le périmètre propre de la cyberdélinquance avec ses diverses méthodologies, la catégorisation de ces activités illégales et de ses acteurs principaux, puis, en conséquence, la présentation globale des schémas de lutte. Pour leur part, les sciences humaines s'attachent à la recherche (principalement sociologique) relative aux acteurs principaux de la cyberdélinquance et à saisir leurs motivations.

Le périmètre menaçant de la « cyberdélinquance »

La notion de « cyberdélinquance » regroupe l'ensemble des infractions commises sur ou par un système informatique généralement connecté à un réseau. « *La cyberdélinquance couvre trois catégories d'agissements : la première considère les technologies de l'information en tant que cibles d'infractions (accès frauduleux à un système informatique, atteinte à l'intégrité de données ou interceptions illégales), la seconde utilise les technologies de l'information en tant que moyen de commettre des actes criminels « classiques » (production et diffusion de contenus illicites ou préparation d'actes terroristes), la troisième enfin, consiste à utiliser les technologies de l'information en tant que vecteur de « contenus informationnels illicites » (pornographie enfantine, racisme et xénophobie) »*[56]. Cette classification des faits, permet de favoriser

[56] Dossier « *Cybercrime et démocratie* » - Contexte (*Forum des droits sur l'internet*, 2001).

la compréhension du phénomène, sans pouvoir toutefois le définir de manière exhaustive. De plus, de nombreux termes sont parfois utilisés de façon interchangeable pour décrire des crimes commis à partir d'ordinateurs : « - *Crime lié à un ordinateur : l'utilisation d'un ordinateur est déterminante pour commettre l'attaque ; - crime Internet : détermine les crimes pour lesquels l'utilisation d'Internet est une caractéristique clé et comprend des infractions telles que posséder des images pédophiles par exemple ; crime électronique : une catégorisation de type général relative aux infractions commises en utilisant un stockage électronique de données ou un outil de communication* »[57].

De fait, le terme *cyberdélinquance* demeure globalement difficile à conceptualiser, car il ne fait l'objet d'aucune définition légale : « *Ce choix des législateurs a conduit la doctrine à multiplier les définitions de ce terme, contribuant ainsi à rendre plus complexes les analyses juridiques. En effet, l'absence de définition légale de ce terme est source de confusions, tant au niveau du domaine de la réflexion, qu'au niveau de l'analyse ou du vocabulaire choisi* »[58]. Ces confusions ont conduit M. Chawki à élaborer une définition pratique de ce qu'est la cybercriminalité, afin de l'appréhender plus facilement, notamment en terme de droit : « *La cybercriminalité [ou cyberdélinquance] peut être définie comme : toute action illicite associée à l'interconnexion des systèmes informatiques et des réseaux de télécommunication, où l'absence de cette interconnexion empêche la perpétration de cette action illicite. Sous cette définition, nous pouvons identifier les quatre rôles que joue le système informatique dans les actes illicites :*

***Objet** : Des cas concernant la destruction de systèmes informatiques, ainsi que des données ou des programmes qu'ils contenaient, ou encore la destruction d'appareils fournissant l'air climatisé, l'électricité, permettant aux ordinateurs de fonctionner.*

---

[57] *« computer-related crime – the use of a computer is integral to committing the offence ; […] - internet crime – refers to crimes in which the use of the internet is a key feature and includes content-related offences such as possession of child pornography for example; - e-crime – a general label for offences committed using an electronic data storage or communications device ».*
Concepts and terms (High Tech Crime Brief, 2005).

[58] *Essai sur la notion de cybercriminalité,* (Chawki , 2006).

***Support** : Un système informatique peut être le lieu ou le support d'une infraction, ou un ordinateur peut être la source ou la raison d'être de certaines formes et sortes d'avoirs qui peuvent être manipulés sans autorisation.*

***Outil** : Certains types et certaines méthodes d'infractions sont complexes pour nécessiter l'utilisation d'un système informatique comme instrument. Un système informatique peut être utilisé de manière active comme dans le balayage automatique de codes téléphoniques afin de déterminer les bonnes combinaisons qui peuvent être utilisées plus tard pour se servir du système téléphonique sans autorisation.*

***Symbole** : Un système informatique peut être utilisé comme symbole pour menacer ou tromper. Comme, par exemple, une publicité mensongère de services non existants, comme cela a été fait par plusieurs clubs de rencontres informatisés* ».

Cette proposition de définition demeure originale face aux multiples catégorisations développées, car souvent soit trop « étroites » impliquant l'utilisation extrême de l'ordinateur, soit trop « larges » incluant des infractions déjà classées comme infractions traditionnelles. En effet, le concept ainsi posé rejoint alors les spécifications du cadre du cyberespace, de sa relation avec la délinquance, et du domaine même de la cyberdélinquance. En fait, cette définition permet de traiter avec pragmatisme de l'objet de recherche.

La cyberdélinquance correspond donc à un ensemble de catégories de délits largement étendu. Les aspects de fraude, de falsification, de sabotage et d'extorsion, l'espionnage industriel, le piratage de logiciels, les crimes contre la propriété industrielle sont autant de délits économiques utilisant le *hacking* comme vecteur. Le « *hacking* » est souvent utilisé comme synonyme du « piratage informatique ». A ce titre, Daniel Martin[59] décline ainsi les catégories suivantes comme définissant le « *hacking »* :

- *accès et maintien frauduleux dans un système d'information ;*
- *lecture des logiciels, fichiers et données,*
- *altération éventuelle du fonctionnement du système ;*
- *suppression ou modification des données ;*
- *introduction de virus, bombes logiques, etc.* »

[59] *La menace de la cybercriminalité* (Martin, 2001).

Attaché à ce kaléidoscope de catégorisations désormais établies, la croissance du phénomène « cyberdélinquance » a, finalement, accompagné et intégré les évolutions technologiques. Ainsi, D. Martin distingue trois temps dans la diffusion de ces menaces :

- « *des années soixante-dix à quatre-vingt, la banalisation de l'informatique s'accompagne du piratage de logiciels et de la contrefaçon des cartes de crédits ;*

- *dans les années quatre-vingt, l'émergence des réseaux locaux et de leurs connexions voit naître les premières affaires de détournement de fonds et les premiers hackers s'attaquant à des cibles prestigieuses (NASA, Pentagone, etc) ;*

- *depuis les années quatre-vingt dix, l'informatique distribuée, la prolifération des systèmes d'information et la croissance d'Internet ont favorisé les formes de criminalité instrumentalisant le virtuel et l'immatériel.* »

Ces enjeux se réfèrent principalement aux types d'acteurs de la cybercriminalité, dans le domaine de l'information « sensible » relative au fonctionnement des entreprises et des objets sur lesquels peuvent s'exercer des droits de propriétés. Afin de parfaire sa compréhension, il importe également de tenir compte du fait que la cyberdélinquance se mesure souvent en termes d'impacts financiers. En effet, de nombreux marqueurs fournissent des preuves tangibles de cette activité et sont largement diffusés et disponibles pour tout public sur Internet. Ces éléments statistiques sont constamment repris en exemple au sein des diverses publications scientifiques dédiées à ce phénomène (voir partie suivante II. 2)). Le FBI (*Federal Bureau of Investigation* - Etats-Unis) évalue, par exemple, le coût total du cybercrime pour la seule année 2005, à 67 milliards $. Plus récemment (2006), le CERT-CC a produit un rapport nommé « *e-crime watch survey*», validant ces faits : ainsi sur un échantillon de 434 entités aux Etats-Unis, les préjudices financiers, associés à des attaques numériques, augmentent de façon significative (en moyenne par répondant 704.000 $ en 2006, contre 507.000 $ en 2005).

Pour éclaircir la notion de périmètre menaçant, nous retiendrons surtout la définition claire et établie de la cyberdélinquance tel que Sean B. Hoar la décline : « *La cyberdélinquance est devenue si commune que désormais la notion fait partie de*

notre vocabulaire, définie comme un crime commis sur un réseau informatique, particulièrement sur Internet »[60].

De la catégorisation de la « cyberdélinquance »

Très tôt la notion de cyberdélinquance fut catégorisée, notamment afin de définir correctement les différents cas quant à la répression à appliquer, selon justement la portée des actes et les motivations souvent associées. « *Le dixième congrès des Nations Unies sur la prévention du crime et du traitement des délinquants a permis en 2000 de catégoriser cinq infractions en tant que cybercrime : - accès non autorisés ; - dommages à des données ou des programmes informatiques ; - sabotages pour entraver le fonctionnement d'un système informatique ou d'un réseau ; - interception non autorisée de données, depuis et via un système ou réseau ; et l'espionnage par ordinateur* »[61]. Au-delà de la nouvelle criminalité, il apparaît clairement que des activités criminelles « classiques » au sein de la société traditionnelle ont su aussi gagner les territoires numériques. A ce titre, il est possible de parler de types de crime qui peuvent subtilement être ainsi classés ainsi : « *Le premier concerne le vol. […] Avec un accès facile au serveur une équipe organisée de criminels peut facilement cloner le serveur et détourner de l'argent vers différents comptes […] Un autre, crucial pour toutes les opérations de crimes organisés ayant progressé avec Internet, est le blanchiment d'argent […] Un autre, ayant pris une nouvelle forme sur Internet, est le vol d'identité [...] Une autre*

[60] « *Cybercrime is so common that it is now part of our lexicon, defined as a crime committed on a computer network, especially the Internet* ».
Trends in cybercrime : the dark side of the Internet (Hoar, 2005).

[61] *The tenth United Nations Congress on the prevention of Crime and the Treatment of Offenders as of the year 2000 categorized five offenses as « cyber-crime » :*
- *Unauthorized access,*
- *Damage to computer data or programs,*
- *Sabotage to hinder the functioning of a computer system or network,*
- *Unauthorized interception of data, from and within a system or network,*

And computer espionage ».
Hacking and Cybercrime (Sukhai, 2004).

nouvelle méthode, pour un crime ancien, est devenue possible via Internet à savoir l'extorsion »[62].

Pratiquement, il n'existe pas de liste définitive des actions de cyberdélinquance, cependant, il est possible de les relever finement pour suivre spécifiquement leur évolution voire leur « amélioration continue ». Broadhurst et Chantler[63] ont permis de déterminer une vue consensuelle récente pour clarifier ces activités : « *Vol de télécommunications, interceptions illégales de télécommunications, piratage de droits d'auteur, prise de contrôle numérique, blanchiment d'argent, vandalisme électronique, cyber-Terrorisme, déni de service, extorsion, ventes et fraudes à l'investissement, contrefaçon, fraude au transfert de fonds, fraude à la vente et à l'investissement, vol d'identité, crime de contenu, matériel offensif, espionnage, vol de ressources, utilisation illégale d'ordinateur* »[64]. Broadhurst et Chantler détaillent très spécifiquement chaque activité, fournissant de nombreux exemples pratiques permettant ainsi de mieux qualifier la catégorisation des actes de cyberdélinquance.

Spécifiquement, S. Hoar[65] énonce également les faits récents de cybercrime : « *En 2005, la dissémination de nouveaux codes malicieux a continué de progresser avec un taux exponentiel […] Selon une étude menée au Etats-Unis, le phishing a causé approximativement 1.2 milliards de pertes directes pour les banques et les émetteurs de cartes bancaires […] La forme la plus dangereuse de phishing est le logiciel malicieux, aussi nommé « malware »* »[66].

---

[62] « *The first crime that has seen both is theft. […] With easy access to a server an organized team of criminals can easily clone the server and divert money into different accounts […] Another crime crucial to all organized crime operations that sees advances with internet is money laundering. […] Another crime that has taken an entirely new form on the internet is identity theft […] Another new method for an old crime made possible by the internet is extorsion* ».

Organized crime and the Internet (Nelson-Palmer, 2006).

[63] *Cybercrime Update : Trends and Developments* (Broadhurst, Chantler, 2006).

[64] « *Telecommunications Theft, illegal Interception of telecommunications, Piracy Copyright Theft, Cyber Stalking, Electronic money laundering and Tax evasion, Electronic vandalism, Cyber-Terrorism, Denial of Service, Extorsion, Sales and Investment Fraud, Forgery (Classic Pyramid Schemes), Electronic Funds Transfer Fraud and Counterfeiting (Carding), Identity Theft and Misrepresentation, Content Crime – Offensive Materials, Espionage, Resource Theft – illegal use of PC* ».

[65] *Trends in cybercrime : the dark side of the Internet* (Hoar, 2005).

[66] « *In 2005, the dissemination of new malicious code continues at an exponential rate […] According to one study, phishing caused approximatively $1.2 billion in direct losses to banks and credit card issuers in the United States in 2003 […] The most dangerous form of phishing is malicious software. Also called «malware* » ».

Au sein des méthodologies de cybercriminalité, et au-delà des technologies innovantes menaçantes, une notion particulière retient depuis peu fortement l'attention, car à l'origine de multiples fraudes cybercriminelles, à savoir la notion de « *hacking* cognitif »[67] (terme défini par l'*Office of Justice Programs, National Institute of Justice, Department of justice, award number 2000-DT-CX-K001 (S1)*). Peu usité, ce terme se réfère aux attaques d'ordinateurs ou de systèmes d'information en relation avec la possible transformation du comportement initial de l'utilisateur, de ses perceptions, et correspondant à des comportements visant la réussite de l'attaque.

Se distinguent alors les attaques « autonomes » qui sont le fait d'une méthodologie reposant exclusivement sur des technologies informatiques, tandis que les attaques « cognitives » se penchent sur les attaques de type « humain » : « *En exemple, les fichiers contenant des informations privées comme des numéros de cartes bleues peuvent être téléchargés et utilisés par un attaquant. Une telle attaque ne requiert aucune intervention par les utilisateurs d'un système attaqué, du fait nous nommerons cette dernière une attaque « autonome* »[68].

Les actes de « *cognitive hacking »* se passent d'attaques directes mais font appel à toute technique de manipulation frauduleuse visant à tromper l'utilisateur : « *Cognitive Hacking » est défini ici comme le fait de gagner l'accès, ou atteindre un ordinateur pour le but d'affecter le comportement humain de celui qui utilise le système dans le but de violer l'intégrité d'un système informatique* »[69] . Deux classes peuvent être distinguées au sein de la notion de « *cognitive hacking* » : « *Avec le Cognitive Hacking manifeste, aucune atteinte n'est effectuée pour cacher le fait qu'un piratage de ce type est effectué (exemple : le « defacement » d'un site web). Un même type d'attaque sous couvert, en*

[67] Usuellement dénommés « *cognitive hacking* ».

[68] « *For example, files containing private information such as credit card numbers can be downloaded and used by an attacker. Such an attack does not require any intervention by users of the attacked system, hence we call it an* « *autonomous attack* ».

Cognitive hacking : a battle for the mind (Cybenko, Giani, Thompson, 2003).

[69] « *Cognitive hacking is defined here as gaining access to, or breaking into a computer system for the purpose of affecting the behavior of a human use the system in a manner that violates the integrity of a computer system.* ».

contraste, peut avoir des conséquences considérables, parce qu'il peut influencer les perceptions d'un utilisateur et son comportement »[70].

Les exemples d'activités de « *Cognitive Hacking »* sont nombreux ; peuvent être cités : les vols de services, les vols d'informations, la fraude financière, la fraude non financière, les « farces », le « *phishing* », etc... Ainsi le « *social engineering* » est par exemple une pratique consistant à user de ressorts psychologiques pour obtenir d'un tiers une information ou des données en vue de commettre une fraude, une intrusion réseau, de l'espionnage industriel ou bien encore un vol d'identité. Un autre exemple pratique de « *cognitive hacking* » : le *phishing*. Cette technique est pratiquée dans le but d'extorquer des informations confidentielles aux internautes, mais ne constitue pas la seule cible de ces actes malicieux. Chaque acte de *phishing* est effectué en abusant de l'image et de la confiance accordées par l'utilisateur à de grands organismes internationalement reconnus.

Ceux-ci paient aussi le prix fort des attaques de *phishing*, comme la banque anglaise NatWest qui s'est vu forcée de suspendre provisoirement une partie de ses services en ligne début novembre 2004 afin de ne pas subir les contrecoups d'une attaque de *phishing* à grande ampleur lancée à son encontre. Les pertes de réputation et les pertes financières sont importantes, autant pour les organismes visés par les attaques de *phishing* que pour les utilisateurs d'Internet dupés et extorqués. Ces sites ont explosés en 2006, et l'Anti-Phishing Working Group (APWG), groupe de travail international de lutte contre ce dénommé « hameçonnage », a fait, en effet, état d'une très forte progression du nombre de nouveaux sites de ce type en octobre 2006 (*au cours de ce mois 37 444 nouveaux sites Internet frauduleux ont été signalés à l'APWG*).

Bien que fortement liée au domaine technique, l'existence même de la cybercriminalité passe également par une multiplicité de profils criminologiques. Le domaine peut, en effet, revêtir :

- un renouvellement des pratiques de la criminalité organisée déjà existante ;
- le développement de la criminalité dite « en col blanc », c'est-à-dire de comportements criminels œuvres d'employés de firme ;

[70] « *With overt cognitive hacking no attempt is made to conceal the fact that a cognitive hack has occurred. For example, website defacement is a type of overt cognitive hacking […] Covert cognitive hacking, by contrast, is likely have more significant consequences, because it can influence a user's perceptions and behavior* ».

- l'apparition de nouveaux criminels, souvent isolés, dont les actions sont strictement liées aux Technologies de l'Information et de la Communication (T.I.C).

Max Kilger, Ofir Arkin, et Jeff Stutzmann[71], experts au sein du HoneyNet Project[72] et rédacteurs pour « *Honeynet 2* » (cf. partie « Relevé de tendances de la cybercriminalité »), précisent qu'il est aussi important de comprendre la technique employée en termes de compétences et d'outils pour le piratage informatique réseau, que le cadre social dans lequel il s'inscrit. Ces chercheurs indiquent ainsi l'importance de replacer le pirate informatique dans son milieu social pour le comprendre. Au cœur du chapitre 16 « *Profiling* » de « *Honeynet 2* », les chercheurs déterminent que la dimension sociale s'avère aussi sensible que la dimension technique. Ainsi connaître la « communauté pirate » est aussi important que connaître les outils techniques. Afin de progresser dans sa connaissance, Max Kilger a choisi d'approfondir la crise d'identité qui existe au sein de la communauté des pirates informatiques, en analysant les motivations des individus et des groupes et en posant un regard scientifique sur la structure sociale combinée des « *black hat* » (« chapeau noir ») et « *white hat* » (« chapeau blanc »), permettant une vue plus large des attitudes, comportements, et actions de ces membres. Il a déterminé une crise forte de « *labels* » au sein de la communauté pirate, qui entraîne pour résultat l'incompréhension de l'acteur social. En effet, le label peut aider à véhiculer une image, mais ce dernier n'est pas directement identifiable en tant que tel, car Kilger indique qu'il n'existe pas de carte d'identité du « *hacker* » : «*Il n'existe pas de carte d'identité du hacker, et pas de caractéristiques physiques visibles […]* »[73].

Quant à l'engagement pour la cyberdélinquance, ces chercheurs précisent que les éléments les plus déterminants pour le comprendre, à travers la communauté informatique, repose sur les motivations suivantes : « *Les six motivations que nous discuterons en relation avec la communauté hacker sont : Argent, Distractions, Ego, Volonté, Entrée dans un groupe social, et Statut, selon l'acronyme « MEECES »* »[74].

---

[71] *Know Your Enemy: Learning about Security Threats (2nd Edition)* (The HoneyNet Project, 2004).
[72] http://www.honeynet.org.
[73] « *There is no official « hacker identity card », no reliable identifiable physical characteristics* […] ».
[74] « *The six motivations we'll discuss in relation to the hacker community are Money, Entertainment, Ego, Cause, Entrance to social group, and Status – which forms the allegorically appropriate acronym MEECES* ».

La défense contre la menaçante « cyberdélinquance »

L'élément fédérateur de la recherche pose la sécurité de l'information comme réponse globale face à la cyberdélinquance. Robert C. Newman décrit cette solution comme des buts à définir et à atteindre pour lutter contre les menaces numériques : «*Une menace est significative d'un point de vue sécurité, car le but de la sécurité informatique est de fournir des aperçus ; des méthodologies et des techniques qui peuvent être utilisées pour mitiger les menaces*»[75]. La sécurité de l'information est posée comme un élément de défense face à l'objet cybercrime. Ces activités menaçantes sont devenues automatisées à grande échelle, ce qui nécessite, de plus en plus, de la rigueur et des solutions de sécurité adaptées en réponses.

Nous avons vu que la cyberdélinquance correspond à un ensemble de délits largement étendu. Au niveau international, les références juridiques essentielles en la matière sont précisées par le « *United Nations Manual on Prevention and Control of Computer-Related Crime* » (http://www.ifs.univie.ac.at/%7Epr2gql/rev4344.html), et d'autre part, par le texte de la convention européenne de Budapest sur les crimes commis *via* Internet et autres réseaux informatiques. « *Une des raisons pour laquelle le cybercrime a reçu une telle attention en hausse, en si peu de temps, est le fait que pendant de nombreuses années, les statistiques concernant les crimes de haute technologie on été extrêmement peu fiables, tel que l'argumente le Chef de la Police Tony Aeilts*[76] ».

Le Federal Bureau of Investigation (FBI) apporte une ouverture dans les moyens de lutte contre la menaçante cyberdélinquance. Le bulletin de janvier 2005 du « *FBI Law Enforcement Bulletin* » est libellé « *Defending Againt Cybercrime and Terrorism* » (« *A new role for Universities* »)[77]. Pour postulat le FBI estime l'activité cyberdélinquance comme augmentant la peur numérique et freinant le développement des T.I.C., entraînant,

[75] « *A threat is significant from a security viewpoint, because the computer security goal is to provide insights ; methodologies, and techniques that can be employed to mitigate threats.*».
[76] « *One of the reasons that cybercrime has received such a significant increase in attention in a relatively short time is the fact that for many years, statistics regarding high-tech crime have been extremely unreliable, as argues Police Chief Tony Aeilts.* ».
Defending Against Cybercrime and Terrorism (A new role for Universities) (Aeilts T., 2005).
[77] *Defending Against Cybercrime and Terrorism* (A new role for Universities) (Aeilts T., 2005).

de facto, un ralentissement de la croissance économique. De plus une nouvelle menace se dessine sur les réseaux de l'information et de la communication, le terrorisme numérique devrait, en effet, sous peu se développer à l'instar de celui connu au sein de la société traditionnelle : « *Depuis le 11 septembre 2001, la nation a plus focalisé sur les résultats du cyberterrorisme parce que bien que les terroristes aient typiquement utilisés des méthodes d'attaques traditionnelles (explosifs, kidnappings, etc), leur attention peut bouger, avec son développement vers le cyberterrorisme »*[78]. Les aspects de cette menace sont non négligeables car ils peuvent toucher de nombreuses infrastructures critiques, cibles privilégiées du terrorisme : « *Différentes formes d'infrastructures technologiques peuvent être vulnérables à une telle attaque; pipelines, centrales électriques, axes routiers, et de nombreuses autres entités dépendant des T.I.C. De plus, les systèmes de communication utilisés à buts financiers, militaires, policiers, et les différentes sociétés, souffrent des mêmes vulnérabilités »*[79]. Ainsi, tant les pouvoirs publics au niveau international, que les entités sectorielles du secteur privé, ont réagi en conséquence :

« *Il est évident, afin de combattre effectivement le chevauchement exponentiel du crime organisé et du cybercrime, qu'une véritable solution d'ensemble et multilatérale est requise. En 2001, l'Union Européenne, les Etats-Unis, le Canada, le Japon, et l'Afrique du Sud ont choisi la bonne direction en élaborant la Convention Cybercrime »*[80].

De même : « *En février 2005, un groupe de quinze cadres des plus grandes compagnies des T.I.C. des États-Unis, dont Adobe, Dell, Microsoft, et IBM, a encouragé l'administration Bush à créer une commission nationale sur le cybercrime organisé […] Un an après, une réunion entre la Business Software Alliance (BSA) et des hauts-fonctionnaires de défense des Etats-Unis a eu lieu, pendant laquelle toutes les parties ont*

---

[78] « *Since September 11, 2001, the nation has focused more on the issue of cyberterrorism because although terrorists typically have used traditionnal methods of physical attack (explosives, kidnappings, and hijackings), their attention may move, with increasing frequency, toward cyberterrorism ».*

[79] « *Various forms of technological infrastructure may be vulnerable to such attack; pipelines, power plants, transportation, and other hard assets rely on cybertechnology. Further, communication systems used for financial, military, police, and corporate purposes suffer from the same vulnerability. ».*

[80] « *It is evident than in order to effectively combat the growing overlap of organized crime and cybercrime, a truly comprehensive and multilateral solution is required. In 2001, the combined nations of the European Union, the United States, Canada, Japan, and South Africa took a step in the right direction by drafting the Council of Europe Convention on Cybercrime. ».*

Organized crime and the Internet (Nelson-Palmer, 2006).

exprimé un désir d'améliorer la coordination entre l'industrie IT et les forces de l'ordre, cela des deux côtés de l'Océan Atlantique. En plus, la BSA a saisi l'occasion de présenter ses 200 études de sécurité, ce qui a accentué l'impact positif des initiatives industrielles menées pour combattre le cybercrime organisé (« Enquête de sécurité 2006 ») »[81].

Enfin, un article « *Cybercrime & Cybercriminals: An Overview of the Taiwan Experience* »[82], permet de présenter l'ensemble des types de cyberdélinquance relevés de 1999 à 2004 : « *Les cinq principaux types de cyberdélinquance concernent les messages en relation avec le commerce sexuel sur Internet, la fraude sur Internet, le vol, la piraterie et la cyber-pornographie* »[83]. En terme d'importance, cette étude montre le haut niveau d'étude généralement atteint par les acteurs de la cyberdélinquance ainsi relevé en Asie : « *La majorité des suspects détiennent des diplômes de hautes écoles (45.5 %) ; le deuxième plus grand groupe détient des licences (27.8 %) ; le troisième plus grand groupe représente ceux diplômés d'un lycée junior (17.9 %)* »[84].

L'intérêt de cette étude, au-delà de l'effort de relevé de la matière à la dimension d'un pays, propose des recommandations face au phénomène, ce qui n'est pas commun pour un article de recherche, mais cependant pertinent face à l'importance des faits. Quatre recommandations sont faites à destination du gouvernement, de la société, des écoles et du monde de la recherche. Pour le gouvernement, la mise en place d'une « *Task Force* » spécialisée en « cyberdélinquance » est fortement recommandée, ainsi que des lois plus complètes afin d'aider les officiers de police pour combattre ce phénomène, et leur permettre de relever les infractions et de déterminer les responsables. Pour les aspects sociétaux, les auteurs de cet article indiquent que seulement 1 % d'actes d'intrusion informatique sont relevés, cela le plus souvent par manque de sensibilisation

[81] « *In February 2005, a group of fifteen technology executives from the U.S.'s largest hardware and software companies, including Adobe, Dell, Microsoft, and IBM, urged the Bush Administration to create a national commission on organized cybercrime […] A year later, a meeting between the Business Software Alliance (BSA) and top law enforcement officials from the United States was convened during which all parties expressed a desire to improve coordination between the high tech industry and law enforcement officials on both sides of the Atlantic. Additionally, the BSA took the opportunity to release its 200 Security Survey, which highlighted the positive impact of industry-led initiatives in fighting organized cybercrime (2006 « Security Survey »).*

[82] *Cybercrime & Cybercriminals: An Overview of th e Taiwan Experience* (Lu, Jen, Chang, Chou, 2006).

[83] « *The top five are distributing messages regarding sex trading or trading sex on the Internet, Internet fraud, larceny, cyber piracy and cyber pornography* ».

[84] « *The majority of suspects held senior high school diplomas (45,5%) ; the second largest group was Bachelor's degree holders (27,8%) ; the third largest group was a junior high school graduates (17,9%).* ».

au phénomène, ainsi que par volonté de préserver sa réputation. Quant aux écoles, il existe un urgent besoin de transmission d'information relative à l'éthique, et la mise en place de programmes d'éducation complet en regard, le monde de la recherche devant aussi y être impliqué plus fortement[85] : « *Cette étude recommande que les agences de gouvernement, les professions légales, les écoles et les chercheurs travaillent ensemble contre la calamité croissante du cybercrime. C'est seulement avec un tel effort coordonné qu'un monde virtuel sûr pourrait être réalisé* »[86]. Colin Rose a estimé que « *La cybercriminalité est la troisième grande menace pour les grandes puissances, après les armes chimiques, bactériologiques, et nucléaires* »[87]. Cet état récent d'éléments pertinents de la recherche, quant à l'objet cyberdélinquance, démontre l'importance mondiale du phénomène, et des risques multiples que cette menace représente pour tous les secteurs d'activité au niveau mondial.

Après avoir présenté un état de l'art de la recherche en la matière, nous tenterons de définir le phénomène cybercrime, sous son acception la plus largement retenue, à savoir une activité illégale, élément clé de catégorisation du phénomène.

2) Définitions d'une activité illégale

La « cybercriminalité » est un terme intégré composé de « cyber » : terme usuel de la virtualité et associé à l'idée des réseaux IT (Technologies de l'Information), notamment Internet, et de « criminalité » : qualificatif de droit qui caractérise la qualification de l'infraction pénale concernée (le plus haut niveau de l'échelle des peines étant associé à la criminalité). À cet égard, il conviendrait plutôt de parler de « cyberdélinquance » plutôt que de « cybercriminalité » qui ne comprendrait que les cas les plus graves de la délinquance virtuelle. Le délinquant étant par définition celui qui est « hors la loi », dans son sens global (On peut d'ores et déjà noter que l'acceptabilité sociale de la condamnation pénale des faits délictueux par leurs auteurs serait peut-être

[85] *Defending Against Cybercrime and Terrorism* (*A new role for Universities*) (Aeilts, 2005).
[86] « *This study recommends that governement agencies, legal professionnals, schools and researchers work together against the growing cybercrime calamity. It is only with such coordinated effort that a safer cyberworld might be achieved.* ».
[87] Voir D. Martin et F.-P. Martin : *Cybercrime* (Paris, Press Universitaires), [2001], avant-propos.

facilitée si on leur accolait le terme de cyberdélinquance, moins stigmatisant et plus proche de la réalité habituelle des faits regroupés sous le vocable délinquance). Concrètement, la cybercriminalité correspond à un « cocktail » de menaces et d'agents menaçants : « *Threat is the frequency, or occurrence rate, of potentially adverse events* »[88] (La menace est la fréquence ou le taux de probabilité d'événements potentiellement nocifs). Toutes les menaces se caractérisent comme une cause potentielle de perte. Deux grandes catégories de menaces peuvent être, à ce niveau, retenues :

1) Les menaces non intentionnelles, de type accidentelles (pannes, accidents naturels), ou bien fortuites (erreurs humaines).

2) Les menaces intentionnelles : passives (ne modifient pas le comportement du système, parfois indétectables), ou bien actives (modification du contenu de l'information).

1) Les menaces non intentionnelles telle que l'erreur humaine**,** qui n'a pas la dimension d'un piratage informatique, peut être à l'origine de sinistres informatiques graves. L'erreur peut consister en une distraction, une négligence qui ne correspond pas au cadre régulier dans une sphère de sécurité donnée. La sensibilisation est un moyen qui aide à diminuer ces erreurs. Dans ce cadre nous trouvons également les désastres naturels (inondations, incendies, tempêtes). Ces risques sont difficilement gérables et doivent donc être impérativement prévus par un « *recovery plan* » (plan de reprise), prévoyant la reprise rapide de l'activité en cas de sinistre portant atteinte au système d'information. Enfin, les pannes matérielles et de logiciels entraînent souvent la perte du service offert par le système d'information (disponibilité) ; il est donc primordial de mettre en place des mécanismes afin de réduire ces pertes potentielles.

2) Les menaces intentionnelles : passives, elles ne modifient pas le comportement du système, et sont parfois indétectables, ou bien actives et modifient le contenu des informations. Généralement *via* réseaux, elles correspondent pleinement aux pirates informatiques, souvent qualifiés, notamment au sein du corpus, de *hackers*. Les actes classiques perpétrés, visant à altérer les services d'information et de communication Internet, sont les suivants :

[88] *Computer Security Handbook* (Bosworth et Kabay, 2002).

- *defacement* (altération de sites web) : cette attaque a pour but de transformer la page de garde d'une organisation afin de la ridiculiser.
- espionnage économique et industriel : l'espionnage économique et industriel a recours à des moyens illégaux, clandestins, intrusifs, coercitifs ou non (manipulation) pour acquérir des renseignements économiques.
- pression sur le personnel : toujours le point faible. Il peur faire l'objet de menaces de toute sorte (corruption, manipulations, entente de groupes, etc…).
- fraude commerciale : la carte bancaire est la plus touchée par la fraude commerciale. Le plus grand risque réside dans le fait que le serveur du site commercial qui stocke les données des cartes bancaires soit attaqué. Les fraudes commerciales sont nombreuses et leur origine en est difficilement détectable. Une solution est d'effectuer les achats en ligne sur un serveur commercial certifié offrant des garanties de qualité *via* l'apposition sur le site d'un certificat de qualité (qui répond à un référentiel).
- déni de service : le déni de service est une attaque qui entraîne la non-disponibilité d'une ressource. La durée du déni de service est variable, peut prendre plusieurs formes et vise des cibles très différentes. Les attaques se déroulent souvent de façon chronologique : consommation de bande passante, saturation de ressources, panne du système et des applications.
- sniffing (logiciel d'espionnage) : le sniffing est l'espionnage de manière passive d'un réseau informatique. Le logiciel dénommé « sniffer » surveille sans se faire repérer une ressource informatique du réseau en vue d'y trouver des informations utilisables pour pirater la ressource. Généralement, l'utilisation d'un « sniffer » consiste à récupérer les informations d'authentification (login + password) qui sont contenues dans chaque en-tête de paquets transitant via un réseau informatique.
- *IP Spoofing* (usurpation d'adresse *Internet Protocole*) : l'*IP Spoofing* vole l'identité d'un utilisateur connecté à un réseau informatique, afin de se faire passer pour quelqu'un d'autre.

Les menaces intentionnelles, *via* réseaux, exploitent généralement des failles bien connues (Avec l'évolution des systèmes ces failles sont désormais comblées, cependant, elles réapparaissent tout de même, de manière continuelle) :

- système de partage de fichiers ou d'imprimantes en réseau : partager des fichiers ou imprimantes en réseau est un véritable problème de sécurité. Dans un réseau local les partages doivent être correctement gérés afin de ne pas ouvrir d'accès confidentiels à des personnes non autorisées. Les partages sont souvent exploités à distance pour pirater le système d'exploitation d'un ordinateur. Les particuliers sont souvent les cibles principales de ce type de pratiques pirates, elles sont souvent concomitantes à l'exploitation d'un cheval de Troie (cf. *infra*) précédemment déposé.
- attaque de type *Netbios* : *Netbios* est le processus d'autorisation à accéder à des fichiers et répertoires situés sur d'autres machines. *Netbios* est le protocole utilisé par *Windows* pour partager des fichiers. Les pirates sont souvent à la recherche de machines dont le port 137 est ouvert (*Netbios*) afin d'exploiter une faille qui permet d'ouvrir un accès sur l'ordinateur victime.
- *ping* « de la mort » : ces attaques inondent un routeur ou un serveur de requêtes. Aucune donnée n'est détournée, il s'agit d'une attaque de déni de service qui permet d'agir sur la disponibilité des ressources.

Les actes classiques perpétrés, visant à altérer les services d'information et de communication, sont notamment les suivants : *defacement* (altération de sites web), espionnage économique et industriel, fraude commerciale, déni de service, *sniffing*, *IP Spoofing*, etc…(les deux derniers ayant été développés *supra*).

La menace, la source du risque, est l'attaque possible d'un élément dangereux pour toute ressource d'un système concernée. Le guide 73 de l'ISO[89] définit un risque par la combinaison de la probabilité d'un événement et de ses conséquences. Cette définition est généralement étendue et on définit un risque à l'aide de ce que l'on nomme l'équation du risque : Risque = f (menace x vulnérabilité x impact (cf. première partie I – I – 1)). Cette équation est celle qui est la plus couramment utilisée et la plus reconnue dans le domaine de la gestion des risques de sécurité. Elle joue un rôle fondamental dans l'identification et l'évaluation du risque. Mais surtout, toute menace constitue une cause potentielle de perte, il convient donc de définir l'impact préjudiciable potentiel. S. Bosworth et M. E.

[89] ISO/IEC Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standards.*

Kabay estiment que le coût de l'incident de sécurité correspond au dommage global subi par l'organisation victime[90]. Le cybercrime est une menace, au cœur de l'équation du risque de sécurité, formalisée par l'existence d'agents menaçants identifiés, et entraînant des préjudices. La menace de type agents humains est la plus rencontrée et la plus présente sur Internet. Les entreprises n'ont aucun moyen d'action sur ces menaces, en interne, elles peuvent avoir recours à des mesures disciplinaires à l'encontre d'un employé malveillant, mais si la menace est externe et virtuelle, c'est impossible. Il est hors de question de prendre des mesures en réponse à une attaque externe. Dans ce cas, seules les mesures judiciaires sont envisageables, ainsi que bien entendu la mise en conformité, visant à pallier les vulnérabilités identifiées.

Au cœur de la réflexion terminologique se trouve la problématique de la spécificité criminelle. La cybercriminalité est-elle une forme de criminalité nouvelle, exploitant des situations socio-économiques inédites à des fins malveillantes, ou bien doit-on inclure la dimension traditionnelle de la criminalité qui se donnerait seulement pour peine d'exploiter ce nouveau média que représente le réseau informatique mondial pour commettre des actes délictueux déjà connus et identifiés ? Deux approches s'opposent.

L'approche par le délit

Selon la généalogie du cybercrime proposée par Pansier et Jez, le premier délit informatique identifié fut commis aux États-Unis en 1966 (il s'agissait alors d'une altération des comptes d'une banque de Minneapolis) ; la criminalité des réseaux est cependant un phénomène plus récent, en expansion constante depuis le début des années 1980, qui s'est généralisée en France, depuis l'avènement d'Internet, fin 1994. La cybercriminalité se définit, communément, comme toute action illicite visant l'intégrité d'un site informatique déterminé ou bien menée à l'aide d'un outil informatique. « *Les vices les plus répandus ont trouvé une place à leur aise dans un espace virtuel où se*

[90] « *Event cost is the total cost in both real and soft dollars related to the total ramifications of a particular exploit experienced by a vulnerable target company or system* ».
Computer Security Handbook (Bosworth et Kabay, 2002).

développe une criminalité bien réelle »[91]. C. Nisbet[92] propose la définition la plus généraliste qui soit du phénomène, au point de ne pas être très éclairante sans doute : « *Le cybercrime est un crime commis en utilisant un ordinateur ou Internet* »[93]. Plus récemment encore, N. Kshetri (*The Simple economics of cybercrimes*, 2006) définit de manière tout aussi basique le cybercrime : « *Nous définissons le cybercrime de manière large comme un crime qui utilise un réseau d'ordinateurs quelle que soit la phase* ». De façon plus précise, mais restant large, D. Guinier affirme que la cybercriminalité correspond à « *tout ce qui regroupe les activités illégales et les actes directement commis à l'encontre ou à l'aide des technologies de l'information et de la communication (TIC), localement ou à distance, et qualifiables de délictueux ou criminels* », (Les systèmes d'information – Arts et pratiques, 2002).

L'approche par les opportunités nouvelles de l'informatique

La cybercriminalité est une nouvelle notion pénale pour un nouveau type de délinquance qui a grandi avec Internet. Ce vecteur constitue, en effet, le vecteur essentiel du crime numérique, une attaque passe dans la majeure partie des cas *via* le jeu de protocoles TCP/IP (*Transmission Control Protocol/Internet Protocol*) de ce réseau de réseaux. Dans notre rapport, nous prendrons peu en compte la transposition de la délinquance traditionnelle, qui utilise l'objet Internet pour ses actes illicites, mais bien les nouveaux sujets qui s'attaquent véritablement à l'objet. Nous appliquerons à notre analyse la maxime de J. Carbonnier : « *L'évolution des mœurs et des techniques donne matière à de nouvelles formes de délinquances* »[94]. « *Avec le développement des réseaux d'information et des nouvelles technologies sont apparues de nouvelles formes de criminalité. Si l'on considère l'ensemble des nouveaux moyens qui ont émergé des mondes de l'informatique et des télécommunications, c'est-à-dire les infrastructures, les réseaux, les outils ou les objets (portables, cartes à puce par exemple), on peut distinguer entre leur utilisation comme instruments nouveaux pour mener des activités criminelles traditionnelles et le fait qu'ils deviennent eux-mêmes l'objet des infractions (fraudes,*

[91] *La criminalité sur l'Internet* (Pansier, Jez, 2000).
[92] *Cybercrime and Cyber Terrorism* (Nisbet, 2002).
[93] Source : *Oxford English Dictionary Online*.

trafic, contrefaçons, intrusion dans les sites) »[95] Ainsi, « *l'émergence de l'ère informatique a donné naissance à de nouveaux comportements délinquants, difficiles à appréhender et marqués du sceau de l'immatérialité* »[96].

Le principe d'une nouvelle délinquance semble bien correspondre à Internet : « *la croissance exceptionnelle de cet univers de communication s'accompagne évidemment de son cortège de méfaits : les nouvelles technologies de l'information et de la communication sont à la fois l'objet et l'outil de nouvelles délinquances. On peut classer ces délinquances en fonction de l'objet technologique concerné ou en fonction de l'usage qui en est fait : si c'est un outil utilisé par le criminel pour commettre son forfait ou s'il en est l'objet même* »[97]. Les T.I.C. sont, soit les armes de l'activité criminelle (outils de la délinquance), soit les victimes d'actes criminels, notamment l'objet virtuel : « *[…] une taxe téléphonique, un programme informatique, des données personnelles ou de la monnaie électronique. Dans cette perspective, on a introduit une nouvelle notion pénale, l'atteinte à un système informatique, sa perturbation ou le fait de s'y introduire par les réseaux, lorsqu'on n'y est pas autorisé* »[98]. Ce sont les crimes et délits informatiques réprimés en France par la loi Godfrain de 1988.

Nous l'avons vu, *via* le juriste D. L. Carter[99], le cybercrime correspondant à toute activité illégale, donc punissable par la loi, qui utilise l'ordinateur soit comme outil (copie non autorisée d'oeuvres et produits déposés, pédophilie, terrorisme, vente illégale et communication) soit comme cible (intrusion dans des systèmes, dans des messageries personnelles...) par des personnes aux motivations diverses (espionnage militaire, industriel...etc, attaques des réseaux publics d'information pour les paralyser et nuire à un ennemi, enrichissement illicite, trafics, culte de la performance et du défi informatique, vandalisme informatique, etc…). Pour le professeur Carter, toutefois, l'appellation « cybercriminalité » dépasse la seule criminalité informatique et relève aussi de l'idée d'une criminalité de haute technologie relative aux ordinateurs, aux communications et à

---

[94] S*ociologie Juridique* (Carbonnier, 1978 : 401).
[95] *L'internet* (Capul, 2000).
[96] *La criminalité sur* l'Internet (Pansier, Jez, 2000).
[97] *L'internet* (Capul, 2000) .
[98] *L'internet* (Capul, 2000).
[99] *Computer Crime Categories : How Techno-Criminals Operate* (Carter, 1992).

l'électronique. Actuellement, la cybercriminalité désigne donc à la fois les attaques de tout type sur des systèmes informatiques (virus, tentatives d'intrusion, etc...), la diffusion de contenus illégaux (racisme, pédophilie, etc...), l'usurpation d'identité en ligne (fraude à la carte de crédit), l'escroquerie en ligne, le cyber-blanchiment d'argent, ou encore la question des atteintes à la propriété intellectuelle (par des échanges de particulier à particulier – « *peer to peer* »).

La délimitation juridico-légale de la cybercriminalité

Une nouvelle génération de délinquants et de technocriminels a donc vu le jour. « *L'évolution de ce phénomène cyber-criminel est constante et a suivi, au cours des vingt dernières années, celui de la démocratisation de l'accès à l'informatique et de la globalisation des réseaux. L'internet lui offre depuis peu une nouvelle plate-forme de développement* »[100]. La progression des crimes et délits réalisés par le biais de l'informatique a conduit les acteurs étatiques à se saisir de cet enjeu, apportant, ce faisant, leur contribution à l'identification sociale de ce type de pratiques frauduleuses.

La première loi de répression de la criminalité informatique provient des États-Unis. C'est le *Comprehensive Crime Control Act*, qui date de 1984. Il a été amendé par le *Computer Fraud and Abuse* dès 1986, et criminalise six types d'accès frauduleux aux systèmes informatiques en fonction de la finalité de l'opération d'intrusion réalisée :

1) Obtention d'informations sur des secrets d'Etat, portant préjudices aux intérêts des États-Unis ou favorisant une action étrangère.

2) Vol de données financières confidentielles.

3) Visite d'un ordinateur appartenant à une administration fédérale.

4) Accès frauduleux à un ordinateur avec une intention d'y commettre des méfaits informatiques.

5) Accès frauduleux à un ordinateur causant un dommage au moins chiffrable à 1 000 dollars.

6) Trafic de mots de passe, lorsqu'ils affectent le fonctionnement du commerce extérieur.

[100] *La criminalité sur* l'Internet (Pansier, Jez, 2000).

Il est aussi important de faire la distinction entre les attaques à l'aveugle sans cible déterminée, et celle prenant pour cible une organisation précise. Un autre organisme officiel a donc apporté sa contribution à la délimitation de la cybercriminalité, le centre de recherche du crime informatique[101] *Computer Crime Research Center*. Il distingue trois catégories selon la cible qui en est victime et donc selon les motivations des auteurs :

- Crime informatique contre des personnes (pédophilie, dommages divers, *happy slapping*…).
- Crime informatique contre la propriété (destruction de site, virus, vol de propriété intellectuelle ; le tout à distinguer si le but est de tirer un avantage concurrentiel ou pas),
- Crime contre un gouvernement (notion de terrorisme informatique).

En 1996, un sous-groupe des pays formant le G8 fut formé suite à une réunion à Lyon, afin d'étudier les nouveaux types de criminalité encouragés par, ou migrant vers, Internet (lutte contre le crime organisé). Ce « groupe de Lyon », qui fait l'objet de consultations suivies entre experts, employait alors le terme de « cybercriminalité » pour décrire, de manière relativement vague, tous les types de délits perpétrés sur Internet ou les nouveaux réseaux de télécommunications. « *Du fait de leur connectivité croissante, les systèmes et réseaux d'information sont désormais exposés à un nombre croissant et à un éventail plus large de menaces et de vulnérabilités, ce qui pose de nouveaux problèmes de sécurité* »[102]. Le développement d'Internet a entraîné celui d'une nouvelle forme de délinquance, qui, en utilisant les Nouvelles Technologies de l'Information et de la Communication (NTIC), menace tout à la fois les individus, les entreprises et les États. Internet devient ainsi la plate-forme présentant la plus forte croissance du crime dans le monde. Face à ce nouveau défi les États ont réagi. La communauté internationale a pris conscience des enjeux liés au développement des technologies numériques, notamment au travers de la Convention du Conseil de l'Europe sur la cybercriminalité (23 novembre

[101] Usuellement dénommé CCRC soit *Computer Crime Research Center*.
[102] *Lignes directrices de l'OCDE régisant la sécurité des systèmes d'information* (O.C.D.E, 2002 : 7) http://www.oecd.org/doc/M00033000/M00033183.doc.

2001) et de son protocole additionnel (7 novembre 2002). Les dispositions contenues dans ces deux textes sont déjà intégrées dans le droit français.

En France, depuis la loi Informatique et Libertés (1978), la législation française a pris en compte la problématique de la cybercriminalité avec la loi du 5 janvier 1988[103], dite « loi Godfrain », la loi du 15 novembre 2001[104] relative à la sécurité quotidienne, la loi du 18 mars 2003[105] pour la sécurité intérieure, la loi du 9 mars 2004[106] portant adaptation de la justice aux évolutions de la criminalité, la loi du 21 juin 2004[107] pour la confiance dans l'économie numérique, et la loi du 9 juillet 2004[108] relative aux communications électroniques et aux services de communication audiovisuelle.

« *En France, les enjeux de la sécurité informatique ont été pris en compte dans la loi Godfrain du 05 janvier 1988 reprise dans le nouveau Code Pénal sous les articles 323-1 et suivants. En cette matière l'arsenal juridique est formé de trois délits distincts visant les atteintes aux systèmes et les atteintes aux données* »[109].

Cet ensemble de lois définit les bases légales de la cybercriminalité sous trois axes :

- Les infractions spécifiques aux technologies de l'information et de la communication :

Sont catégorisés :

- les « atteintes aux systèmes de traitement automatisé de données (STAD) » (Loi Godfrain – articles 323-1 à 323-7 du Nouveau Code pénal institué par la loi du 22 juillet 1992, entrée en vigueur le 1er mars 1994) :

- suppression /modification de données : Code Pénal (article 323-1 al.1),
- altération de fonctionnement : Code Pénal (article 323-1 al.2),
- entrave au fonctionnement : Code Pénal (article 323-2),

[103] Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique.
[104] Loi n°201-1062 du 15 novembre 2001 relative à la sécurité quotidienne.
[105] Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure.
[106] Loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux evolutions de la criminalité.
[107] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[108] Loi n°2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle.
[109] La criminalité sur l'Internet (Pansier, Jez, 2000).

    - introduction, suppression, modification de données : Code Pénal (article 323-3),
    - groupement de pirates : Code Pénal (article 323-4),
    - tentative d'infraction sur un STAD : Code Pénal (article 323 al.1).
- les traitements automatisés de données personnelles,
- les infractions aux cartes bancaires,
- les chiffrements non autorisés ou non déclarés,
- les interceptions.

<u>- Les infractions spécifiques aux contenus des technologies de l'information et de la communication</u> :

    - la pédopornographie,
    - le terrorisme, la haine raciale, etc…,
    - les atteintes aux personnes (menaces, atteintes à la vie privée…),
    - les atteintes aux biens.

<u>- Les infractions facilitées par les technologies de l'information et de la communication :</u>

    - l'escroquerie en ligne,
    - l'atteinte à la propriété intellectuelle,
    - les jeux de hasard.

En 1994, le Service Central de la Sécurité des Systèmes d'Information (S.C.S.S.I) (devenu depuis D.C.S.S.I[110]) édite un guide intitulé « la menace et les vulnérabilités des systèmes d'information »[111]. Un chapitre présente plus particulièrement les attaquants (éléments menaçants) : « *Les motifs de l'agresseur sont nombreux et variés ; ils évoluent dans le temps. Il n'est pas possible de dresser une liste exhaustive des motivations des criminels en col blanc…* ». Concrètement, les menaces intentionnelles

[110] *Direction Centrale de la Sécurité des Systèmes d'Information, dépendant des services de M. le Premier Ministre.*
[111] *La menace et les attaques informatiques* (S.C.S.S.I., Service Central – N°650 du 28 mars 1994).

sont caractéristiques d'individus dont les motivations diffèrent et qu'il est alors possible de catégoriser :

Menaces à caractère stratégique :

- elles visent des informations concernant les secrets de Défense et la Sûreté de l'Etat, le patrimoine national (scientifique, technique, industriel, économique ou diplomatique), mais aussi la déstabilisation des systèmes dont dépendent ces informations ;
- pour une entreprise, voire un particulier, la menace d'origine stratégique aura pour but d'obtenir des renseignements sur les objectifs et le fonctionnement de l'organisation, obtenir un fichier client, des procédés de fabrication, des résultats de recherche et développement.

Menaces à caractère terroriste :

- elles regroupent toutes les actions concourrant à déstabiliser l'ordre établi *via* la destruction physique de systèmes voire *via* la désinformation ; l'effet recherché est souvent la médiatisation de l'impact engendré. La déstabilisation et l'atteinte à l'image d'un pays ou d'un gouvernement, y compris par la désinformation relayée par des groupes actifs sur Internet, constituent ainsi des menaces à prendre très au sérieux, désormais.

Menaces à caractère cupide :

- le but essentiel réside dans l'obtention d'un gain qui peut-être financier, matériel ou de tout autre ordre. L'atteinte permet un gain pour l'attaquant ou bien une perte pour la victime entraînant un gain pour l'agresseur.

Menaces à caractère idéologique :

- peut être vraisemblablement les plus importantes, et souvent les plus extrêmes. Cela correspond à un courant de pensée qui prédomine dans le milieu dit « *underground* » et qui constitue une menace évidente ;
- la mise en avant du caractère libre de l'information, ne pouvant être la propriété d'une personne, d'un groupe, d'une organisation ou d'un état.

Menaces à caractère ludique :

- ce sont les agissements par amusement ou loisir, souvent associés à une soif d'apprendre le domaine des technologies de l'information à travers leur pénétration. Souvent ce type d'attaques vise à la reconnaissance de l'attaquant.

Menaces à caractère vengeur :

- il peut s'agir de la réaction d'une personne en réponse à une frustration quelconque (exemple : licenciement, brimades, conflits, etc…) et qui n'a d'autre but que de détruire tout ou partie d'un système informatique ou de données, pour infliger un coup préjudiciable à l'adversaire. Ces motivations sont les plus fréquentes ; elles sont souvent combinées et engendrent ainsi des attaques lourdes de conséquences.

Après en avoir décliné les différentes définitions, nous proposons de détailler enfin un historique rapide du phénomène cybercrime, pour validation des faits et de leur représentation sociale.

3) Historique de la cyberdélinquance

Si l'on se réfère au rôle habituel des dictionnaires, comme enregistreur des tendances sociales du langage, alors il convient de souligner que l'année 2006 marque un tournant, traduisant un marquage fondamental dans le reconnaissance de la représentation sociale établie de la cyberdélinquance. En effet, depuis janvier on trouve dans le *Petit Larousse* les premières définitions des termes « *cybercriminalité* », « *hacker* » et « *pirate informatique* ».

- *Cybercriminalité* : « *ensemble des infractions pénales commises sur les réseaux de télécommunication, en particulier Internet. On distingue les infractions liées aux technologies (virus, piratage, etc.), celles liées aux contenus (racisme, pédophilie, etc.) et celles facilitées par les réseaux (copies illicites de logiciels ou d'œuvres audiovisuelles, etc.)* ».

- *Hacker* : (mot anglais) : « *personne qui par jeu, défi ou souci de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique. Reconnaissance officielle : « fouineur » ».*

- Pirate : « Reconnaissance officielle pour « cracker », personne qui contourne à des fins malveillantes les protections d'un logiciel, d'un ordinateur, ou d'un réseau informatique ».

- Pirater : « accéder, par effraction à un système informatique en vue de copier, d'en modifier ou d'en détériorer les informations ».

En août 2006, l'inspecteur général de l'industrie et du commerce au Ministère de l'Économie, des Finances et de l'Industrie, Gérard Pinchault (haut fonctionnaire chargé de la terminologie et de la néologie) a mis également en évidence de nouveaux mots entrés dans le langage de l'administration française, dont « pirate » pour « *cracker* ». Mais avant d'en arriver à cette « sanctification » linguistique par le dictionnaire, plus de vingt années se sont écoulées. Un historique rapide du phénomène de la cybercriminalité est nécessaire afin de mieux saisir son évolution tant sur le fond que sur la forme, jusqu'à sa représentation sociale acquise. Généralement, ce phénomène est décliné à travers la généalogie des *hackers*, personnages clés du phénomène qui font l'objet d'un historique conséquent.

Les années 1980 – Le temps des pionniers

Dès 1981, par exemple, Ian Murphy est officiellement la première personne inculpée pour un crime informatique, aux États-Unis, suite à son intrusion dans le système informatique de « *AT&T* », et à la modification du programme de facturation, étendant les heures creuses à toute la journée. Dès 1983, le film *War Games* popularise les *hackers* et le phénomène du cybercrime. En 1985, le phénomène du piratage continue à prendre de l'ampleur et à se généraliser avec la sortie aux États-Unis du journal Phrack *(*fondateur, Chris Goggan), premier magazine « *underground* » concernant le piratage informatique et les *hackers*. Depuis bien d'autres ont suivi, notamment en France (*Hackers*, *Pirates Mag*, *Hackerz Voice*, *Pirat'z*, *Hackmania*, *Zataz Magazine*) et aux Etats-Unis (« 2600 » créé par E. Goldstein – magazine majeur, car fédérateur actuellement de la communauté « *underground* » mondiale).

En 1986, le premier virus informatique voit le jour au Pakistan, il se nomme *Brain* et infecte les ordinateurs IBM. La même année, la première loi contre la fraude

informatique est votée par le Congrès américain et rend punissable par la loi l'accès non autorisé aux ordinateurs du gouvernement. L'année suivante, le virus *Jerusalem* est détecté. Il est conçu pour supprimer les fichiers infectés les vendredis 13 ; c'est un des premiers virus capables d'infecter et de détruire des fichiers.

En 1988, Robert Morris, « lâche » dans la nature le premier ver Internet qui va se répandre sur 6000 machines connectées. Robert Morris tentera d'expliquer après coup qu'il s'agissait d'une erreur de programmation ; il sera néanmoins condamné à 3 mois de prison avec sursis et à 10 000 dollars d'amende. Au même moment, Kevin Mitnick[112] est condamné à un an de prison suite à son intrusion dans les ordinateurs d'une grande société aux États-Unis.

En 1989, le phénomène des virus prend de l'ampleur, on en découvre une trentaine. En 1990, une guerre est déclarée entre deux groupes de *hackers* rivaux. Ils vont brouiller des lignes téléphoniques, faire des écoutes avec comme seul but de s'introduire dans les ordinateurs du groupe rival. À la fin de l'année suivante, il y a plus de 1000 virus en circulation. Il faut noter qu'il est indéniable qu'au tout début, les programmateurs de virus s'amusaient. Le virus « *Cookie* » affichait ainsi à l'écran « *I want a cookie* » (je veux un biscuit), de manière toujours plus insistante, jusqu'à ce que l'utilisateur frappe c-o-o-k-i-e sur son clavier. Mais à cette époque a succédé un usage plus ciblé et surtout plus destructeur du virus, notamment lorsqu'il s'agit de se venger d'un employeur en sabotant son installation informatique. Kevin Poulsen a ainsi été arrêté après avoir détourné tous les appels entrants dans une station de radio de Los Angeles et fait croire au nom de la radio que l'auditeur avait gagné des gros lots, tels que des voitures de luxe par exemple. En 1991, le virus *Michelangelo* est conçu pour détruire les données sur les ordinateurs, le 6 mars de chaque année, jour de la naissance de Michel Ange. La même année, les pirates « *Dark Angel* » et « *Nowhere Man* » lancent le premier générateur de virus, fonctionnant de manière simple, permettant à n'importe qui de créer un virus.

En 1992, un adolescent est arrêté à Washington pour avoir créé le virus *SatanBug*, qui détruit des données. *Monkey* est pour sa part un virus qui efface le disque-dur, lorsque l'on tente de le supprimer. En 1994, le mathématicien russe Vladimir Levin subtilise

[112] *L'art de l'Intrusion* (Mitnick, 2005) .

électroniquement dix millions de dollars à la Citybank ; s'introduisant sur le réseau bancaire international *SWIFT*, il fit ainsi perdre à la banque dix de ses plus gros clients. Interpellé à Londres en 1995, il fut condamné à trois ans de prison par un tribunal américain. De nombreuses ramifications de son réseau s'étendent en Europe, jusqu'en France, où les relais mafieux de Levin sont contrôlés à temps, notamment avant tout acte de piratage sur le réseau bancaire français. Actuellement, encore, l'équipe d'origine de Vladimir Levin, installée à Saint-Petersbourg, n'a pas été totalement mise hors contrôle. La même année, Mark Abene, alias *Phiber Optik*, un des leaders du groupe de pirates *Masters of Deception* fut emprisonné pour avoir détourné des lignes téléphoniques. À sa libération, il sera nommé par le magazine *New York Magazine*, dans le top 100 des plus intelligentes personnalités de la ville.

1995 – Année de la véritable prise de conscience du phénomène « cybercrime »

Elle est marquée par la seconde arrestation de Kevin Mitnick, recherché par le FBI pendant 7 ans, pour avoir détourné des informations confidentielles, piraté des centraux téléphoniques et violé des correspondances électroniques. Le préjudice est évalué à plus de 80 millions de dollars. Il est condamné à cinq ans de prison. A sa sortie, il est interdit d'accès aux téléphones, réseaux et ordinateurs. La même année, Philippe Blanchard, montre dans son livre[113] « *[…] une France en proie aux vices du hacking, cracking et autres « maladies » […] »* liées à l'espionnage industriel. Pour la première fois en France, des témoins parlent : les pirates eux-mêmes, la Police Judiciaire, la DST (Direction de la Surveillance du Territoire), France Télécom et diverses autres institutions. Les affaires de piratages informatiques relatées révèlent la vulnérabilité de certaines entreprises et de l'administration française, qui jugeaient, a priori, impossibles de telles intrusions. Elles montrent aussi à quel point les motivations des pirates peuvent être variées et laissent songeur quant aux conséquences potentielles de telles attaques. Le phénomène, qui a débuté fin 1994, commence à être relayé à travers la presse, cependant, la diffusion des revues reste encore limitée.

[113] *Pirates de l'informatique, enquête sur les hackers français* (Blanchard, 1995).

1996 - 1997 – Une menace qui s'installe

En 1996, *Concept*, le premier virus macro infectant les documents Word, devient le virus le plus répandu dans le monde. En France, de sources policières confirmées et vérifiées, les attaques informatiques se multiplient. Elles se concentrent notamment sur les réseaux universitaires, les faits émanant souvent du même réseau : notamment les écoles d'ingénieurs. Pour anecdote, l'E.P.I.T.A. (École *Pour l'Informatique et les Technologies Avancées* – Paris XIII) est même surnommée à l'époque « École *de Pirates Informatiques Très Avancés* ». De plus, les meetings « 2600 » évoqués dans la presse transparaissent dans la réalité et les premiers rendez-vous du groupe « 2600 » français prennent place, chaque premier vendredi du mois, Place d'Italie à Paris. Les diffusions de livres grand public sont en préparation ; un domaine de spécialisation apparaît dès lors : la sécurité des systèmes d'information.

1998 à 2003 – « Le champ de bataille Internet »

En 1998, un groupe de *hackers* dénommé « *The Cult of the Dead Cow* » développe *Back Orifice*, un « cheval de Troie » permettant un accès complet aux ordinateurs infectés ; de nombreux piratages ont lieu sur des sites militaires américains mais aussi sur le site du *New York Times*. On retient aussi la création du NIPC (*National Infrastructure Protection Center*) pour lutter contre le cybercrime et les sabotages des infrastructures informatiques aux États-Unis.

En 1999, des *hackers* serbes et kosovars se livrent une guerre électronique en piratant les sites de l'adversaire, tandis qu'en Chine deux cybercriminels sont condamnés à mort pour avoir *piraté* une banque et détourné 87 000 dollars vers leurs propres comptes. La même année, le virus *Melissa* créé par David Smith entraîne une panique dans le monde et cause plus de 80 millions de dollars de dégâts. Les risques de ces attaques deviennent encore plus importants lorsque deux groupes de *hackers* serbes menacent l'OTAN, affirmant qu'ils vont détruire leur système informatique en réponse à la guerre contre la Serbie. On retient aussi le piratage du site *web* de la Maison Blanche qui se retrouve « *defaced* » (image d'entrée du site transformée) par des graffitis rouges.

Dans le même ordre d'idées, un groupe de *hackers* appelé « *phreak.nl* » pirate plusieurs sites dont ceux de la *NASA* et du ministère de la Défense américain en « defaçant » les pages d'accueil pour mentionner « *Hack the Planet* » (voir Partie III – II – 2), modes d'organisation de la mouvance *« underground »*).

En France, afin de prévenir un désastre électronique, une « *Brigade Centrale de Répression contre le Crime Informatique – BCRCI* » est mise en place. Il s'agit de l'actuel O.C.L.C.T.I.C. (O*ffice Central de Lutte contre la Criminalité liée aux Technologies de l'Information*). En novembre 2000, le journal *Hackerz Voice* édite un entretien exclusif avec Charles Neal, agent spécial de la Brigade d'intervention des crimes informatiques du FBI. Une définition du « cybercrime » lui est demandée : « *on ne peut définir de manière précise le cybercrime. Le fait qu'un ordinateur soit l'outil d'un crime n'en fait pas pour autant un cybercrime, à notre avis. Quand on parle de crimes informatiques ont fait allusion à ceux qui sont en rapport avec une intrusion frauduleuse sur le réseau* ».

L'année 2000 est finalement riche en piratages. En février, les serveurs de sociétés symboles de la nouvelle économie font l'objet d'assauts électroniques concentrés. Les conséquences sont importantes : quelques heures de paralysie, un retentissement médiatique mondial immédiat et, le mois suivant, un krach boursier sans précédent des valeurs technologiques. En mai, des centaines de milliers d'internautes dans le monde reçoivent une déclaration d'amour : « *I LoveYou* », un virus de type ver (*Un ver est un logiciel très similaire à un virus. Cependant et contrairement au virus, un ver n'a ni besoin de l'intervention humaine, ni d'un programme hôte pour infecter une machine. Il dispose de son propre moteur, un automatisme qui lui permet de délivrer et d'exécuter automatiquement son code, comme par exemple un mini serveur de mail lui permettant de transmettre une copie de son code par e-mail, puis, par la suite, de chercher des nouvelles cibles à infecter. [cf. http://www.cases.public.lu]*).

En octobre, Microsoft découvre *QAZ* sur ses serveurs. Ce ver remplace l'exécutable *Notepad.exe* par un cheval de Troie. Le numéro un mondial du logiciel s'est fait visiter pendant plusieurs semaines sans s'en apercevoir. L'accès des *hackers* à sa base de programmes est cependant déclaré « *sans conséquence sur les produits qui seront fournis aux clients »*. Les faits sont désormais établis dans toutes les consciences, Internet

génère des dangers *via* des acteurs particuliers dénommés *hackers* ou pirates informatiques selon le diffuseur. Les préjudices peuvent être conséquents. En 1998, Serge Le Doran et Philippe Rosé définissent des crimes traditionnels qui profitent des N.T.I.C. : « D*e tout temps le crime organisé a su tirer un maximum de profit de la technologie. Les gangs de Chicago ont été parmi les premiers utilisateurs du téléphone. A l'heure d'Internet et des autoroutes de l'information, les nouvelles technologies apportent aux mafias de la planète des opportunités inespérées. Cosa Nostra, les triades chinoises, les gangs californiens, la mafia russe, pratiquent désormais des hold-up électroniques. Ceux-là même qui blanchissent aujourd'hui leur argent sale dans les paradis fiscaux le feront demain en utilisant la monnaie électronique* » [114].

En 2000, David Dufresne et Florent Latrive, sont auteurs du livre *Pirates et flics du Net*, qui traduit le développement nécessaire de la régulation face à la multiplication des affaires de cyberdélinquance. « *Dans l'ombre, ils manipulent les fichiers informatiques comme personne. En solo, ou en bandes, ils traquent les failles qui leur permettront de fouiller dans tous les ordinateurs connectés. Ce sont les pirates informatiques, hackers, héros négatifs d'un monde du réseau-roi et du tout-électronique* ».

Enfin, à partir de 2000, les premiers ouvrages de référence consacrés au sujet de la cybercriminalité sont publiés : « *Stratégie anti-hackers* »[115], est rédigé par dix des plus grands experts de la sécurité américaine et offre un panorama complet des techniques de piratages les plus utilisées. Le but est de mieux connaître son ennemi pour pouvoir s'en protéger. *Sécurité Optimale*, guide rédigé en 2001 par un ex-*hacker* (restant anonyme), destiné aux responsables de la sécurité des systèmes d'information, aux administrateurs réseaux et aux personnes qui doivent protéger leurs systèmes, leurs réseaux et leurs sites Internet de toute intrusion.

Enfin, avalisant un nouveau domaine rendu nécessaire en réponse à la menace, le livre référence de Donald L. Pipkin, *Sécurité des systèmes d'information*, vise, par de nombreux conseils sécurité, à permettre une protection globale de l'entreprise. Il permet de passer en revue les problèmes liés à la communication d'informations et de les hiérarchiser. *« Des check-lists résument ce qu'il faut considérer afin d'établir la*

[114] *Cyber Mafias* (Le Doran, Rosé, 1998).
[115] Stratégies anti-hackers (Russel, 2001).

meilleure stratégie de défense pour l'entreprise ». En 2003, trois spécialistes de la cybercriminalité exposent *via Hackers, le 5ème pouvoir* »[116], un portrait saisissant des différents individus et groupes qui ont lancé le *hacking* et érigé le piratage de sites Internet en un véritable mode d'expression. Depuis 2003, les actes de cyberdélinquance se multiplient, les techniques se spécialisent.

2003 à nos jours : évolution, sophistication et criminalisation des menaces

Les dernières années marquent l'évolution rapide des attaques de type *phishing*. L'origine du mot vient de « *password harvesting fishing* » (littéralement « pêche pour une moisson de mots de passe ») et donne l'image d'un pirate de données qui « pêche » des données personnelles et des mots de passe. Face aux virus et aux spams, le *phishing* fut considéré, très longtemps, comme un problème apparemment négligeable et donc par conséquent inconnu. Au milieu des années 90, apparut le premier grand cas de *phishing*. Le mot de passe de nombreux utilisateurs d'AOL (*American On Line*) a été usurpé de manière grossière pour utiliser leur compte d'accès Internet. Malgré des cas similaires dans les années qui suivirent, peu de gens avaient entendu parler du *phishing* jusqu'en 2003. En un laps de temps relativement court ce thème a toutefois pris une importance certaine. Tandis qu'en septembre 2003 le nombre d'e-mails de type *phishing* identifiés par MessageLabs n'était que de 279, ce chiffre atteignit deux millions un an après. Au total 18 millions d'e-mails de type *phishing* ont été interceptés en 2004, la tendance va en s'intensifiant.

L'aspect quantitatif n'est pas le seul important à ce niveau, l'énergie criminelle est également sous-jacente au phénomène. Le *phishing* s'est renforcé aujourd'hui grâce à des bandes organisées et il est pratiqué de façon systématique. Le procédé typique : tout d'abord, copies des sites Web existants d'entreprises et de marques en vue ; cela va des prestataires financiers et des banques jusqu'aux agences de voyage en ligne en passant par des sites de vente aux enchères. Par le procédé d'envoi en masse, organisé de manière professionnelle, des centaines de milliers de mails sont ensuite envoyés ; ceux-ci doivent attirer le destinataire vers un site « *web* » falsifié. L'espoir : une partie de ces courriers

[116] *Hackers ! : Le 5ème pouvoir – Qui sont les pirates de l'Internet* (Chatelain, Roche, 2003).

électroniques va atteindre des clients existants ou des intéressés potentiels de ces entreprises. Le but : les clients crédules donnent ensuite leurs données personnelles, leurs mots de passe ou leur numéro de carte bancaire, comme lors d'une commande fictive de marchandises. Comme pour les *spams*, un pourcentage de réussite très faible d'un ou de deux pour cent est déjà suffisant pour que les *phisheurs* soient satisfaits de leurs efforts ; finalement cet envoi massif est pour ainsi dire sans frais. Et la réalité montre qu'il est bien au-dessus dans la plupart des cas : L*'Anti-Phishing Working Group* (*APWG*) créé par l'industrie et le commerce comme contre-offensive estime ainsi le pourcentage de réussite des attaques de type *phishing* à cinq pour cent (Une récente étude relevé par un *HoneyNet* (G-D de Luxembourg), montre que 15 personnes sur 40 000 *mails* de *phishing* envoyés, répondent en fournissant sans réserve leur codes et données personnelles. Il appert que les sites Internet frauduleux sont immédiatement interceptés par le réseau aussitôt qu'un client attentif les a découverts ou qu'ils sont identifiés par les services de surveillance. Malgré tout, selon les données de l'APWG, la durée de vie d'un site *phishing* est en moyenne de 6,4 jours, sachant que le chiffre maximal est de 31 jours. Combinés à des taux de retour à atteindre, les exploitants peuvent être certains que les coûts et les dépenses valent la peine : les « pertes directes » pour les banques ou les instituts de crédit s'élèvent entre-temps à des milliards. Comme la situation juridique entre les victimes et les entreprises n'est pas claire, ce sont les clients finaux qui supportent eux-mêmes le plus grand préjudice. Celui-ci a été estimé par Gartner à plus de 50 milliards d'euros.

Beaucoup de grandes banques ont été touchées par le *phishing* dans le monde. En Allemagne, la *Postbank* a dernièrement de nouveau été la cible des attaques de type *phishing*. Les *mails* avertissent ici des clients potentiels de manière ironique d'un danger d'usurpation, c'est pourquoi celles-ci doivent conforter la sécurité de leur compte (mais sur un site falsifié). Le site falsifié de la *Postbank* a été bloqué rapidement, cependant le risque de nouvelles créations de phishing persiste. *MessageLabs* intercepte actuellement entre deux et cinq millions d'e-mails de type *phishing* par mois, qui chaque jour dirigent vers 80 à 100 sites falsifiés. Les groupes-cibles les plus récents d'attaques de type *phishing* sont outre les clients des banques en ligne, également des utilisateurs de services de paiement comme *Paypal* et des plate-formes de commerce électronique comme *eBay*.

Très récemment est en outre apparue une page *Web* falsifiée pour commander en ligne des billets d'avion. Chaque organisation professionnelle qui fait passer des transactions par le biais d'Internet représente une cible potentielle. Les conséquences pour les entreprises concernées vont de la méfiance des clients et du ternissement de l'image jusqu'aux conflits juridiques en passant par une perte de productivité.

La méthodologie utilisée se spécialise. Aujourd'hui, le progrès technologique n'est pas à négliger. Les *phisheurs* sont arrivés – tout comme les *spammeurs* – à prendre le contrôle des réseaux à large bande passante et à les utiliser en tant que «*Botnets*» pour abriter le site falsifié. Par ce biais, ce n'est pas simplement la véritable identité du site qui reste plus longtemps dissimulée. En raison de l'utilisation d'un réseau partagé venant d'ordinateurs escamotés, même des attaques de type *phishing* de grande envergure peuvent être exécutées en diffusion massive.

Lors des dernières attaques de type *phishing*, de nouvelles techniques douteuses sont apparues qui exigent moins d'intervention de la part de l'utilisateur. Les *phisheurs* diffusent dans les mails envoyés en masse des troyens, des vers et des programmes *spyware* qui utilisent les failles de sécurité dans les systèmes d'exploitation et vont se nicher sur les disques durs. Les pirates invisibles y enregistrent les suivis des touches, les adresses Internet visitées ou les mots de passe. Les données capturées sont ensuite envoyées pour une «réutilisation» à des centres de données cachés. De plus, les «techniques» d'ingénierie sociale se sont entre-temps affinées ; ainsi des *phisheurs* offrent par exemple à des destinataires naïfs de leur créditer une somme sur leur compte lorsqu'ils participent à un sondage en ligne. Pour recevoir l'argent on doit évidemment donner son numéro de carte bancaire et son code PIN. Parfois les fraudeurs se font passer pour des employeurs potentiels et demandent des données personnelles comme les coordonnées bancaires. Tellement contents d'obtenir un emploi, les candidats oublient souvent de rester vigilant. Et finalement : plus un profil de données personnelles volées est complet, mieux il sera revendu. Le commerce d'identités volées est aussi un commerce lucratif.

Récemment, une nouvelle forme de menace est apparue ; il s'agit du « *pharming* ». Ici les pirates de données reprennent une méthode bien connue dans les cercles de piratage : il s'agit du « *domain-spoofing* ». L'adresse Internet d'un site Web est détournée

de manière raffinée par le fait que la définition de l'adresse est manipulée sur Internet. L'adresse IP du serveur, code numérique, est normalement transmise par la définition de l'adresse à partir de l'adresse URL qu'un utilisateur inscrit dans la fenêtre de son navigateur. Les serveurs DNS (*Domain Name System*) qui administrent de vastes tableaux avec des noms de domaine et d'adresses IP correspondantes prennent en charge cette tâche. Lors du *pharming* les serveurs DNS sont manipulés par une méthode qui s'appelle le « *DNS-Cache-Poisoning* » de sorte que les véritables adresses IP ne sont plus transmises par les noms de domaine, mais par les adresses IP trafiquées des serveurs Web sur lesquelles finalement l'utilisateur atterrit. Une autre variante du *pharming* transforme le fichier « *host* » qui peut prendre en charge de la même manière la conversion de l'URL en adresse IP sur les ordinateurs *Windows*. Il contient un tableau avec les adresses IP les plus utilisées. Si ce fichier est écrasé, l'utilisateur reçoit automatiquement lors de chaque sélection d'une page souhaitée, un page contrefaite. Pour ce faire, il faut en outre qu'un programme nuisible soit préalablement arrivé sur l'ordinateur de l'utilisateur pour prendre en charge les modifications.

Les serveurs *proxy* sont un autre danger du *pharming*. Beaucoup d'internautes utilisent des serveurs *proxy* pour abriter leur propre adresse IP. Dans le pire des cas l'adresse d'un tel serveur *proxy* est attaquée et l'utilisateur voit apparaître une page de banque contrefaite bien que son système travaille correctement.
Les attaques de type *pharming* sont particulièrement dangereuses parce que l'utilisateur même en tapant l'adresse ou en utilisant ses favoris n'arrive pas à la page souhaitée mais sur le serveur manipulé. Depuis ce développement d'activités « dangereuses », de nombreux instruments de surveillance se sont mis en place, les détails statistiques récents de cette activité seront détaillés, à ce titre, en chapitre III – 2 de notre première partie.

Après avoir présenté cet historique du phénomène cybercrime, il semble important de décliner spécifiquement les différentes réalités cybercriminelles possibles, pour prendre plus en avant en compte sa réelle « sédimentation sociale ».

III – Identification des cadres de construction et de renforcement de l'image statistico-démonstrative et illégale de la cyberdélinquance

Pour cadre de la construction et comme révélatrices de l'image illégale et statistico-démonstrative, nous relèverons les principales entités permettant de déterminer cet état de fait, à savoir les professionnels du champ de la sécurité de l'information. Nous avons donc détaillé les initiatives nationales de sensibilisation à la sécurité des systèmes d'information et de la communication. Il importe de spécifier ces entités qui, par leur existence, permettent de transcrire la réalité d'un phénomène réel pour lequel elle propose des solutions spécifiques[117]. Principalement, nous détaillerons la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information), le CLUSIF (CLUb de la Sécurité de l'Information France), la CNSSI (Commission de Normalisation pour la Sécurité des Systèmes d'Information), CASES (*Cyberworld Awareness and Security Enhancement Structure*), CLUSSIL (CLUb de la Sécurité des Systèmes d'Information Luxembourg), et CNLSI (Comité de Normalisation Luxembourg pour la Sécurité de l'Information). Après avoir relevé de la pertinence des entités de la sécurité de l'information et de la communication, pour répondre aux besoins face aux menaces des systèmes concernés, nous présenterons les statistiques les plus éprouvées dans le domaine de la cyberdélinquance. Il importe de les détailler avant de se questionner sur la génération d'une image différente possible de la cyberdélinquance, et en conséquence du pirate informatique.

[117] Note : en regard de notre implication nationale et des liens étroits entre la France et le Grand-Duché de Luxembourg (à ce titre, de nombreux contacts ont eu lieu et sont encore en cours entre le Grand-Duché de Luxembourg et la France) quant à la promotion de la sécurité de l'information, nous présenterons des structures centrales de la sécurité de l'information émanant de ces deux pays.

1) Les « entrepreneurs » de la sécurité de l'information

Exemples d'organes de sécurité de l'information en France et au Grand-Duché de Luxembourg

- DCSSI – Direction Centrale de la Sécurité des Systèmes d'Information

En France, la DCSSI joue le rôle d'organe national fédérateur pour cette thématique sous l'égide du Secrétariat Général de la Défense Nationale (SGDN – http://www.ssi.gouv.fr). Ce serveur fédérateur, portail de la sécurité des systèmes d'information (SSI) français très riche, offre de nombreux documents et méthodologies afin d'améliorer ses préoccupations relatives à la sécurité des systèmes d'information, notamment *via* la promotion de la méthode de gestion des risques de sécurité EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité).

L'entretien avec M. Stéphane Piallat, Commissaire divisionnaire à la DCSSI, a notamment permis de mieux comprendre cette structure (voir troisième partie - I - 1)). La DCSSI, dans ses missions de SSI, répond à deux objectifs principaux :

- Assurer la SSI de l'Etat (administrations et infrastructures vitales).

- Créer les conditions d'un environnement de confiance et de sécurité propice au développement de la société de l'information en France et en Europe.

La connaissance des milieux des pirates informatiques et des cybercriminels n'est pas au cœur des problématiques traitées par cette direction de la Défense Nationale. L'objectif ici n'est pas de combattre la cybercriminalité, mais de mener une réflexion au niveau interministériel et de fournir des analyses concrètes en la matière. L'aspect opérationnel est également représenté. En effet, le Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques (CERT-A – cf. troisième partie – III – 2)) présente deux aspects liés à la cybercriminalité :

1) l'assistance aux services d'enquête,
2) le travail de veille.

L'activité des professionnels du CERT-A profite exclusivement à la défense des intérêts de l'Etat, et à l'administration au sens large. L'assistance et l'expertise technique

sont destinées par exemple aux services de la police judiciaire et sont fournies par des ingénieurs de très haut niveau. On s'adresse à ces experts de la sécurité des systèmes d'information pour des questions très complexes. Le travail de veille est pris en charge par le service COSSI qui fait partie du CERT-A. Il s'agit d'alerter, d'informer les responsables de l'Etat en cas d'attaque informatique (cyber-terrorisme, intrusions sur les serveurs du gouvernement). Le conseil, la correction et l'analyse de cas concrets sont les trois niveaux de compétence du CERT-A. Le SGDN peut, si besoin, mener une procédure administrative qui consiste à apporter du secours aux administrations attaquées.

La DCSSI est donc une direction à l'approche très opérationnelle appliquée en matière de conseil, d'analyse et d'intervention concrète. Un centre de formation est également rattaché à cette direction : le CFSSI[118] (Centre de Formation SSI) ; il dispense des formations de très haut niveau aux fonctionnaires de l'Etat français, aux services d'enquête, etc. Des formations *ad hoc* sont également créées à la demande (ex. : stages organisés pour la Gendarmerie Nationale). Pour les formations de « réponse sur incidents de sécurité », les intervenants sont des ingénieurs du CERT-A, ainsi que d'autres professionnels et experts en matière de protection des systèmes d'information. Il existe un module sur la cybercriminalité qui propose une approche très concrète concernant la mise en application du cadre juridique.

- CLUSIF – CLUb de la Sécurité de l'Information France

Au niveau associatif, le CLUb de la Sécurité de l'Information France (CLUSIF : www.clusif.asso.fr) joue un rôle non négligeable en terme de réflexion globale sur la problématique. Chaque année ce club relève les tendances sur la cybercriminalité

[118] Note : le CFSSI permet également de suivre, par exemple, les formations relatives à la méthodologie de gestion des risques de sécurité EBIOS® (Cf. troisième partie – I – 2). Nous avons notamment rencontré M. Robert Longeon, en date du 24/02/06, alors Chargé de Mission SSIC au CFSSI, (actuellement chargé de mission Sécurité des Systèmes d'Information au CNRS), qui nous a présenté le catalogue de formation de haut niveau présenté par cet organisme (nous avons suivi depuis, à ce titre, la formation EBIOS) et l'intérêt mesuré de la perception juste du phénomène du cybercrime, notamment en regard de ses aspects sociétaux en France, ainsi que de son traitement aux fins de protéger les diverses infrastructures sensibles et critiques en France. M. Longeon est co-rédacteur du *Guide de la Sécurité des systèmes d'information* (Archimbaud, Longeon, 1999).

effective de l'année écoulée (voir première partie « état statistique – quantitatif » – III – 2)), il s'agit d'une véritable synthèse médiatique des actes de cybercriminalité.

Les buts sont de :

- mettre en avant quelle a été, au cours de l'année écoulée, l'apparition des nouveaux risques,
- les tendances vis-à-vis des risques déjà connus.

Il s'agit d'un :

- indicateur fortement attendu désormais chaque année, notamment par les autorités françaises qui s'informent des tendances du cybercrime (dans ce document les attentes des problématiques particulières du cybercrime sont retenues par consensus par des experts sécurité).

- CNSSI – Comité de Normalisation de la Sécurité des Systèmes d'Information

En France, il existe une commission de l'AFNOR (Agence Française de NORmalisation) ; la Commission Nationale pour la Sécurité des Systèmes d'Information (CNSSI) a pour but de veiller à la promotion de l'utilisation de techniques normalisées comme vecteur important, ce qui permet la transparence et la comparaison. En tant que miroir de ISO/JTC1/SC27 (« *IT Security Techniques » de Joint Technical Committee 1, de International Standardization Organization*), CNSSI assure un rôle transversal de coordination sur tous les secteurs applicatifs de l'ISO concernés par le thème de la SSI. CNSSI est un forum de pilotage des sujets de sécurité traités par l'ISO et d'échange d'informations pour d'autres comités internationaux traitant de la SSI.

Rôle et missions :

- participer, aux plans national et international, à la normalisation dans le domaine de la SSI,
- renforcer et assurer un rôle transversal de coordination avec les secteurs applicatifs (banques, santé…etc),
- assurer un minimum de suivi des travaux de certains comités internationaux (IETF (*Internet Engineering Task Force*), ETSI (*European Telecommunications Standards Institute*), etc…),

- identifier les thèmes à développer, non encore traités au niveau de la normalisation.

- CASES – Cybeworld Awareness & Security Enhancement Structure

Au Grand-Duché de Luxembourg, la structure CASES (*Cyberworld Awareness & Security Enhancement Structure* – www.cases.public.lu) joue le rôle de portail national de la sécurité de l'information. Il s'agit d'un projet pluriannuel du Ministère de l'Économie et du Commerce extérieur visant à sensibiliser et à prémunir contre les risques liés à la sécurité de l'information. Il fournit à travers un site Internet, des formations, et une structure d'alertes rendues anonymes, tout en mettant l'accent sur la compréhension facile des enjeux par les internautes et les PME. CASES crée, participe et gère aussi une structure européenne d'échanges d'information sur le domaine de la sécurité de l'information. Ses missions sont de :

- sensibiliser par l'éducation,
- prévenir par des campagnes,
- promouvoir les « *best practices* » SSI,
- offrir des solutions aux problèmes,
- émettre des alertes,
- promouvoir et renforcer l'importance des concepts de sécurité,
- favoriser la coopération et l'échange.

- CLUSSIL – CLUb de la Sécurité des Systèmes d'Information Luxembourg

Au Grand-Duché de Luxembourg, le CLUb de la Sécurité des Systèmes d'Information Luxembourg (CLUSSIL, www.clussil.lu) joue globalement le même rôle que le CLUSIF en France. Les objectifs de cette association, créée en 1986, sont :

- prendre, de manière générale, toutes initiatives susceptibles de contribuer à la promotion et à l'amélioration de la sécurité des systèmes d`information,
- la rédaction et la diffusion des méthodologies et de recommandations concernant la sécurité des systèmes d'information,

- le recueil dans une banque de données d'informations relatives aux sinistres informatiques, afin de pouvoir analyser les facteurs de risques et d'améliorer la prévention.

Le CLUSSIL réunit de nombreux groupes de travail et de rencontres SSI. Son rôle est important au Grand-Duché de Luxembourg quant au suivi de l'évolution de la matière. Il demeure un relais essentiel.

- CNLSI – Comité de Normalisation Luxembourg pour la Sécurité de l'Information

CNLSI (Comité de Normalisation Luxembourg pour la Sécurité de l'Information), correspond au Comité technique JTC1/ISO/SC27 Luxembourg, composé d'experts de la sécurité de l'information, et qui a pour rôle de commenter et de voter les normes ISO/SC27, en regard des spécificités et intérêts du G-D de Luxembourg. L'intérêt repose souvent sur la qualification en construction de nombreux points relatifs au cybercrime, un exemple de commentaire ISO précise par exemple la définition d'une attaque numérique ainsi : « *Une attaque consiste en une tentative concrète d'exploitation d'une vulnérabilité par une menace, effectuée par un utilisateur malveillant. Il s'agit d'un événement pouvant mener à un incident* »[119].

L'organisation de l'europe pour la sécurité de l'information

La sécurité des réseaux est un domaine complexe notamment lorsqu'il s'agit de l'améliorer. Il en ressort un véritable défi. Pour ce faire, les institutions européennes ont traité le sujet et dégagé deux axes de travail forts :

[119] « *ISO First Working-Draft « Information Security Management Systems – Fundamentals & Vocabulary » : « Proposition for a new definition for Attack «Attack is the concrete attempt of exploitation of a vulnerability by a threat, done by a malicious user. It is an event that can lead to an incident.* » *More information about the notion* of « *attack* » *can be found in : Donald G. Firesmith, Common Concepts Underlying Safety, Security, and Survivability Engineering, Technical Note CMU/SEI-2003-TN-033, Software Engineering Institute, Pittsburgh, Pennsylvania, December 2003.* »

- Améliorer la sécurité des systèmes d'information, au niveau organisationnel, technique et légal (agir sur les vulnérabilités).
- Renforcer la lutte contre la cybercriminalité (agir contre les menaces).

L'Union européenne travaille donc en ce sens ; le Plan d'action eEurope[120] 2002 (Bruxelles – 14.06.2000) a souligné l'importance revêtue par l'amélioration de la sécurité des systèmes d'information et la lutte contre la cybercriminalité. Au niveau européen, la sécurité des réseaux est considérée comme un élément essentiel pour instaurer la confiance des utilisateurs, notamment dans le commerce électronique.

Le Plan d'action eEurope 2002 avait dégagé trois domaines d'action :
- Améliorer l'offre de solutions pour la sécurité d'Internet.
- Mieux coordonner la lutte contre la délinquance informatique.
- Renforcer la sécurité d'accès aux services électroniques en encourageant l'utilisation de cartes à puce sous toutes les formes.

Le Plan d'action eEurope 2005 succèdera au plan d'action eEurope 2002, avec pour objectif une « *Société de l'Information pour tous, dans un cadre sécurisé* ». Les diverses mesures prises par l'Union européenne et le Conseil de l'Europe sont résumées ci-après.

- **Communication[121] de la Commission européenne (Plan e-Europe 2002) : 26.01.2001[122]** : « *créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité* » (COM/2000/0890 final).

La Commission européenne constitue l'organe exécutif de l'Union européenne ; situé à Bruxelles, elle veille à la correcte application des dispositions des traités et des décisions prises par les institutions de l'Union. Cette Communication de la Commission prévoit une proposition visant à rapprocher d'avantage les systèmes de droit pénal positif dans le domaine de la « criminalité de haute technologie ».

[120] La Commission européenne a lancé l'initiative « eEurope » en décembre 1999, afin de « *mettre l'Europe en ligne* ».
[121] Une Communication telle qu'une Recommandation ou un Avis ne constitue pas un instrument contraignant.
[122] http://europa.eu.int/eur-lex/fr/com/cnc/2000/com2000_0890fr01.pdf.

- <u>Communication de la Commission européenne : 06.06.01</u>[123] : « *sécurité des réseaux et de l'information : proposition pour une approche politique européenne* » (COM(2001)298 final).

Cette Communication analyse les problèmes de sécurité des réseaux et de l'information, détermine une approche politique européenne de ce phénomène. Elle met en évidence le manque flagrant de sensibilisation objective de l'utilisateur final, mais aussi l'importance de la collaboration entre système d'alerte et d'information de type *CERT*.

- <u>Convention cybercrime du Conseil de l'Europe : 23.11.2001</u>[124]**<u>.</u>**

Le Conseil de l'Europe est une organisation internationale dont le siège est à Strasbourg et rassemblant 43 états démocratiques de l'Europe. La Convention a été signée au Parlement hongrois à Budapest par vingt-six pays membres du Conseil de l'Europe et les quatre Etats non membres ayant participé à son élaboration (Etats-Unis, Canada, Japon et Afrique du Sud (statut d'observateurs)).

Une convention constitue un outil de coopération internationale unique. A l'origine, le chantier a été ouvert en 1997 par les quarante trois Etats membres du Conseil de l'Europe et les quatre pays observateurs. Le texte a connu vingt-sept versions successives. Le but poursuivi est d'harmoniser les législations pénales nationales afin de lutter contre la criminalité spécifique aux technologies de l'information (c'est-à-dire contre les réseaux informatiques, par exemple : atteinte au système de traitement automatisé de données par intrusion volontaire dans le serveur d'une entreprise), mais aussi contre la criminalité facilitée par les technologies de l'information (c'est-à-dire à travers les réseaux informatiques, par exemple : pédophilie etc….).

L'objectif est de poursuivre une politique pénale commune destinée à protéger la société contre la cybercriminalité, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale. La Convention s'avère évolutive ; des

[123] http://www.europa.eu.int/eur-lex/fr/com/cnc/2001/com2001_0298fr01.pdf.
[124] http://www.conventions.coe.int.

protocoles additionnels pourront la compléter afin de l'adapter aux nouveaux défis dans le contexte international. La Convention tente de concilier à la fois les intérêts de l'action répressive qui doit être menée et le respect des droits de l'homme fondamentaux, à savoir la liberté de rechercher, d'obtenir ou de communiquer des informations et des idées de tout type (même au-delà des frontières) et le droit au respect de la vie privée.

***- Council Framework Decision on attacks against information systems (Proposal for presented by the Commission*)** (Décision cadre du Conseil sur les attaques des systèmes d'information) (Proposition par la Commission) : 19.04.2002[125].

Une Décision est exécutoire (intégralement) pour les destinataires qu'elles désignent ; ainsi, elle ne requiert pas de législation nationale pour son exécution ; elle peut être adressée à un, à plusieurs ou à tous les Etats membres, à des entreprises ou à des particuliers.

Cette Décision spécifie que le Droit Pénal des Etats membres comporte des vides juridiques importants susceptibles d'entraver la capacité des services de police et des autorités judiciaires à lutter contre la cybercriminalité visant les systèmes d'infraction. L'Union européenne prend des mesures dans ce domaine afin de garantir l'efficacité de la coopération des services de police et des autorités judiciaires.

Même si la cybercriminalité est alors encore considérée comme un phénomène marginal, elle n'en demeure pas moins une forme de criminalité qu'il faut combattre. Cette décision va contribuer à améliorer les infrastructures d'information européennes aux fins de mise en place d'une économie fondée sur la connaissance. Par crimes, la Commission vise aussi bien le piratage que les virus ou les attaques par déni de service. La demande est faite aux états membres de punir les actes de cybercriminalité par une peine maximale qui ne doit pas être inférieure à quatre ans d'emprisonnement.

[125] http://europa.eu.int/scadplus/leg/en/lvb/l33193.htm.

– Communication de la Commission européenne (dans le cadre du Plan e-Europe 2005) : 28.05.2002 : « *une société de l'information pour tous* » (COM(2002) 263 final)[126].

Ce plan d'action eEurope 2005 en définition succèdera au plan d'action eEurope 2002 approuvé par le Conseil européen à Feira en juin 2000.

Cette Communication vise à créer un environnement favorable à l'investissement privé et à la création d'emplois, à stimuler la productivité, à moderniser les services publics et à donner à chacun la possibilité de participer à la société mondiale de l'information. eEurope 2005 vise par conséquent à stimuler le développement de services, d'applications et de contenus sécurisés, exploitant une infrastructure à large bande abondamment disponible (donc sans entrave communicationnelle).

Depuis, et suite à l'ensemble de ces considérations marquées, l'Union européenne a mis en place une agence européenne en charge de fédérer les aspects de sécurité de l'information pour ses membres : l'ENISA (Agence Européenne de la Sécurité de l'Information de l'Union Européenne[127]).

Les instances de répression

S'il n'existe donc pas de vide juridique à proprement parler concernant tout ce qui relève de l'espace du Net, on constate malgré tout qu'il y a quelques difficultés pour y transposer le droit courant. Par conséquent, a été créé un certain nombre de commissions et même d'initiatives privées pour pallier cette difficulté de transposition (voir partie III – I – 1)).

En France, par exemple, la D.S.T. (Direction de la Surveillance du Territoire) dispose depuis les années 80 d'une « section informatique ». En 1994, la police judiciaire de Paris créa un Service d'Enquêtes sur les Fraudes aux Technologies de l'Information

[126] http://europa.eu.int/information_society/eeurope/news_library/eeurope2005/index_en.htm.
[127] http://www.enisa.eu.int.

(SEFTI), dans lequel une vingtaine de policiers sont chargés des usages frauduleux des télécommunications.

La même année, une Brigade Centrale de Répression de la Criminalité Informatique (BCRCI) fur créée à la direction centrale de la police judiciaire. Depuis septembre 1997, le ministère français de l'intérieur a mis en place un service spécial, la « cellule Internet » au sein de la direction générale de la police nationale qui emploie une douzaine de policiers spécialisés, issus à la fois des directions centrales de la police judiciaire, des Renseignements Généraux (R.G.) et de la surveillance du territoire. Les débuts furent prometteurs, puisque 161 procédures furent ouvertes en 1997 et 85 en 1998.

L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLTIC) est opérationnel depuis 2001 et succède à la Brigade Centrale de Répression de la Criminalité Informatique (BCRCI) à une époque où Internet était encore une curiosité technologique. Depuis, les choses ont bien changé. Cet office central, composé de 35 membres, travaille en collaboration avec les services de police, de gendarmerie, des douanes et la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF).

La matière principale traitée, par l'ensemble de ces instances, est le piratage informatique. L'ensemble des enquêtes et résultats est souvent reconditionné *via* des statistiques publiques, qui permettent de rendre compte du phénomène.

2) Des statistiques éprouvées

Bien que spécialisé et disposant d'instrument de mesure non négligeables, ces entités de sécurité sont-elles en mesure de mesurer le « taux de cybercrime » effectif chaque année ? Certainement non. En effet, un nombre non déterminé d'agressions ne sont pas déclarées à la police (par peur d'atteinte à l'image de marque, de mauvaise publicité, de perte de confiance de clients, ou encore de représailles). De fait, de nombreuses plaintes ne sont pas enregistrées par la police. Il existerait donc un « chiffre noir » de la délinquance mesurant l'écart entre la délinquance déclarée et la délinquance réelle. Dans cette partie nous nous attacherons à présenter l'état des statistiques

finalement disponibles sur la quantification du phénomène cybercriminel, permettant de le révéler.

L'OCLCTIC (Office Central de Lutte contre la Criminalité des TIC) collecte les données d'infractions numériques auprès des services de police et de gendarmerie. En 2003, 1280 atteintes aux systèmes de traitement automatisé de données (piratage) sont relevées (+9 %), tandis que 792 diffusions de programmes informatiques permettant de fabriquer de fausses cartes bancaires sont identifiés (+149 %).

En marge de ces données, deux rapports en lien avec la cybercriminalité sont attendus chaque année ; en effet, ces derniers permettent de donner le « pouls » de cette problématique. Il s'agit du rapport « *Computer Crime and Security Survey* » du CSI/FBI (*Computer Security Institute/Federal Bureau of Investigation (San Francisco Federal Bureau of Investigation's Computer Intrusion Squad*)) et du « Panorama Cybercrime » du CLUSIF (CLUb de la Sécurité de l'Information France). Ces deux rapports sont rendus publics chaque début d'année, en regard des activités de type « menaces IT » relevées l'année précédente. Notre approche consiste à présenter les deux derniers rapports des deux organismes cités *supra*, de les replacer dans le contexte, puis de rendre compte en particulier de leur mode de construction.

Les deux rapports se distinguent, en effet fortement sur ce dernier point. Le premier vise à apporter un rendu des coûts engendrés par le cybercrime, et ses principales tendances sur un échantillon très particulier d'entreprises aux Etats-Unis. Tandis que le second est une vue de la communication médiatique internationale attachée à ce phénomène, cela sur l'année écoulée. Ces approches différentes permettent cependant de dégager une vue intégrée de l'objet de notre étude, tant au niveau des préjudices engendrés qu'au niveau des tendances générales de cette problématique.

- Rapport CSI/FBI (2005 – exemple traité)

Le CSI[128] constitue une des principales organisations mondiales relatives au domaine de la sécurité de l'information. Depuis plus de 31 ans, le CSI aide des milliers

[128] Http://www.gocsi.com.

de professionnels de sécurité à protéger leurs systèmes d'information, en les sensibilisant *via* des conférences, des publications et divers avantages associés.

A ce titre, le CSI édite annuellement un bulletin de sensibilisation lié à la sécurité des systèmes d'information pour des utilisateurs variés : professionnels du monde de la sécurité et autres. Ce bulletin est rédigé en collaboration avec le FBI[129], service de contre-espionnage américain, notamment spécialisé sur la thématique du cybercrime aux Etats-Unis, *via* son bureau de San Francisco. Chaque année, ce rapport CSI/FBI dresse un tableau de la criminalité informatique aux Etats-Unis. Ce rapport est attendu par l'ensemble des experts de la matière, car il donne une tendance claire des attaques, de leur coût, tout en tenant compte des mesures de sécurité mises en œuvre. Ce rapport intégré CSI/FBI est concentré sur un petit panel d'industriels et d'abonnés aux services de l'organisme CSI.

Les personnes sondées déclarent, dans plus de 64 % des cas, avoir été financièrement victimes de fraudes NTIC. La moyenne des pertes se situe aux environs de 2 400 $ par déclaration. A titre de comparaison, selon les rapporteurs du FBI, dans le monde, les escroqueries téléphoniques ne dépassent pas un milliard de dollars par an. Les virus et « *spywares* » (logiciels de type espions) constituent encore le gros des menaces remarquées (83 et 80 % des réponses). Les attaques proviennent généralement des Etats-Unis même (26 % des origines situées), mais également, par exemple, de la Chine (23 % des cas).

Chaque année, depuis dix ans, le rapport CSI/FBI dresse donc le bilan d'une année de cybercriminalité sur un échantillon particulier d'entreprises aux Etats-Unis. Deux parties essentielles composent cette étude. La première s'intéresse principalement aux répondants à l'enquête, la seconde aux impacts des menaces sur les systèmes d'information étudiés. En 2005, selon le CSI/FBI, 70 % des agressions sont jugées sérieuses et 42 % ont occasionné des pertes financières. Plus de la moitié des menaces est véhiculée depuis Internet et cette tendance ne cesse d'augmenter. Le CSI/FBI rappelle que prémunir son système d'information contre les risques d'intrusion ou de malveillance

[129] Note : Le FBI fournit également chaque année un rapport annuel global reprenant les attaques de type cybercrime, mais sur l'ensemble du territoire américain. Ce rapport est plus pessimiste que celui du CSI/FBI, le crime informatique aurait, en effet, coûté 67 milliards de dollars aux Etats-Unis en 2005.

impose la mise en œuvre d'un ensemble de composants : architecture réseau, pare-feu, authentification des utilisateurs, chiffrement des données, antivirus, administration et protection des données, etc... Cet ensemble de contre-mesures est aussi pris en compte par le CSI/FBI au sein de son enquête, en termes d' « implémentation » effective. Les détails de l'étude 2005 sont présentés en annexe 2.

L'importance des systèmes d'information informatisés croît considérablement depuis une vingtaine d'année. Depuis 1995, Internet joue aussi un rôle crucial pour le développement économique des organismes modernes. La sécurité informatique a donc trouvé sa place en se focalisant au départ sur la question d'ordre technique comme le chiffrement, les contrôles d'accès ou encore les systèmes de détection d'intrusion.

Plus récemment, les aspects de sécurité de l'information, dépassant la seule préoccupation technique, sont également devenus importants, en complément aux aspects techniques. En lien avec cette extension nécessaire, Chris Keating, directeur du CSI, préconise que les entreprises haussent leur niveau de sensibilisation et de partage de connaissance dédié à la sécurité, vecteur d'une raison d'espérer des retours mesurables sur leurs investissements. En effet, plus la connaissance sur les causes et conséquences des failles de sécurité IT s'accroît, plus la sécurité sera améliorée. Le partage de la connaissance des attaques cybercriminelles est devenu primordial (sic).

- Panorama cybercrime - CLUSIF (2005 – exemple traité)

- Objectif du panorama :

Chaque année, le CLUSIF[130] (CLUb de la Sécurité de l'Information France) rend une copie très attendue : « *Le panorama cybercrime* ». Le but de ce panorama de la cybercriminalité est de mettre en avant quels ont été, au cours de l'année écoulée, les nouveaux risques attachés à cette thématique et les tendances vis-à-vis des risques déjà connus[131].

[130] http://www.clusif.asso.fr.

[131] Note : cependant, il est important de relativiser et de mettre en perspective ces incidents « relevés » et médiatisés, car tous ne sont pas forcément déclarés, donc connus (notamment en lien avec les explications données en amont, *via* le rapport CSI/FBI : « *afin de ne pas nuire à l'image de marque des compagnies qui ont été victimes d'attaques* »).

Les différents cas traités englobent la criminalité dite de haute technologie, mais également des atteintes dites plus « classiques ». Afin de réaliser cet objectif, la sélection des cas d'études du panorama cybercrime CLUSIF[132] a été réalisée par un groupe de travail pluridisciplinaire avec par exemple : des RSSI (Responsable de la Sécurité des Systèmes d'Information), des assureurs, des officiers de police et de gendarmerie en France.

Un entretien avec M. Pascal Lointier (Président du CLUSIF), en date du 24/02/06, a permis de déterminer les origines de ce panorama. Ce dernier nous l'a défini comme le bilan médiatique international de l'année du cybercrime : une compilation vers les sociétés, mais de plus en plus vers les citoyens, et ouvert à un large public.

La construction de ce rapport s'effectue de la manière suivante :

- novembre de chaque année M. Lointier organise un GT (Groupe de Travail) CLUSIF spécifique « cybercrime »,
- suite à cette réunion physique des divers protagonistes du GT, l'ensemble du travail s'effectue ensuite par mail,
- les membres du GT cybercrime rassemblent leurs données collectées annuellement du mois de janvier précédent à celui de l'année de présentation. L'activité par membre repose sur différents thèmes,
- le président du CLUSIF précise que le choix final des thèmes est un choix collégial, en fonction des données de l'ensemble des membres du GT, pour détermination finale fin janvier. Les membres du GT retiennent surtout des thèmes présentant des aspects innovants et importants (certains thèmes pouvant être mal interprétés (réutilisés) : pédophilie par exemple ou encore les blogs des enfants approchés par des « déviants », sont mis de côté),
- fin janvier, le panorama est présenté *via* une conférence annuelle par le président du CLUSIF,

[132] Note : les relais locaux du CLUSIF, en région, sont les CLUSIR (CLUb de la Sécurité de l'Information Régional).

- ensuite durant le premier semestre de l'année, le panorama est diffusé en province. (Metz (Université Paul Verlaine), par exemple, le 16 mai 2006, pour présentation du panorama cybercrime 2005).

Forme de présentations du rapport :

- un fichier de type powerpoint (.ppt) permettant de présenter le panorama (deux heures).
- un fichier de type powerpoint (.ppt) en téléchargement, avec des liens web permettant d'approfondir l'information transmise (*via* un processus de communication fort : avec référence et indicateur de tendance)
- supplément depuis le panorama cybercrime 2005 : des vidéos des présentations (AVI).

Le panorama cybercrime du CLUSIF est un indicateur très attendu désormais chaque année, notamment par les autorités françaises qui s'informent des tendances du cybercrime (car l'attente des problématiques particulières cybercrime est retenue par consensus par des experts sécurité, au cœur de ce panorama). Les détails de l'étude 2005 sont présentés en annexe 3.

Internet est un fabuleux outil de communication et de connaissances, mais dans certains cas, il est devenu aussi un nouveau vecteur de violences. Les nouveaux actes de cybercrime relevés par le panorama sont nombreux et même affolants. Ils sont l'œuvre majeure de l'être humain, réalité sociale parfois peu comprise. L'aspect humain des souffrances engendrées chez les victimes à causes de ces offenses ou violences doit aussi être considéré. Les atteintes psychologiques sont longues à guérir, sans compter que les conséquences sont parfois irréparables. Il existe un réel besoin d'information et de prévention contre certaines de ces atteintes. Cependant, il est impossible d'en prévenir encore certaines formes…

L'interconnexion des réseaux informatiques au niveau mondial a généralisé la problématique des menaces. Elles sont à caractères multiples et ne connaissent pas de frontières. Une analyse des référentiels de sécurité des systèmes d'information et de la communication permettra de tirer une synthèse des principales menaces et de mettre en

lumière leurs acteurs principaux (Cf. troisième partie – I – 2). Seront également développées les pratiques et méthodologies des acteurs particuliers des menaces intentionnelles au cœur de la société de l'information. Dans son rapport annuel, *MessageLabs* soutient que « la convergence des menaces via *emails*, la messagerie instantanée et le web augmentera les risques pesant sur les entreprises dans le courant de l'année 2006, même si 2005 aura été une des années les plus rude ». Ce rapport met également en évidence que la communauté des auteurs de virus et de *spam* ciblera de plus en plus la messagerie instantanée, celle-ci présentant une « porte dérobée » grandissante pour les entreprises : « *Tandis que l'adoption des messageries instantanées augmente et que les plateformes se standardisent, les messageries deviendront une cible plus attirante pour les spammeurs et d'éditeurs de chevaux de Troie. Les appareils mobiles deviendront également des cibles pour les malwares qui permettent de pénétrer incognito dans les entreprises, en tirant parti de l'ignorance des utilisateurs, mais aussi des faibles niveaux de sécurité de ces appareils* ».

L'année 2005 restera dans les annales comme l'année où les atteintes à la sécurité de la messagerie sont passées d'attaques en masse et au hasard, à des menaces hautement délibérées et ciblées, a confié Mark Sunner, *Chief Technology de MessageLabs*. « *Au cours de cette année, nous avons observé les menaces passer de la perturbation simple du service au vol de données, de propriété intellectuelle et d'identité* ». Cependant, le taux de *spam* par rapport à celui de 2004 se nivelle ; 2005 aura été une année d'attaques ciblées notamment dans le cadre de l'espionnage industriel (souvent par un cheval de Troie), particulièrement à l'encontre des administrations, des entreprises de loisirs et de tourisme ou de manufactures. Le *phishing* reste une menace importante, puisqu'un email sur 304 a été identifié comme une tentative d'hameçonnage. Enfin, les attaques redoublent d'agilités grâce aux *botnets* (les réseaux *zombies*) où les cybercriminels préfèrent maintenant contrôler un plus grand nombre de réseaux d'ordinateurs piratés plus petits et plus discrets. En ce sens, en 2005 la taille moyenne d'un réseau *zombie* a diminué.

En 2006, les attaques et des envois de courrier indésirables se sont diversifiés de plus en plus dans l'espace de la messagerie instantanée. Par ailleurs, les criminels se sont aussi attachés à trouver une voie d'accès aux appareils mobiles des utilisateurs.

Quant à *Symantec*, l'éditeur de solutions de sécurité soutient aussi que malgré l'ajout de fonctions visant à prévenir les attaques, les *hackers* continueront à prendre pour cible de nouvelles plates-formes. Ainsi, *Linux* ou *Mac*, *BlackBerry* ou *Palm*, ou même la *PlayStation* de *Sony*, etc…ne sont plus autant à l'abri qu'aujourd'hui. « *L'utilisation croissante de technologies secrètes, notamment sous la forme de rootkits, s'inscrit dans une évolution naturelle des méthodes d'attaques, a aussi estimé Symantec. Comme les hackers ne veulent pas se faire prendre, ils utilisent des méthodes offrant une couverture. On remarque la même tactique au niveau des virus codés, où un cryptage est utilisé pour tromper les logiciels antivirus. En plus, depuis un an et demi, Symantec observe une tendance inquiétante au niveau des codes malveillants. Les auteurs de codes malveillants utilisent des modules capables de se mettre à jour. Ces codes malveillants (vers, virus ou chevaux de Troie) ne possèdent à l'origine que des fonctions limitées. Une fois le code installé sur un ordinateur infecté, d'autres modules de code malveillants sont toutefois téléchargés avec d'autres fonctions. L'ordinateur infecté subit alors une attaque plus importante, ou une attaque DoS est lancée* ». Enfin, *Symantec* prévient des dangers de la VoIP. « *La Voice Over IP se développe rapidement comme une alternative très répandue au système de téléphone analogique traditionnel. On constate actuellement peu d'attaques ciblées sur les systèmes VoIP. Pourtant, Symantec estime qu'en raison de la large acceptation de cette nouvelle technologie de communication, ce n'est qu'une question de temps avant que ces systèmes ne soient davantage pris pour cibles* ». (LuxBox 3.6 Mars 2006).

- *Symantec Threat Report*[133]

La neuvième édition du rapport *Symantec* relatif aux menaces sur la sécurité informatique met l'accent sur une présence dominante des codes malicieux utilisés pour commettre des actes criminels liés à l'internet et aux TIC. Les techniques des délinquants ont évolué d'un type d'attaques larges multi-cibles vers des attaques à petite échelle, mais visant des cibles bien définies. Les menaces les plus répandues sont désormais liées aux « *botnets* » et aux codes malicieux modulaires. Les attaques ciblées deviennent la priorité

[133] *Symantec Internet Security Threat Report. Trends for July 05 – December 05*, Volume IX, *Published March 2006* (www.symantec.com/fr).

des cybercriminels. Alors que l'activité frauduleuse traditionnelle était motivée par une curiosité et une volonté de démontrer sa virtuosité technique, les actes criminels actuels ont pour objectif le gain financier. Le rapport propose une analyse complète des tendances en matière de sécurité Internet dans le monde entier. On constate une augmentation du nombre de menaces conçues pour faciliter la cybercriminalité. Le texte qui couvre la période du 1er juillet au 31 décembre 2005, indique les résultats dans quatre catégories : 1) les attaques 2) la vulnérabilité 3) les codes malicieux 4) les risques de sécurité supplémentaires.

Cette neuvième édition révèle une utilisation accrue des réseaux de *bots*, des codes malicieux modulaires et des attaques ciblant les applications Web ou les navigateurs Web. En s'appuyant sur ces conclusions et celles de ses précédents rapports, *Symantec* prévoit une utilisation accrue de menaces plus diversifiées et plus sophistiquées, ainsi qu'une augmentation du nombre de vols d'informations confidentielles, financières et personnelles motivées par l'appât du gain.

Alors que les attaques étaient auparavant conçues pour détruire les données, celles d'aujourd'hui visent davantage à voler discrètement les données, sans provoquer de dégâts notables qui avertiraient l'utilisateur. Dans son précédent rapport, *Symantec* signalait une progression des codes malicieux conçus à des fins financières ; cette tendance s'est maintenue tout au long du second semestre 2005. Les codes malicieux permettent désormais d'accéder majoritairement à des informations confidentielles (80 % des 50 principaux codes malicieux répertoriés, contre 74 % au cours du premier semestre 2005).

Les menaces liées à la cybercriminalité gagnent en puissance grâce à l'utilisation de « *crimeware* », des outils logiciels conçus dans le but de commettre des escroqueries en ligne ou de dérober des informations. Les attaquants ciblent désormais des dispositifs de sécurité classiques tels que les pare-feu et les routeurs. Ils concentrent leurs efforts sur des cibles régionales, des ordinateurs et des applications Web susceptibles de permettre à l'attaquant de dérober des informations confidentielles, personnelles ou financières qui peuvent ensuite être utilisées dans d'autres activités criminelles.

Les *bots*, programmes furtifs qui permettent aux attaquants de prendre le contrôle d'un ordinateur sans y être autorisés, contribuent également au développement de la

cybercriminalité. Si le nombre d'ordinateurs infectés par des bots a baissé de 11 % par rapport au précédent semestre (en moyenne 9 163 systèmes infectés répertoriés par jour au cours du deuxième semestre 2005), les réseaux de *bots* sont davantage utilisés pour des activités criminelles telles que les tentatives d'extorsion par déni de service. *Symantec* estime que ce chiffre ne représente qu'une partie de l'activité mondiale et que le nombre réel d'infections est probablement beaucoup plus élevé. *Symantec* a répertorié en moyenne 1 402 attaques par déni de service par jour, soit une augmentation de 51 % par rapport au précédent semestre. Les *bots* et réseaux de *bots* devraient en outre connaître une progression très importante dans la mesure où les attaquants commencent à exploiter un nombre croissant de vulnérabilités dans les applications de navigateurs Web.

Dans son précédent rapport, *Symantec* annonçait que les attaques dirigées contre les applications Web se multiplieraient. Ainsi, au cours du second semestre 2005, 69 % des vulnérabilités signalées à *Symantec* concernaient des technologies d'applications Web, soit 15 % de plus que pendant le précédent semestre. Les applications Web, dont l'interface utilisateur repose sur un navigateur, sont des cibles plus faciles pour les attaquants en raison de leur accessibilité *via* des protocoles courants tels que « *http* » par exemple.

Symantec a également observé l'augmentation du nombre de codes malicieux modulaires, qui sont dotés au départ d'une fonctionnalité limitée mais conçus pour s'enrichir automatiquement de nouvelles caractéristiques plus nuisibles. Les codes malicieux modulaires donnent souvent accès à des informations confidentielles exploitables pour le vol d'identité, l'utilisation frauduleuse de cartes de crédit ou d'autres activités financières criminelles. Au cours des six derniers mois de 2005, ils ont représenté 88 % des 50 principaux codes malicieux répertoriés par *Symantec*, soit 77 % de plus qu'au premier semestre.

Par ailleurs, la Chine a enregistré la plus forte augmentation du nombre d'ordinateurs infectés par des « *bots* » (robots) – avec une progression de 37 %, soit 24 points de plus que l'augmentation moyenne. Elle se place ainsi en deuxième position dans cette catégorie, juste derrière les Etats-Unis. Ce phénomène est probablement lié à la multiplication très rapide des connexions Internet haut débit. Le nombre d'attaques originaires de ce pays affiche également la plus forte croissance globale : progression de

153 % par rapport au précédent semestre, soit 72 points de plus que l'augmentation moyenne. Les *bots* sont vraisemblablement de plus en plus souvent la source de cette activité.

Au cours du deuxième semestre 2005, le *phishing*, dont le but est de tromper l'utilisateur et de le pousser à transmettre des informations confidentielles, a continué à se développer et vise désormais des cibles régionales plus petites. *Symantec* a répertorié en moyenne 7,92 millions de tentatives de *phishing* par jour, contre 5,70 millions de tentatives quotidiennes au cours du précédent semestre. *Symantec* prévoit à l'avenir une augmentation du nombre de messages de *phishing* et de codes malicieux diffusés par le biais des services de messagerie instantanée.

Symantec a répertorié 1 895 nouvelles vulnérabilités logicielles, un chiffre record depuis 1998. Parmi ces vulnérabilités, 97 % étaient considérées comme modérées à très graves, tandis que 79 % étaient considérées comme faciles à exploiter.

Symantec a calculé le temps nécessaire aux attaquants pour compromettre la sécurité de systèmes d'information nouvellement installés dans des déploiements standards en tant que serveurs web ou ordinateurs personnels. Concernant les serveurs, Windows 2000 Server sans *patch* est en moyenne compromis plus rapidement que les autres systèmes, tandis qu'il a été impossible de compromettre Windows 2003 Web Edition avec *patch* et RedHat Enterprise Linux 3 avec ou sans patch durant la période de test. S'agissant des ordinateurs personnels, Microsoft Windows XP Professional sans patch est en moyenne compromis plus rapidement que les autres systèmes, tandis que le même système doté de tous ses patches et le système SuSE Linux 9 Desktop n'ont pas été compromis.

Au cours du second semestre 2005, il s'est écoulé en moyenne 6,8 jours entre la publication d'une vulnérabilité et l'apparition du code d'exploitation correspondant, contre 6 jours pour le précédent semestre. Les fournisseurs diffusent les patches requis en moyenne 49 jours après la publication de la vulnérabilité. Les entreprises et le grand public sont donc exposés à des attaques potentielles pendant 42 jours, ce qui montre que les utilisateurs doivent appliquer les patches disponibles aussi vite que possible. Selon *Symantec*, la commercialisation des recherches de vulnérabilité devrait augmenter,

parallèlement au développement des forums de marché noir et l'accroissement des achats de vulnérabilités à des fins criminelles.

Du 1er juillet au 31 décembre 2005, *Symantec* a répertorié 10 992 nouvelles variantes de vers et virus Win32, ce qui ne représente qu'une faible augmentation par rapport aux 10 886 variantes répertoriées au cours du précédent semestre. Cette tendance s'inscrit dans le cadre d'un déclin notable des menaces de catégories 3 et 4 (modérées, et extrêmement graves) et d'une augmentation proportionnelle des menaces de catégories 1 et 2 (faibles et très faibles). Le nombre de nouvelles familles de virus Win32 a lui aussi baissé de 39 % (de 170 nouvelles familles au cours du premier semestre 2005, à 104 au cours du second semestre). Ces chiffres indiquent que les développeurs de codes malicieux préfèrent modifier le code source déjà en circulation plutôt que de créer de toutes pièces de nouvelles menaces.

- CERT CC (Computer Emergency & Response Team – Coordination Center)

Sur la période 1994-1995, 4752 incidents de sécurité ont été relevés par le CERT-CC (cf. partie I – I – 2)). Sur la période 1996-2001 : 92 714 incidents (explosion de 1998 à 1999 passant de 3734 incidents relevés à 9859). En 2002 : 82 094, puis en 2003 : 137 529.

Sur la période 1988-2003 : 319 992 incidents de sécurité ont été relevés en tout. A partir de 2004, le CERT a mis en production le rapport « *E-Crime Watch Survey Shows Significant Increase in Electronic Crimes* » (qui remplacera à terme les statistiques de type rapports d'incidents). L'ensemble statistique relevé par cet organisme permet d'offrir principalement la vision experte quantitative du phénomène, *via*, les qualifications et justifications provenant de diverses approches.

Cette première partie nous a permis de rendre compte de la réalité des faits quant au contexte global entourant notre objet de recherche. La cyberdélinquance est surtout rendue de manière quantitative et sous l'angle du préjudice généralement. L'état de la réalité du concept de la cyberdélinquance nous conduit donc à rendre compte de sa réalité sociale. Cependant, autant les méthodologies et possibilités sont « exposées » de manière

évidentes, autant les acteurs sociaux responsables des faits ne transparaissent pas clairement *via* ces faits. Cela semble engendrer un certain flou qui masque la réalité sociale de l'objet de recherche. Nous avons pu établir une réalité des faits de la cyberdélinquance, ce domaine pouvant être présenté comme un fait social déterminé, qui s'impose à nous, et qui laisse peu de place aux significations. L'état de la cyberdélinquance est, en effet, résolument tourné vers des données statistiques, quantitatives, avec un cadre législatif précis et international ne permettant pas vraiment de prendre la mesure sociale, ni la dimension humaine, qualitative des acteurs mêmes de ce concept. Cet état de fait nous permet de poser la cyberdélinquance comme un objet devenu alors socialement construit, tandis que les significations associées au pirate informatique, acteur principal du phénomène seraient encore sous forme de processus en construction.

3) Représentation sociale et cyberdélinquance

Selon Moscovici[134] (1961), les représentations sociales sont des « *univers d'opinions* » propres à une culture, une classe sociale ou un groupe et relatifs à des objets de l'environnement social. Depuis, les compléments apportés se sont surtout attachés à préciser les modes de construction des représentations et leur finalité. Une représentation sociale se présente comme un ensemble d'éléments cognitifs (opinions, informations, croyances) relatifs à un objet social. La première caractéristique de cet ensemble est d'être organisé, cela signifiant que les éléments qui constituent une représentation sociale entretiennent entre eux des relations. Plus exactement, cela signifie que les individus s'accordent à établir des relations entre ces divers éléments. La deuxième spécificité d'une représentation est d'être partagée par les individus d'un même groupe social, cependant ces consensus que l'on rencontre à propos des éléments d'une représentation donnée dépendent à la fois de l'homogénéité du groupe et de la position de l'individu par rapport à l'objet de représentation. La troisième caractéristique d'une représentation réside dans son mode de construction, elle est collectivement produite à l'occasion d'un processus global de communication. Ainsi, les échanges interindividuels et l'exposition

[134] *La psychanalyse, son image et son public* (Moscovici, 1961)

aux communications de masse permettent aux membres d'un groupe de mettre en commun les éléments qui vont constituer la représentation sociale. Enfin, la quatrième spécificité d'une représentation concerne sa finalité, elle est socialement utile, d'abord pour appréhender l'objet auquel elle se rapporte, mais elles interviennent aussi dans les interactions entre groupes. Roussiau et Bonardi[135] définissent ainsi : « *[…] une représentation sociale est une organisation d'opinions socialement construites, relativement à un objet donné, résultant d'un ensemble de communications sociales, permettant de maîtriser l'environnement et de se l'approprier en fonction d'éléments symboliques propres à son ou ses groupes d'appartenance* ». Comment les représentations sociales s'élaborent-elles ? « *Une représentation se définit par deux composantes : ses éléments constitutifs d'une part, et son organisation, c'est-à-dire les relations qu'entretiennent ces éléments d'autre part* » (J.L Rouquette et P. Rateau[136]). En d'autres termes, il s'agit du contenu et de la structure de la représentation. Les éléments qui la composent sont interdépendants et la cohérence de la représentation est basée sur cette dépendance. L'existence même d'une représentation sociale s'explique par la mise en œuvre de deux processus : l'objectivation (avec la constitution d'un noyau figuratif) et l'ancrage. S. Moscovici admet « *Objectiver, c'est résorber un excès de significations en les matérialisant* », et définit ainsi l'objectivation comportant trois phases (construction sélective, schématisation structurante, naturalisation), qui met en forme les notions abstraites constituant l'activité mentale et matérialisant les idées en leur fournissant un « contour » (image ou figure). Le second processus est l'ancrage. Il assure l'enracinement social de la représentation, avec les valeurs cognitives particulières qu'elle revêt dans le groupe de référence. L'ancrage opère en amont de la représentation sociale en renvoyant à des univers de sens et de savoir. En aval, l'ancrage confère une valeur fonctionnelle au contenu représentationnel, le rendant ainsi disponible pour son usage dans le groupe. Le processus d'ancrage comporte plusieurs aspects :

- Le sens : l'objet représenté est investi d'une signification par le groupe concerné par la représentation. A travers le sens, c'est son identité sociale et culturelle qui s'exprime.

[135] *Les représentations sociales* (Bonardi, Roussiau, 1999).
[136] *Introduction à l'étude des représentations sociales* (Rouquette, Rateau, 1998).

- L'utilité : les éléments de la représentation ne font pas qu'exprimer des rapports sociaux mais contribuent à les constituer. Le langage commun qui se crée entre les individus et les groupes à partir d'une représentation sociale partagée, leur permet de communiquer entre eux. Le système de référence ainsi élaboré exerce à son tour une influence sur les phénomènes sociaux.
- L'enracinement dans le système de pensée préexistant : pour intégrer de nouvelles données, les individus ou les membres d'un groupe les classent et les rangent dans des cadres de pensée socialement établis. Des attentes et des contraintes sont en même temps associées aux éléments de la représentation, en termes de comportements prescrits.

La notion de noyau figuratif, élaboré par Moscovici, a été reprise et développée par Abric sous le terme de noyau central (ou noyau structurant). Selon sa théorie, une représentation est un ensemble organisé autour d'un noyau central, composé d'éléments qui donnent sa signification à cette représentation. Ce noyau structurant est l'élément fondamental de la représentation ; son repérage permet l'étude comparative des représentations sociales. Le noyau structurant a deux fonctions principales, une fonction génératrice (le noyau central est à l'origine des différents éléments de la représentation ; il leur donne sens et valeur et c'est ce par lui que peuvent se transformer ces éléments), et une fonction organisatrice (selon Abric « *il détermine la nature des liens qui unissent entre eux les éléments de la représentation. Il est en ce sens l'élément unificateur et stabilisateur de la représentation* »). De fait, ce n'est que lorsque le noyau central est modifié que la représentation se transforme. Ce qui peut être généralement conséquent dans le temps. Le noyau central est constitué de la nature de l'objet représenté, de la relation de cet objet avec le sujet ou le groupe, et du système de valeurs et de normes (le contexte idéologique).

Au cœur de cette explication théorique, et suite à notre première partie, nous pouvons établir que l'objet cyberdélinquance fait montre d'une objectivation ainsi que d'un ancrage concret. Nous considèrerons, en effet, que des différents éléments d'organisation structurelle du champ de la sécurité de l'information, des moyens concrets de lutte contre la cyberdélinquance, décrits et établis de manière consensuelle au niveau

international (spécifiquement vu en Europe, au Grand-Duché de Luxembourg ou encore en France), mais aussi des nombreuses statistiques éloquentes et évoluant dans le même sens, découle alors la notion de représentation sociale de la cyberdélinquance. En terme de noyau « dur », le noyau central de la cyberdélinquance est spécifiquement son caractère illégal et fortement menaçant pour le monde numérique, les nombreuses définitions, lois et engagements internationaux décrits *supra* permettent de l'établir.

Même si le noyau central est le fondement de la représentation, les éléments périphériques tiennent une place importante dans la représentation. C. Flament leur assigne trois fonctions essentielles (prescriptive, de personnalisation, de protection du noyau central). Selon Abric « *Ils comprennent des informations retenues, sélectionnées et interprétées, des jugements formulés à propos de l'objet et de son environnement, des stéréotypes et des croyances …Ils constituent … l'interface entre le noyau central et la situation concrète dans laquelle s'élabore ou fonctionne la représentation* ». A ce titre même, il semble véritablement que les significations du pirate informatique, acteur principal de la cyberdélinquance, soient un produit satellite de la représentation sociale de la cyberdélinquance, en fait un « élément périphérique » de cette dernière.

La représentation sociale de la cyberdélinquance semble établie au regard des divers instruments et réactions étudiés en première partie de notre propos. Cependant, quant à notre objet de recherche, et dans cette perspective étudiée et retenue *supra*, de quelle manière son processus de construction sociale se forme-t-il, en périphérie du noyau central de la cyberdélinquance ?

Nous tiendrons compte de la fonction de personnalisation des représentations et des conduites qui lui sont rattachées : ils autorisent une certaine souplesse dans les représentations, qui tient compte de l'appropriation individuelle et du contexte dans lequel elles s'élaborent. Cette fonction rejoint la fonction de régulation définie par Abric, selon laquelle les éléments périphériques permettent l'adaptation de la représentation aux évolutions du contexte. Notre approche pour atteindre ce processus de construction nous conduit à poser notre travail de manière opposée à la filiation durkeimienne qui tend à distinguer une société sans sujet : « *Est fait social toute manière de faire, fixée ou non, susceptible d'exercer sur l'individu une contrainte extérieure ; ou bien encore, qui est générale dans l'étendue d'une société donnée tout en ayant une existence propre,*

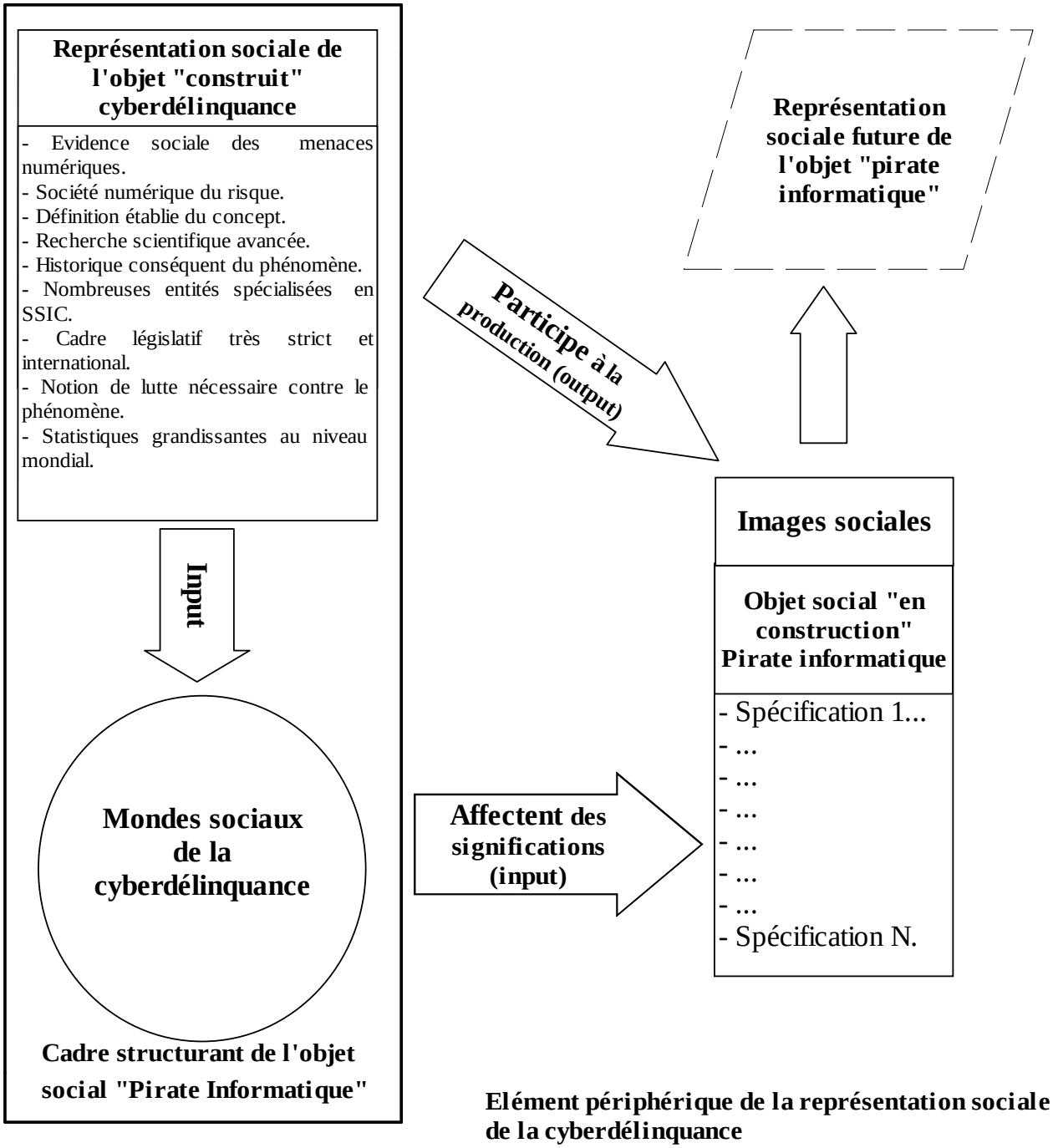
indépendante de ses manifestations individuelles »[137]. Afin de penser notre objet de recherche de manière opposée à ce courant, nous prendrons alors en compte, dans la lignée de Simmel ou de Weber, la réflexivité et la compétence des acteurs. Nous nous sommes ainsi interrogés sur le statut d'une connaissance sociologique qui n'est pas éloignée de la connaissance familière mise en œuvre dans la vie courante : « *La sociologie compréhensive s'efforce de dégager les significations vécues par les acteurs et de mettre en évidence les logiques qui sous-tendent leurs actions* »[138]. A l'instar de Simmel, nous posons l'individu, objet de notre recherche, comme acteur du sens de son existence et de ses liens avec les autres : « *C'est à l'homme seul qu'il est donné, face à la nature, de lier et de délier les choses, selon ce mode spécial que l'on suppose toujours l'autre (…) Dans un sens immédiat aussi bien que symbolique, corporel aussi bien que spirituel, nous sommes à chaque instant ceux qui séparent le relié ou qui relient le séparé* »[139].

Il est primordial de considérer l'objet social cyberdélinquance sous forme d'état établi. Cet objet social construit va apparaître comme structurant pour la formalisation des images sociales de notre objet de recherche. En effet, l'absence de mise en relation directe du citoyen avec le pirate informatique va engendrer la production d'une image sociale relative à ce dernier (une signification particulière), avec association de valeurs particulières, cela en interdépendance avec l'objet social représenté de la cyberdélinquance. Nous l'avons vu *supra*, les images sociales sont attachées à un objet et correspondent pour partie au jugement de ce dernier. L'objet social « pirate informatique » n'existe pas, en tant que tel pour l'instant, mais plutôt des images de ce dernier. « *Mais les images sociales ne sont pas des représentations, elles en sont le produits (Moliner, 1996)* ». « *Les images sociales orientent non seulement la cognition sociale, mais également les conduites et positions à l'égard de l'objet qui devient, de la sorte, accepté ou refusé, préféré ou dénigré, élu ou banni (Moscovici, 1961, 1976)* »[140]. L'objet de recherche difficilement perceptible serait donc en construction *via* des groupes particuliers qui vont lui affecter des valeurs spécifiques. L'objet de recherche étudié

[137] *Les règles élémentaires de la méthode sociologique* (Durkeim, 1977).
[138] *L'interactionnisme symbolique* (Le Breton, 2004).
[139] Simmel, 1988, 159-160.
[140] *Les représentations sociales* (Mannoni, 2001).

semble donc dépendre de la représentation sociale de la cyberdélinquance, et d'un contexte social particulier qui donne un cadre structurant à sa construction, que nous avons nommés les mondes sociaux de la cyberdélinquance. L'objet de recherche, en construction, dépend donc de la représentation sociale de la cyberdélinquance qui est à la base de la production des images sociales de ce dernier, et dépend également du contexte social associé alimentant la production même de ces images sociales. La construction sociale de notre objet de recherche est donc en interdépendance avec ces deux éléments structurants, nous l'analyserons ainsi dans la suite de notre recherche (voir modélisation graphique en figure 1 – *infra*).

- Figure 1. Modélisation graphique des représentations sociales de la cyberdélinquance



Pour comprendre les éléments structurants de la construction sociale du pirate informatique, tel que définie *via* notre modélisation graphique, notre deuxième partie traitera, dans un premier temps, de l'approche communicationnelle possible du milieu social de la cyberdélinquance, en tentant d'identifier quel est le reflet dominant de l'image du pirate informatique.

Nous déclinerons ainsi, les contextes d'émergence probables des images sociales du pirate informatique, nous montrerons le rapport des médias à la construction de l'image sociale du pirate informatique, pour enfin mettre en évidence d'autres mondes « bâtisseurs » d'images du pirate informatique, cet ensemble constituant les mondes de la cyberdélinquance (voir figure 1 *supra*), comme contexte social de production.

Ces images sociales seront considérées comme des produits (issus de la représentation sociale de la cyberdélinquance et du contexte social associé). A ce titre, il nous importe de retenir la définition d'un produit comme le résultat d'un processus, et d'interroger, dans ce cadre, le processus de construction social du pirate informatique.

DEUXIÈME PARTIE

Titre II - Approche communicationnelle du contexte social de la cyberdélinquance : reflet médiatique dominant du pirate informatique

L'état quantitatif est un des aspects retenu pour expliquer notre question de recherche et traduire un des attributs de notre objet. Cependant, cette approche, voisine de la statistique, ne peut suffire pour comprendre notre problématique. En effet, le but de notre recherche est de rendre moins complexe la multiplicité d'images transmises et/ou construites du pirate informatique, en se plaçant du point de vue de l'acteur à différents niveaux. Nous déterminerons, pour ce faire, que la délivrance des attributs et des fonctions de l'objet « pirate informatique » provient d'un réseau social entourant ce dernier, que nous avons nommés les mondes sociaux de la cyberdélinquance.

Face à la virtualité de l'objet de recherche, tel que la maxime « *Nobody knows you're a dog on Internet* » (« *Personne ne sait que tu es un chien sur Internet*), finalement « *Personne ne sait que tu es un pirate sur Internet* » pourrait également être reprise sur le même ton. Ne pouvons-nous pas définir ainsi que nous assistons plutôt à un « conformisme de fortune » ? Ce dernier étant construit *via* un lissage des significations attribuées à l'objet, que la majorité ne rencontrera jamais, mais se représente tout de même, *via* l'adoption des représentations du grand groupe, quelquefois, par l'individu, en dépit de ses propres perceptions : «*le conformisme se présente avant tout comme détermination par la majorité non du jugement de l'objet mais de l'objet du jugement »* (S. Asch, 1940). En effet, peut-on parler d'une ou de plusieurs images sociales du pirate informatique ? Pourquoi et comment peut-il exister autant d'angles de vues relatifs au pirate informatique ? Comment se formalisent ces images multiples ? De ces divers interrogations à l'ingénierie de cette image se décline donc la nécessité d'une approche communicationnelle afférente à l'objet de recherche, à savoir la prise en compte du point de vue de l'acteur social, en préconisant l'entrée au cœur de chaque monde social entourant l'objet de recherche, sous l'angle de la communication.

L'état quantitatif décliné en première partie reflète finalement une vision qui ne peut être occultée, l'objet cyberdélinquance est proposé comme construit ou plutôt majoritairement présenté comme étant ainsi, cependant, une vue plus globale semble nécessaire. Le but de nos travaux est de rendre compte et de respecter la construction sociale de l'objet, ses processus d'ingénierie conduisant à celle-ci. Nous nous intéresserons alors aux représentations collectives, en tenant compte aussi des principes

de réalité que s'est efforcé de fonder Durkheim : « *Puisque l'observation révèle l'existence d'un ordre de phénomènes appelés représentations, qui se distinguent par des caractères particuliers des autres phénomènes de la nature, il est contraire à toute méthode de les traiter comme s'ils n'étaient pas* »[141].

Autant l'existence des faits de cyberdélinquance paraît claire, autant l'existence des acteurs responsables paraît floue. A ce titre, il semble qu'à la réalité du phénomène, par exemple *via* la mise en évidence d'un préjudice économique, se juxtapose la virtualité des acteurs responsables, restant souvent inconnus ou mal définis. Il semble important de séparer la réalité des faits de la naturelle représentation des acteurs, puisque virtuels, mais effectivement imaginés, et de manière fictive. Indépendamment de la réalité technique, l'image sociale du pirate informatique n'apparaît donc pas forcément de façon strictement singulière. En effet, il semble que l'objet représenté est flottant et varie en fonction des mondes qui le représentent. Les représentations sociales du pirate informatiques semblent être socialement élaborées, plutôt que constitutives de l'objet social. Les attributs des significations lui sont affectés, *via* différentes sources. Ainsi, il convient de vérifier, dans ce « nouveau » cadre social, si l'objet est construit ou en construction et de quelle sorte, au sein de l'espace public, des médias, voire d'autres mondes spécifiques.

I – Contexte et images sociales de la cyberdélinquance

Via notre première partie nous avons montré les prémices d'une évolution sociale certaine du pirate informatique (voir première partie – II – 3) - Historique)) : une « grandeur » à l'origine, puis une rapide décadence de son image, en regard notamment de la réalité statistico-démonstrative et illégale de la cyberdélinquance. Cela a permis de montrer les éléments à l'origine de la production de la représentation sociale de la cyberdélinquance. En corrélation, de manière globalisée, le pirate informatique, acteur de ce concept, est finalement passé « *du chevalier de l'innovation au cybercriminel* ». Le

[141] *Revue de métaphysique et de morale* (Durkheim, 1898).

rôle des médias aurait joué une part non négligeable pour cet aspect. A ce titre, l'approche communicationnelle mérite toute l'attention pour comprendre l'ingénierie de l'image, posée pour notre objet de recherche. Avant d'interroger le rapport des médias à la construction de l'image sociale du pirate informatique, nous déclinerons le contexte(s) et les produit(s), en termes d'images, de ce dernier. Pour ce faire, nous détaillerons le contexte social de la cyberdélinquance, comme moteur productif de(s) image(s) du pirate informatique, puis nous rendons compte d'un sondage public visant à relever de la réalité sociale représentée de la cyberdélinquance et de l'image sociale dominante du pirate informatique, pour enfin déterminer si cette dernière est principalement issue des médias.

1) Le contexte social du pirate informatique

Elément de caractérisation sociale du cyberdélinquant

Le pirate informatique vit dans un contexte social particulier, celui que nous avons décrit en première partie : la cyberdélinquance. Dans l'usage courant, délinquance et criminalité sont des termes qui, entendus dans leur généralité, recouvrent approximativement une même réalité : l'ensemble des agissements considérés comme antisociaux, tombant sous le coup de la loi pénale, qui surviennent dans un pays ou dans un groupe déterminé, au cours d'une période donnée, envisagés selon leur fréquence et leur nature, rapportés enfin à la personnalité de leurs auteurs. Les sciences sociales considèrent ainsi le comportement criminel comme la manifestation d'un conflit de cultures et comme une déviation par rapport aux normes culturelles en vigueur dans la société.

Le délinquant est une personne qui n'a pu établir, ou rétablir, l'équilibre entre les impulsions de son « moi » et les normes de la culture figurant au Code pénal, ou encore les us et coutumes. D. Szabo, professeur titulaire à l'Ecole de criminologie de l'Université de Montréal admet qu'une distinction s'impose enfin entre la conduite déviante et la conduite proprement criminelle. La première est liée à la structure de la personnalité et à celle du milieu socioculturel ; la seconde est l'œuvre de forces historiques plus ou moins fortuites, codifiées par le droit. Raisonner en termes de « conduites déviantes » et parler de conduites criminelles serait une source de regrettables

confusions. Nous souhaitions établir cette caractéristique, sachant que nous avons défini dès le départ que nous ne ferons pas, de distinction volontaire, entre les termes cyberdélinquance et cybercriminalité. Cependant, il se dégage certainement une différence entre un cyberdélinquant et un cybercriminel, en tenant compte de la distinction étayée *supra*, que nous ne traiterons pas dans notre propos, mais qui touche surtout à la gravité des actes.

Cela nous rapproche d'une des préoccupations constantes de Durkheim en regard de la pathologie sociale, le problème du « normal » et de l' « anormal ». « *Il n'y a pas de sociétés connues, déclare-t-il, où sous des formes différentes, ne s'observe une criminalité plus ou moins développée. Il n'est pas de peuple dont la morale ne soit pas quotidiennement violée. Nous devons dire que le crime est nécessaire, qu'il ne peut pas ne pas être, que les conditions fondamentales de l'organisation sociale, telles qu'elles sont, l'impliquent logiquement* ». Il conclut : « *Par conséquent, le crime est normal* »[142]. Le doyen Carbonnier affirme aussi que « *L'évolution des mœurs et des techniques donne matière à de nouvelles formes de délinquances* »[143]. Transposé à la société de l'Information, il semblerait aussi normal d'y déceler des formes de crimes.

Mais comment appréhender cette forme de délinquance ? Le terme de délinquance vient du latin *delinquere*, « *commettre une faute* » ; à ce titre, il relève d'une action particulière illicite. La criminologie n'a eu de cesse de brosser des portraits psychologiques, voire raciaux des délinquants. C. Lumbroso, « inventeur » de l'anthropologie criminelle a mis en évidence la méthode des « types criminels » (les « criminels nés ») qui s'est avérée peu pertinente. En effet, pourrait-on asseoir tel raisonnement vis-à-vis de notre objet de recherche. Une recherche de ce type pourrait être entreprise, bien que P. Breton indique : « *Aucune des catégories habituelles de la criminologie classique ne s'applique pour comprendre le comportement des « pirates » qui régulièrement attaquent des sites sur Internet* »[144]. Depuis la fin des années « soixante », trois paradigmes, considérés tantôt comme concurrents tantôt comme complémentaires, dominent ainsi la réflexion dans la sociologie de la délinquance.

[142] *Le suicide* (Durkheim, 1897).
[143] S*ociologie Juridique* (Carbonnier, 1978).
[144] *Le culte de l'Internet, une menace pour le lien social ?* (Breton, 2000).

Le premier privilégie l'étiologie du comportement criminel afin de mieux cerner les conditions du passage à l'acte. Il se nourrit d'une tradition qu'illustrent les travaux de Glueck (1950), aux Etats-Unis, de H. Goppinger (1986) en Allemagne, de B. di Tullio (1967) en Italie et de J. Pinatel (1975) en France. Le deuxième prend comme point de départ l'acte criminel : il fait du délit l'élément central entre le délinquant et la victime d'une part, et entre le délinquant et les forces de l'ordre d'autre part. Ce paradigme s'enracine dans la tradition écologiste de l'école de Chicago (Shaw et McKay, 1942) et de l'école de l'écologie sociale (Hawley, 1950). Le troisième se propose d'étudier, puis d'expliquer la criminalité comme phénomène collectif, ses déterminants et ses mouvements. Le problème majeur concerne le contrôle social considéré comme un mécanisme de la réaction sociale au phénomène criminel.

Aujourd'hui, criminologues et sociologues s'entendent plutôt pour définir un délinquant avant tout par ses actes, rejoignant le deuxième paradigme. C'est la perspective « actionniste » (tenant compte du « choix » personnel des acteurs), opposée à la vue déterministe (la société pour responsable). Nous avons choisi de tenir compte de cette perspective pour éclairer notre objet de recherche. Selon la définition actionniste, le délinquant est celui qui enfreint la loi, le cyberdélinquant n'échappant finalement pas à cette règle. Cependant, les actes de cyberdélinquance ne sont pas les plus fréquents, sur l'ensemble des actes de délinquance ; ils échappent à la définition des actes délinquants les plus caractéristiques : le vol, le trafic de drogue ou encore l'agression de personnes. Souvent, le contexte social du cyberdélinquant est confondu avec celui du délinquant classique. Cependant, nous l'avons défini dès le départ, il existe des actes de cyberdélinquance propres à l'attaque même des ordinateurs et réseaux, les prenant pour cible et ayant déterminé un nouveau cadre de loi du piratage informatique. Pour exemple, dans ce cadre, le Boston Consulting Group (BCC), a édité le 31 janvier 2002 « *The Boston Consulting Group Hacker Survey* ». Le BCC présente des statistiques appliquées aux motivations des *hackers*, les champs « *Intellectually stimulating* » (stimulation intellectuelle) et « *Improves skill* » (améliorations de compétences) représente 43.2 % : « *La motivations des hackers : les croyants (33 %), font cela parce qu'ils souhaitent que le code source soit ouvert, les professionnels (21 %), font cela par défit intellectuel, par amélioration des connaissances (21 %), font cela pour l'amélioration de leurs*

compétences[145] ». Le BCC est surtout un organisme qui établit ses enquêtes sur la base de la Communauté *Open Source*, point de ralliement spirituel de nombreux *hackers*.

Bien entendu, il est clair que le mouvement « *hacker* » ne constitue pas la majorité des attaques de cybercriminalité, les motivations décrites par le BCC n'étant pas les principales à l'origine de l'ensemble des attaques relevées. Les distinctions entre *crackers* et *hackers* sont fréquentes et revendiquées, le partage entre cybercrime et cyberdélinquance aussi, la distinction entre les actes à « classifier » comme étant l'œuvre ou non d'un pirate informatique également. Il appert que ce contexte social du pirate informatique semble large et ouvre finalement à la production de plusieurs images sociales, nous nous proposons alors de l'éclaircir.

Qu'est-ce qu'une image sociale ?

« *Les êtres et les objets qui nous entourent éveillent dans notre esprit un « écho » que l'on nomme, sans trop réfléchir à la confusion sous-jacente ou aux amalgames latents, une idée, un concept, une image, une figure, un schème, une définition, etc. Toutes ces notions renvoyant de près ou de loin aux représentations […]* »[146]. Le cerveau humain est en effet organisé pour traiter des informations absentes, qui ne correspondent à aucune perception, grâce à sa fonction anticipatoire. L'homme par sa mémoire peut revivre, à travers le récit, des événements très anciens. C'est la grande différence entre les humains et le monde animal, l'homme pouvant se permettre de jouer et rejouer ses aventures cognitives ou effectives en dehors des objets matériels que ces récits évoquent. Cela nous intéresse au plus haut point, puisqu'en effet, hors du contexte social de la cyberdélinquance, un individu peut s'approprier n'importe quelle image du pirate informatique, s'il le souhaite. Ces représentations mentales chez l'homme sont des images chargées émotionnellement qu'il se « re-présente » ou que l'on « re-présente » à d'autres intentionnellement dans la perspective d'une communication d'informations intellectuelles ou affectives, qui ont valeur dans l'échange social interhumain.

---

[145] *« Motivations segment hackers : believers (33 %), do it because they believe source code should be open, Professionals (21%), do it for work need and professional status, Fun seekers (25 %) do it for non-work intellectual simulation, Skill Enhancer (21 %), do it for skill improvement* ».
The Boston Consulting Group Hacker Survey (BCC, 2002).

[146] *Les représentations sociales* (Mannoni, 2001).

Les représentations mentales, telles que les idées reçues, les préjugés, les stéréotypes sont ainsi des éléments constitutifs de la pensée commune qui participent puissamment au système de représentations avec lequel ils entretiennent des rapports certains non seulement de coexistence mais également de consubstantialité. Selon P. Mannoni, il existe un jeu de connexion et d'échange entre ces divers éléments psychiques que sont les préjugés, les stéréotypes et les représentations sociales. Les mêmes matériaux interviennent, en effet, dans leur constitution, il s'agit essentiellement des caractères porteurs du sens d'où dérive la valeur finale de l' « image mentale ».

Les représentations sociales se situent en aval par rapport à certaines d'entre elles qui jouent le rôle d'organisateurs de schèmes cognitifs, comme les représentations mentales ou psychiques et les fantasmes. En revanche, elles se présentent en amont des clichés, stéréotypes, superstitions, croyances, contes, mythes, pour lesquels elles jouent un rôle constituant. Les images sociales sont finalement le résultat d'un processus de constructions mentales diverses de la représentation de l'objet. Ainsi, nous avons souhaité investiguer les différents mondes participant au contexte social du pirate informatique, et relever les éléments de construction propre s'y rapportant. Le concept de monde social est un réseau d'acteurs en interaction pour la construction d'un objet partagé. Chaque monde participe à la construction de l'image sociale du pirate informatique selon des codes, culture, besoins, histoire qui lui sont propres. Parler vrai de l'objet semble ainsi possible, en entrant dans les mondes, et en se plaçant du point de vue de l'acteur de chaque monde[147].

Suivant cette même idée, notre travail de recherche vise l'étude des mondes de la cyberdélinquance, dont trois majeurs : le monde médiatique, le monde des pirates informatiques et le monde des experts SSIC. Trois mondes qui mobilisent de nombreux acteurs sociaux, coopérant ou non, utilisant ou non des procédures conventionnelles au sein des réseaux que l'on peut dénommer : « Mondes de la cyberdélinquance » (cf. Introduction). Ces mondes engendreraient des significations spécifiques formalisant, *sui generis*, une image singulière du pirate informatique. Chaque monde forgeant alors une

[147] Note : Howard S. Becker, décrit dans *les Mondes de l'art*, comment dans tous les arts, la production, la diffusion, la consommation, l'homologation esthétique et l'évaluation des œuvres mobilisent des acteurs sociaux appelés à coopérer selon un certain nombre de procédures conventionnelles au sein de réseaux dénommés par ce dernier : « Mondes de l'art ».

catégorisation particulière de ces acteurs sociaux. Biella Coleman (anthropologue - *Rutgers University*) indique que les évènements de type « *underground* » permettent de rencontrer en réalité des personnages actifs « *on-line* » et rarement atteignables. « *Virtuality needs sociality* » (la virtualité a besoin de sociabilité). L'absence de rencontre et d'implication au cœur du monde « *underground* » peut engendrer la facilité de la pensée vulgaire, entraînant la formalisation d'une image du cybercrime et de ses acteurs principaux en décalage avec la réalité des faits, et des significations du monde concerné.

Il est urgent, pour pallier à cet état de fait, de privilégier la promotion d'une culture de l'insécurité objective, tenant compte d'une matrice cognitive interculturelle, à savoir la prise en compte des mondes sociaux déclinés dans notre étude. Ce qu'on appelle le cybercrime ne peut être, par conséquent, simplement réduit à une perception subjective objectivée, cette notion posant le problème de la connaissance. La construction sociale du cybercrime est aussi le fait de la construction d'une image par un individu dans un champ donnée (un monde social donné). La connaissance du cybercrime découlera alors de la prise en compte de la construction de plusieurs images, *via* l'ensemble des mondes sociaux de la cyberdélinquance concernés.

Chicago pour modèle de réflexion ?

La première école de Chicago permet de parfaire notre recherche. En 1892, le département de la sociologie de Chicago était le premier de son espèce aux Etats-Unis. Son fondateur *A. Small* le dirigera jusqu'en 1924. Il voit la sociologie comme une discipline spécifique centrée sur l'étude des formes concrètes de la vie sociale. *A. Small* et son équipe ont la vision d'une société dominée par le darwinisme social ou le libéralisme de *Spencer*, compensée par la conviction de pouvoir contribuer activement à l'amélioration du bien-être social (réformisme). Pour eux, le savoir doit être utile à l'action sociale. Leur recherche évolue aussi vers ce qui se nomme l'*interactionnisme symbolique*, soutenant que la sociologie s'intéresse à la conception que l'individu se fait du monde social. Cette notion est due à *H. Blumer* (années 30). Elle part de l'idée que les individus ne subissent pas les faits sociaux, mais qu'ils les produisent par leur interaction. Ils privilégient l'observation directe (elle consiste pour un enquêteur à s'impliquer dans le groupe qu'il étudie pour comprendre sa vie de « l'intérieur » et le point de vue de

l'acteur. 1930 marque un tournant dans l'histoire de l'école de Chicago avec de nouveaux sociologues comme *H. Blumer* et *Hughes*. Alors que l'école avait jusque là privilégié une approche souvent holiste, elle évolue désormais vers une vision plus individualiste. Il se dégage en fait deux courants principaux : l'un se situe dans le prolongement de la première période de l'école c'est-à-dire « l'étiquetage des populations » tandis que l'autre se tourne vers ce que l'on nommera l' « *ethnométhodologie* ». Plusieurs thèmes majeurs sont étudiés : le paysan polonais de *Thomas* et *Znaniecki* inaugure une longue série d'études sur le processus de migration et d'assimilation. *Thomas* élabore une monographie décrivant la migration Pologne-Etats-Unis comme une suite de désorganisations et réorganisations successives. Il distingue la « désorganisation sociale » (déclin collectif des valeurs) de la « démoralisation », qui caractérise la déviance individuelle. Un des ouvrages les plus importants de l'école de Chicago « *the citie* », est signé en 1925 par *Burgers, Mc Kenzie* et *Park*. Chicago, qualifiée de « laboratoire social » y est étudiée sous l'angle de la répartition dans l'espace des communautés et des classes sociales. Les vagues successives de migrants transforment la ville, en même temps qu'ils s'y adaptent en aménageant leur espace propre. L'instabilité de l'équilibre urbain est l'illustration de la « désorganisation » que vivent certains groupes. La ville est un mode de vie « éclaté » : impersonnalité et superficialité des contacts. La montée de l'individualisme mène à une différenciation sociale accrue, et à la porte des contacts primaires. En 1923, *Anderson* publie une enquête sur les « *hoboes* » (sans-abri). Il montre comment ces gens forment une micro-société avec ses spécificités, ses lois non écrites, et ses lieux : il existe une « université *hobo* » où les sans-abri peuvent exprimer leur idées sociales. Le thème de la déviance continue d'être étudié à Chicago : 1928 : *Carvan* étudie le suicide, 1939 : *Faris* et *Dunham* enquêtent sur les maladies mentales dans les quartiers pauvres, 1963 : *Becker* formalise la théorie de « l'étiquetage » dans Outsiders.

La criminalité est à Chicago à l'image de l'histoire de la ville : irlandaise au début du 20è siècle, elle devient polonaise et italienne à l'époque de la prohibition. Les sociologues, répondant à une forte demande sociale, ne cesseront de s'intéresser à la délinquance, organisée ou non. Après la guerre des gangs de 1924, *F. Thrasher* réalise une étude sur les « gangs de quartier », où il décrit les bandes de jeunes comme une forme de réorganisation sociale. En 1929, *Landesco* produit une étude sur le grand

banditisme. En 1930 et 1931, *Shaw* analyse à partir de leur biographie la carrière de deux jeunes délinquants : *Stanley* « le détrousseur d'ivrognes », et *Sydney* « le violeur ». Il introduit ainsi les histoires de vie dans le champ de la criminologie et montre que certaines constantes apparaissent : quartiers pauvres, famille brisée, scolarité inexistante.

En regard de ces évolutions de caractérisation, le pirate informatique, acteur implacablement lié à la cyberdélinquance demeure pour nous une véritable question de communication, à l'instar de la criminalité de Chicago. Qui est-il ? Comment est-il représenté, perçu ? Le terme intégré « cyberdélinquance » est aussi composé de « cyber » : terme usuel de la virtualité et associé à l'idée des réseaux IT, notamment Internet. Le piratage informatique peut, en un sens, être considéré comme un acte de communication particulier. Mais comment se représente ce personnage social intimement lié à des actions illicites ? Une première clé, nous l'avons vu, demeure dans une approche menée à la lumière des définitions relatives à l'acteur. En effet, cette détermination sémantique offre un premier axe de réponse. Puis la mesure des représentations sociales permet également de rendre compte de l'image sociale dominante du pirate informatique. Ce phénomène est également largement relayé par les différents médias. Cette approche des phénomènes criminels du réseau de réseaux est cependant très peu étudiée par les sciences de l'information et de la communication. Des éclairages ont surtout été apportés *via* des études spécifiques consacrées à l'objet Internet. Cependant, la réflexion en sciences de l'information et de la communication est moins soutenue quant aux relations entre criminalité et Internet. Nous rendrons compte pour corroborer ces résultats de notre première partie, de la perception publique de l'objet de recherche.

2) Sondage public de l'image sociale dominante du pirate informatique

Afin de rencontrer la perception sociale du cyberdélinquant, nous avons procédé à la mise en ligne d'un sondage composé de plusieurs questions (cf. annexe 6). Ce questionnaire a été construit selon notre expérience du domaine et de son actualité. Le questionnaire a fait l'objet de nombreuses critiques, surtout sur la forme du questionnement mais aussi sur le fond, reconnu comme parfois difficilement compréhensible. Ces remarques furent enrichissantes et constructives, nous entraînant, par la suite, à écrire de nouveau notre questionnaire (cf. annexe 7). Ce premier sondage

(mené avec la première version du questionnaire) a tout de même permis de dresser un tableau de considérations sociales vis-à-vis de l'objet de recherche. Une première question visait surtout à mesurer l'empreinte sociale des personnes se donnant la peine de répondre à un tel sondage en ligne sur un sujet très particulier, sachant que celui qui aura pris ce temps peut représenter celui qui se sent le plus concerné, et/ou aussi le plus préoccupé. De plus, la mise en ligne a de ce questionnaire a tenté de ne privilégier aucun monde social en particulier (voir détails *infra*).

Résultats détaillés du questionnaire « Mondes de la cyberdélinquance et image sociale du pirate informatique ».

Afin de percevoir plus clairement les significations sociales de notre objet de recherche, nous avons procédé à l'élaboration d'un sondage strictement relatif au pirate informatique et à sa perception. Le but de ce questionnaire était de mesurer comment les mondes de la cyberdélinquance pouvaient réagir face à l'objet social étudié, en développant des questions ciblées sur leurs niveaux de connaissances du domaine. Conscients du fait que ce sondage d'opinion peut apparaître « directif » : « *je veux dire par là non pas que la pensée des autres est inaccessible à ceux qui leur posent des questions, mais que souvent les questions imposent leur langage et leur économie aux réponses* »[148], notre investigation plus participante portera plus spécifiquement sur les autres mondes de la cyberdélinquance définis. Ce sondage a apporté ses propres résultats et fut analysé en tant que tel.

Ce questionnaire a été mis en ligne le 26 janvier 2006[149]. Ce dernier a permis de mettre en valeur certaines évidences. Sa promotion en a été faite dès cette date, *via* « *mailing* » et « *news* » sur des sites dédiés http://www.clussil.lu, http://www.cases.lu, http://www.zataz.com (autant de sites permettant de couvrir la plupart des mondes de la cyberdélinquance déterminés, en effet, le questionnaire a été relayé via les sites suivants :

[148] *Le chercheur et le quotidien. Phénomènologie des sciences sociales* (Auge, 1994).
[149] http://jph-cases.cc.org (de fin janvier à fin février 2006 : 161 personnes ont répondu entièrement à ce questionnaire : 90 se disent « citoyens »).

ZATAZ[150] représentant la communauté pirate, le site du CLUSSIL[151] représentant le monde de TIC et de la sécurité, enfin le site de CASES[152] ciblant plus spécifiquement le citoyen, les petites et moyennes entreprises, ainsi que les administrations). Il est intéressant de constater que la première réponse obtenue fut une tentative de piratage de la machine hébergeant le questionnaire. Cette anecdote traduit véritablement l'intérêt de ce monde social « *underground* » particulier, la complexité de ce milieu, et l'intérêt notable de notre question de recherche.

Notre questionnaire a permis de recueillir 161 réponses dont 90 citoyens déclarés comme tels. Certains de ces derniers observèrent des problèmes de définition quant au sujet traité empêchant la compréhension de quelques questions (« *on parle de qui ?*» - « *on ne comprend pas certaines questions!* » - « *les questions s'adressent à des spécialistes !* »…). Une réflexion s'est alors imposée sur les difficultés de compréhension de l'utilisateur IT (identifié alors en tant que tel) vis-à-vis du questionnaire que nous considérions comme basique. Ce dernier, destiné à l'origine à alimenter un sondage, devient dès lors un outil de recherche non négligeable. Le fossé semble, en effet, immense entre un expert du domaine, maîtrisant une image déterminée de l'objet social, et le citoyen, utilisateur IT profane, n'arrivant pas à fixer cette représentation. Il appert véritablement que des significations différentes du même objet sont données selon le monde social dans lequel l'individu s'inscrit. Ainsi, la construction sociale du pirate informatique serait le fait que tout individu pris dans un champ donné de l'espace social, par les dispositions particulières de l'habitus (ensemble de dispositions acquises par l'individu d'un champ donné, ces dispositions étant autant cognitives (opinions, schèmes de pensées, croyances, …) que pratiques (manière de parler, de marcher, de se vêtir, …)) qu'il y a acquises, se trouve prédisposé à concevoir et traiter les pirates informatiques d'une manière plutôt que d'une autre. Au cœur des significations sociales citoyennes, le pirate informatique n'est pas majoritairement considéré comme un personnage dangereux (40 % des réponses). Il est, par contre, majoritairement perçu comme un personnage

[150] Portail web de la communauté pirates francophones : http://www.zataz.com.
[151] Club de la Sécurité des Systèmes d'Information Luxembourg.
[152] *Cyberworld Awareness & Security Enhancement Structure Luxembourg*.

sympathique (pour 51 % il est génial, tandis que 19 % ne savent pas). Le pirate informatique n'est donc pas perçu comme un danger par le citoyen.

Pour ce dernier, l'image du pirate informatique est une représentation car dans la majorité des cas, il est rare pour ce dernier de rencontrer un pirate informatique. Il s'agit alors d'une représentation personnelle construite à travers des significations propres ou véhiculées. Nous parlerons d'images mentales, « *entités de « nature cognitive » reflétant, dans le système mental d'un individu, une fraction de l'univers extérieur à ce système*[153] ». Tout sujet dispose d'un ensemble de représentations constitutives de son information et de sa mémoire sémantique : ce sont les représentations-types. « *Cependant, comme il est impensable de traiter de l'être humain comme d'un sujet désinserré de tout milieu et compris comme « esprit pur », il y a lieu d'envisager la production des représentations mentales dans l'échange que chaque sujet entretien avec son milieu, puisque aussi bien ce sont les caractéristiques du milieu qui, à travers les situations vécues, mettent en jeu la production de telle ou telle représentation mentale* »[154]. Classiquement, on appelle ces représentations les représentations-occurrences. Pour origine de la représentation « citoyenne », allant au-delà des représentations-types, le vecteur des médias arrivant en tête (40 %).

Il est à noter que les diverses réactions à notre questionnaire démontre que la notion même de pirate est mal comprise ou à tout le moins sujette à controverse, la population ne semblant pas comprendre la même chose en parlant du même objet. Ainsi, à la question « comment vous représentez-vous le pirate ?», 50 % le posent en personnage génial ou sympathique, tandis que 34 % le trouve dangereux (16 % sont sans opinion). Puis le degré de dangerosité associé au personnage est jugé faible par 15 %, moyen par 42 %, important par 40 % (3 % sont sans opinion). De ses deux premières questions ressort un constat : la perception d'un personnage dangereux n'est pas flagrant, au contraire, l'objet semble jouir d'une certaine « reconnaissance », voire d'impassibilité. L'objet « pirate informatique », ainsi imaginé, tend à rimer avec « chevalier de l'innovation » (57 % le trouve en effet innovant, alors que 19 % seulement l'estime délinquant). Malgré tout, l'image négative est dominante (pour 63 %), ce qui peut

[153] Définition du Grand Dictionnaire de la psychologie, Paris, Larousse, 1992, p. 667 s.
[154] *Les représentations sociales* (Mannoni, 2001).

paraître paradoxal, mais en lien certainement avec la superposition d'autres représentations telles que celles médiatiques et experts SSI, par exemple, en terme de représentations-occurences. L'action malveillante est plutôt globalisée sous le format du délit (53 % des actions apparaissent comme répréhensibles de manière délictuelle, 8 % seulement de manière criminelle). Enfin, après une présentation de classification des pirates informatiques sous le format *Hackers*/*Crackers/Script-Kiddies* : 50 % relient correctement les termes avec les définitions correspondantes, tandis que 28 % se trompent sur la différence des définitions entre « *hacker* » et « *cracker* ». Une classification jugée d'importance pour les significations des experts sécurité, que les citoyens n'effectuent pas forcément.

La menace « humaine » de l'objet social est certainement la plus rencontrée et la plus présente sur Internet. Mais les utilisateurs ne connaissent pas les buts véritables des pirates informatiques, qui peuvent être très variables selon la personne et le contexte. Ainsi, les attaques génériques médiatisées dont on ne peut déterminer l'origine ou le(s) responsable(s), se traduisent souvent par un faux sentiment de vulnérabilité souvent non fondé. Identifier les menaces appropriées le concernant véritablement demeure pour l'utilisateur IT un enjeu complexe et difficilement maîtrisable. Ainsi, ce dernier peut soit se surprotéger ou encore n'appliquer alors aucune mesure de sécurité particulière. Un décalage de significations pouvant entraîner des appréciations de sécurité non appropriées, dans certains cas.

Ce qui semble certain, c'est un véritable décalage entre la représentation sociale acquise de la cyberdélinquance (avec pour socle central la reconnaissance de l'illégalité, et la vérification du jugement majoritaire des actes de cyberdélinquance comme moyennement ou fortement dangereux) et l'acteur même de cet acte qui jouit d'une certaine « bienveillance », d'un capital sympathie de la part du citoyen. Il est établi un décalage de valeur entre l'état de la cyberdélinquance et le pirate informatique qui jouit d'une image différente et paradoxalement inversée. Un objet social et des images sociales coexistent donc et les deux sont interdépendants. Il existe, à ce niveau, une reconnaissance de l'illégalité de l'acte, mais aussi une certaine légitimité pour l'acteur responsable des faits, semblant déterminer deux objets sociaux différents, un construit et l'autre en construction, ce dernier via alors différentes images, avec pour input non

seulement la représentation sociale de la cyberdélinquance, mais aussi une forte implication du monde social dans lequel l'acteur se situe, entraînant ces images différentes.

***

*

Résultats chiffrés du questionnaire « Mondes de la cyberdélinquance et image sociale du pirate informatique »

(Questionnaire mené de fin janvier à fin février 2006 : 161 personnes ont répondu entièrement à ce questionnaire, dont les résultats se déclinent ainsi (classement par ordre décroissant, pour chaque tableau la somme totale de réponses est de 161) :

<u>Question 1</u> : Qui êtes vous ?

Origine	Citoyens	Non catégorisés	Pirates informatiques	Institutionnels	Experts SSIC	Journalistes
Nombre de réponses	90	30	16	13	9	3

- Tableau 1. Questionnaire cyberdélinquance – Résultats question N°1

<u>Question 2</u> : Comment vous représentez-vous le pirate informatique ?

Il s'agit d'une représentation dans la majorité des cas, car il est rare d'être en présence d'un pirate informatique, il s'agit d'une présentation rejouée à travers des significations. L'objet est alors grandement construit à travers ce qu'en disent les autres.

Représentation perçue du pirate informatique	Nombre de réponses
Dangereux	55
Génial	43
Sympathique	37
Sans catégorisation	26

- Tableau 2. Questionnaire cyberdélinquance – Résultats question N°2

<u>Question 3 :</u> Quel degré de dangerosité associez-vous au pirate informatique ?

Degré de dangerosité associé au pirate informatique	Nombre de réponses
Moyen	68
Important	64
Faible	24
Ne savent pas	5

- Tableau 3. Questionnaire cyberdélinquance – Résultats question N°3

<u>Question 4 :</u> Qui vous permet principalement de fournir cette représentation du pirate informatique ?

Fournisseur de la représentation du pirate informatique	Nombre de réponses
Médias	46
Expérience personnelle	41
Pirates informatiques eux-mêmes	29
Experts SSIC	27
Aucune réponse	18

- Tableau 4. Questionnaire cyberdélinquance – Résultats question N°4

Les réponses à cette question entrent au cœur de notre problématique.

<u>Question 5 :</u> Comment trouvez-vous les pirates informatiques ?

Caratéristiques du pirate informatique	Nombre de réponses
Innovant	91
Déviant	34
Délinquant	30
Ne savent pas	6

- Tableau 5. Questionnaire cyberdélinquance – Résultats question N°5

<u>Question 6 :</u> Comment trouvez-vous l'image du pirate informatique ?

Image du pirate informatique	Nombre de réponses
Négative	100
Neutre	37
Positive	23
Ne sait pas	1

- Tableau 6. Questionnaire cyberdélinquance – Résultats question N°6

La majorité sait dire le rendu sociétal de l'objet en terme de représentation, et c'est véritablement une orientation négative qui est retenue. Ce qui ne veut pas dire que ces personnes trouvent le pirate informatique négatif, mais que la représentation sociale semble elle-même négative.

<u>Question 7 :</u> Pensez-vous que cette image est largement dominante au cœur de la société :

Image du pirate informatique	Nombre de réponses
Oui	72
Non	61
Ne savent pas	28

- Tableau 7. Questionnaire cyberdélinquance – Résultats question N°7

<u>Question 8 :</u> Comment les actions des pirates informatiques sont-elles répréhensibles ?

Type de répression pour les actes de piratage informatique	Nombre de réponses
Répréhensibles de manière délictuelle	74
Répréhensibles de manière contraventionnelle	27
Ne savent pas	25
Répréhensibles de manière criminelle	20
Non répréhensibles	15

- Tableau 8. Questionnaire cyberdélinquance – Résultats question N°8

<u>Question 9 :</u> Comment définiriez-vous la cyberdélinquance ?

- Le moyen d'utiliser un médium informatique pour un crime ou délit conventionnel ?
- Le moyen d'attaquer un médium informatique en tant que cible ?
- Les deux sont possibles ?

Définition de la cyberdélinquance	Nombre de réponses
Les deux approches sont possibles	97
Le moyen d'utiliser un médium informatique pour un crime ou délit conventionnel	42
Le moyen d'attaquer un médium informatique en tant que cible	22

- Tableau 9. Questionnaire cyberdélinquance – Résultats question N°9

<u>Question 10 :</u> Un *hacker :* c'est un pirate qui vise à détruire ou voler des données disponibles sur un site victime ?

Définition du *hacker* proposé (voir *supra*)	Nombre de réponses
Faux	111
Vrai	50

- Tableau 10. Questionnaire cyberdélinquance – Résultats question N°10

<u>Question 11 :</u> Un *cracker* : c'est un pirate qui recherche des failles de sécurité afin de progresser au niveau technologique ?

Définition du *cracker* proposé (voir *supra*)	Nombre de réponses
Faux	104
Vrai	57

- Tableau 11. Questionnaire cyberdélinquance – Résultats question N°11

<u>Question 12 :</u> Les pirates informatiques forment-ils une véritable communauté au niveau international ?

Les pirates informatiques forment une véritable communauté	Nombre de réponses
Vrai	93
Faux	68

- Tableau 12. Questionnaire cyberdélinquance – Résultats question N°12

<u>Question 13 :</u> Connaissez-vous cette classification des acteurs de la cyberdélinquance :

- «*Script kiddies*» : jeunes pirates informatiques de bas niveau

- «*Crackers*» : pirates qui attaquent un site pour destruction ou vol de données

- «*Hackers*» : pirates qui visent à découvrir des failles de sécurité pour en comprendre le fonctionnement

Cette classification vous semble t-elle :

- Juste ?

- Fausse ?

- Restrictive ? Pourquoi ?

Catégorisation des pirates informatiques proposée (voir *supra*)	Nombre de réponses
Juste	73
Restrictive[155]	46
Fausse	39
Ne savent pas	3

- Tableau 13. Questionnaire cyberdélinquance – Résultats question N°13

(Exemple de commentaires (sic)) :

« - Vous parlez partout de « pirates » ; c'est sûr qu'après on en a une image si négative.

- Vous orientez trop votre formulaire, on n'a pas de choix, en gros les pirates sont méchants.

- Un cracker « crack » des protections (de logiciel par exemple alors qu'un « lamer » attaque pour détruire).

- Tout n'est pas exact.

- Tout n'est pas blanc ou noir...

- Où se trouve la notion de piratage musique/film, etc… fortement présente dans les medias.

[155] Voir *infra* des exemples de commentaires reçus en réponses à cette classification.

- Nous n'avons pas la définition de « pirate ».

- Les hackers ne sont pas nécessairement assimilables à des pirates.

- Les critères sont trop hétérogènes.

- Les Crackers visent aussi à decouvrir des failles de sécurité (pas tous bien évidemment).

- Les crackers cassent aussi des protections logicielles, leur cible n'est pas uniquement internet.

- Le crackeur casse des mots de passe ou des protections.

- Le cracker, celui qui crack, qui casse la protection qu'elle soit logiciel, mot de passe, ...

- Le « hacker » vise à comprendre les technologies et à dépasser les limitations existantes.

- La scène est formée de nombreuses « castes ».

- Il y a un grand nombre de catégories, celles-ci ne sont que les principales!

- If Hacker = Pirate Then Msgbox « Vous êtes en tord ».

- Difficile de catégoriser les pirates.

… ».

<u>Question 14 :</u> Le dernier rapport « *e-crime watch survey* » du *Computer Emergency and Response Team-CC* (CERT-CC) faisait état de quelles pertes estimées, relative à la cyberdélinquance ?

Montant des pertes estimées par le CERT-CC (en dollars)	Nombre de réponses
666 millions	87
222 millions	55
111 millions	19

- Tableau 14. Questionnaire cyberdélinquance – Résultats question N°14

***

*

Nous avons pu également tester, sur un petit échantillon (quinze personnes), notre seconde version du questionnaire amélioré (cf. annexe 7), suite aux nombreux commentaires reçus par rapport au premier réalisé et utilisé (cf. *supra*). Il ressort de ce second sondage des qualifications plus fines. En effet, nous avons souhaité globaliser les résultats pour le premier sondage afin d'obtenir une vue générale de la perception de l'objet de recherche. Cependant, nous avons eu l'occasion de consulter, pour le second, un monde spécifique (90 % des répondants étaient, en effet, étudiants, spécialistes ou experts en SSIC) appartenant donc à un monde social particulièrement concerné, données recueillies lors d'une conférence sécurité organisée par nos soins en septembre 2006[156]. Il en ressort, forcément (en relation avec leur contexte social direct), que ces derniers ont, avec les médias, répondu en majorité que l'image du pirate informatique est nourrie par les experts SSIC (Il semble, en effet, que lorsqu'on est attaché à un monde, on y puise au moins forcément ses propres significations sociales, et que ce monde oriente les significations attachées. Pour le citoyen, non expert ou ne fréquentant pas ces réseaux, il s'agira des médias). A ce titre, il appert que les résultats sont, sur certains points, éloignés de ceux retenus et globalisés par le premier sondage (cela traduisant la différence effective de culture et de connaissance selon le monde d'appartenance, pour interroger un objet). Cependant, nous ne pouvons effectuer une comparaison directe, le questionnaire même ayant été fortement refondu aux fins de simplification compréhensive, et de facilité d'analyse des résultats. De ces personnes qualifiées dans le domaine, une seule se trompe, par exemple, sur la différence sémantique entre un *hacker* et un *cracker*. De plus, la classification des pirates, distinguant « *hackers* », « *crackers* » et « *script-kiddies* » est à 90 % reconnue comme juste. Par contre, pour la perte financière, l'estimation des répondants est souvent surestimée vis-à-vis des chiffres de référence du CERT-CC, plus de la moitié estiment, en effet, les pertes à plusieurs milliards de dollars (alors que le chiffre de référence en réponse est de 666 millions de dollars). Mais la nouvelle version du questionnaire permet surtout de rendre compte de la perception des risques associés et retenus de la cyberdélinquance, et ressortent majoritairement comme étant « le préjudice financier » et « les pertes graves » pour 85 % des répondants. Cela confirme la

[156] http://www.spiral.lu

représentation sociale de la cyberdélinquance comme un « repère » social fort en termes d'impacts préjudiciables de cet objet (pouvant aussi expliquer la surestimation précédente). Ensuite, la qualification du pirate informatique est unanime : le pirate informatique est une personne « compétente en informatique » et « dangereuse » (mais soit « potentiellement » ou bien « moyennement »). Ainsi, pour 80 % des répondants, l'image du pirate informatique est négative et dominante (finalement, cette caractérisation par un monde expert, entraîne, de facto, une baisse du capital « sympathie » globalisé par le premier sondage). Mais, à ce titre, la qualification des actes de cyberdélinquance est considérée comme un délit sans plus, voire un acte peu grave, tout en étant toujours qualifié comme hors-la-loi ; et très peu (25 %) estime que le pirate informatique fait preuve d'innovation (alors qu'il apparaissait dominant dans les résultats du premier sondage global). La caractéristique la plus intéressante repose sur la qualification pénale des peines, en effet une seule personne répond en souhaitant une répression par la prison pour ces actes de cyberdélinquance, tandis que le reste estime des peines d'amendes suffisantes (ce qui correspond à la plus basse classe de répression). Encore une fois, cela préfigure un paradoxe entre l'état de la cyberdélinquance considérée comme dangereuse, entraînant la perception d'une image du pirate informatique dangereux mais avec des peines de répression (émanant de la société même) souhaitées très basses, sans commune mesure avec leur gravité. Ainsi, l'acteur même de cet acte jouit encore d'une certaine « bienveillance », de la part du répondant, même issu d'un monde très spécialisé sur le domaine.

Fondamentalement, ces questionnaires n'ont pas vocation à donner aux résultats une dimension générale ; cependant, ils permettent de rendre compte des éléments d'opinion publique qui constituent un cadre structurant pour notre propos, visant à déterminer la complexité d'un acteur social, soumis à de nombreux paradoxes en terme d'images sociales, et objet de recherche incontestable des sciences de l'information et de la communication. Plus en avant, vis-à-vis de notre problématique, nous investiguerons, en premier lieu, le monde qui est souvent cité comme référence de production de l'image du pirate informatique, par la somme globale des répondants, et semble guider les représentations publiques, à savoir les médias. De plus, selon leur spécificité même et

leur but, les médias sont interrogés de manière nécessaire en relation avec notre problématique, comme le principal vecteur possible et majoritaire de l'image véhiculée du pirate informatique, au cœur de l'opinion publique. Il s'agit du repère primaire du citoyen quant à la diffusion et à la pénétration possible des images véhiculées de notre objet de recherche. Il sera étudié en tant que tel.

3) L'image médiatique « dominante » du pirate informatique

Dans ce contexte, les attaques numériques sont relativement maîtrisées au niveau sociétal notamment *via* la sensibilisation, les nombreuses mises à jour disponibles des failles de sécurité, ou encore l'offre de la mise en place de contre-mesures. Mais, au-delà des attaques techniques connues, il semble que l'être humain, à son tour, soit devenu le véritable danger sur les réseaux informatiques. Nous nommerons « pirate informatique » celui que nous considèrerons comme l'élément principal déclencheur du risque numérique. Si nous considérons le risque traditionnel comme un objet social construit, nous avons vu que la problématique se pose aussi quant au risque numérique, et se « sédimente » finalement *via* la cyberdélinquance reconnue ainsi. Mais est-il aussi plutôt de l'ordre d'un objet social en construction, notamment au regard de la complexité de la représentation de son auteur principal : le pirate informatique difficilement appréhendable socialement? Principalement guidé par cette interprétation, réside la difficile mais nécessaire représentation pour tout un chacun des pirates informatiques, car peu présent physiquement au quotidien, et rarement rencontrés directement en tant que tels. Par défaut, le milieu « *underground* » demeure inconnu et non perçu directement par la majorité. Ce dernier ne peut alors échapper aux nécessaires représentations, tel que le définit P. Mannoni (cf. *supra*). Toutes ces notions renvoyant de près ou de loin aux représentations, nous analyserons la multiplicité des significations possibles du pirate informatique, *via* différents mondes sociaux, ne favorisant résolument pas la représentation unifiée de ce dernier, mais plutôt sa représentation « différentielle ». Ainsi, nous avons prévu de poser notre objet de recherche comme complexe en termes de représentation sociale (non acquise, nous parlerons plus facilement de « significations sociales »). Nous tenterons de cerner cette complexité, et d'apporter des pistes de compréhension à travers l'observation des mondes sociaux qui apparaissent comme les

plus directement concernés, comme ceux qui traitent principalement de ce sujet, qui apportent ainsi des significations spécifiques à l'objet de recherche, et qui participent à la construction de sa réalité, de sa connaissance.

Les différentes significations des menaces numériques :

Aujourd'hui, les solutions techniques simples de sécurité (anti-virus, *firewall* personnel…) semblent connues et/ou bien maîtrisées par la plupart des utilisateurs IT. Cette appropriation a notamment été facilitée par les fournisseurs de solutions techniques et, les dernières années, par la médiatisation constante des besoins de sécurité associés. Au-delà des appropriations techniques, il demeure cependant très complexe de déterminer et de qualifier les véritables responsables de ces attaques, de surcroît pour l'utilisateur IT. En effet, cette menace ne trouve-t-elle pas finalement pour écho une acquisition sociale floue voire parfois inexistante, notamment en raison de l'obscurité du milieu « *underground* » ? Pour le vérifier, nous avons rendu compte d'un sondage récent permettant d'établir une vue de cette perception par une majorité d'utilisateurs IT (cf. *supra*). Ensuite, nous proposons d'identifier les principaux mondes qui traitent de notre objet social de recherche, afin d'en interpréter les significations qu'ils produisent. Nous distinguerons, à ce titre, nous l'avons vu, les mondes suivants : les médias, les experts sécurité et enfin les pirates informatiques eux-mêmes. Ces mondes encadrent et déterminent, en effet, les attributs sociaux de l'objet et les présentent en tant que tel. Pour chacun, nous avons déterminé des moyens particuliers d'investigations permettant de dégager et de décrire des spécifications sociales précises.

Les représentations médiatiques dominantes :

Nous avons identifié, *via* notre sondage et corroboré par notre expérience professionnelle, que la représentation médiatique de notre objet de recherche joue un rôle clé dans la formalisation de sa connaissance pour l'opinion publique. Les travaux récents en sciences de l'information et de la communication, par exemple, ont permis de souligner le rôle d'amplification que les médias peuvent avoir dans l'émergence d'un événement, ainsi que leur influence sur les décisions politiques pouvant en découler. Les

représentations médiatiques du pirate informatique, sont nombreuses et peuvent être traitées à travers différents médias comme le cinéma, la presse écrite, la télévision, ou encore Internet. L'effet de cadrage des médias conduit à la construction d'un univers mental de représentations qui peut induire une image plus ou moins positive et une acceptabilité sociale plus ou moins étendue d'une activité donnée. Les médias sont pour le grand public, quasiment le seul outil permettant d'obtenir des informations « accessibles et compréhensibles » sur le phénomène de la cybercriminalité. Nous avons donc cherché à évaluer la manière dont le thème de la cyberdélinquance circule dans l'espace médiatique, afin de mieux cerner la façon dont peut s'y construire les significations du pirate informatique.

Ainsi, dans le cadre d'une recherche précédente[157], nous avons effectué une démarche de mise en indexation et de veille d'articles, de presse généraliste et spécialisée informatique, substantiels consacrés à la cybercriminalité. En d'autres termes, il s'agit d'articles, présentant Internet comme porteur de menaces, et mettant en scène de facto le pirate informatique. Ce corpus est constitué de 28 références dont 18 titres parus dans la presse généraliste et 10 dans la presse spécialisée, sur la période 1995-2002. Durant celle-ci, les discours médiatiques sur la cybercriminalité observent deux grandes tendances. Tout d'abord la volonté d'informer et d'instruire au sujet de ce phénomène nouveau que les journalistes découvrent en même temps que le public. Les médias traitent, dans un premier temps l'information dans le but d'éveiller les consciences face à une menace afin de susciter chez les utilisateurs la nécessité de se doter de SI sécurisés. La plus grande médiatisation accordée à cette question s'attache à montrer le caractère illégal des activités cybercriminelles. En marge du développement de la cyberculture et de la sacralisation de « l'internet », de nouvelles nuances sémantiques et thématiques apparaissent qui correspondent au développement de nouveaux phénomènes sociaux, politiques et économiques liés à la cybercriminalité. Vont alors apparaître sur la scène médiatique des concepts tels que « *hacktivistes* » et « cyber-résistance », par exemple. De son côté, la presse spécialisée s'en tient plutôt aux aspects techniques et pratiques de la question tout en essayant de poser une définition du phénomène cybercrime et de ses

[157] *La cyberdélinquance, un risque pour Internet ?* (Humbert, 2003).

acteurs principaux. Tout proche du phénomène « cyberculture », la deuxième grande tendance dans les discours médiatiques est l'approfondissement de la connaissance sur le sujet à travers une réflexion sur le profil type du « *hacker* » et de sa philosophie, ainsi que de la culture « *underground* ». Les journalistes, quel que soit leur médium de rattachement, ont tenté de déterminer la différence entre les « *hackers* » et les « *crackers*». L'image des « *hackers* » se voit mise en valeur : on les définit comme des passionnés qui aiment les défis et maîtrisent à la perfection les moindres détails des SI. Leurs activités sont certes illégales, mais ils agissent en respectant une certaine éthique. En opposition au discours alarmiste de la situation dangereuse, l'« image » des « *hackers* », véhiculée par les médias, semble plutôt sympathique et débarrassée de véritables attributs négatifs. Ceci expliquerait la perception actuelle des citoyens, mise en évidence par notre sondage réalisé.

Cette analyse du discours médiatique de 1995 à 2002 (qui n'a pas véritablement changée au cours de ces dernières années) se traduit par diverses représentations que nous allons relever afin d'en évaluer la pertinence. En effet, des experts du domaine ont-ils été systématiquement convoqués pour vérifier tel ou tel faits, le monde « cybercriminel » a t-il été observé de l'intérieur ? Souvent, face à une exigence d'empathie, et le besoin de sensationnel, de « scoop », le stéréotype, par exemple, peut alors devenir économe et consensuel (nous entendons par stéréotype, un cliché mental stable, constant et peu susceptible de modification). Les stéréotypes relèvent de ce qu'on appelle plus facilement les idées reçues, rendant plus facile la communication, et permettant d'éviter un exposé long, discursif ou démonstratif. Ainsi, si ce dernier rencontre l'adhésion du plus grand nombre, il va aussi pouvoir s'installer dans les imaginaires de la communauté, des citoyens. Le besoin de convaincre peut, dans ce cadre, aussi occulter le besoin de véracité, car les médias apportent souvent l'image du héros, la recherche du challenge, le génie, vis-à-vis de faits qui font appel à des événements qualifiés légalement de gravité souvent extrême. Ce clivage peut entraîner la difficulté de représentations par l'utilisateur, voire l'erreur de représentation sociale. En effet, un amalgame dangereux entre des faits illégaux et des acteurs sociaux exclus de toute responsabilité, devient alors possible au sein des représentations citoyennes. Ces réflexions nous engagent à étudier plus spécifiquement la construction des significations médiatiques en regard de notre

objet de recherche, cela en utilisant plusieurs instruments conceptualisés, en plus de l'analyse du corpus de presse annoncé *supra*.

II – Rapport des médias à la construction de l'image sociale du pirate informatique

Après les avoir établis et détaillés, notre approche d'observation participante, à la lumière de notre expérience professionnelle, et de notre méthodologie retenue, va permettre d'approcher de l'intérieur les différents mondes de la cyberdélinquance. Ce « plongeon » vise essentiellement à « éclairer » le personnage principal de la cyberdélinquance : le pirate informatique. Un objet résolument en construction, car multi-faces, *via* son contexte social complexe ? Notre recherche vise, dans un premier temps, l'investigation des représentations médiatiques de la cybercriminalité (en tenant compte de leur rôle particulier dans la formalisation des connaissances de l'opinion publique, en regard de l'objet de notre étude). Pour ce faire, nous analyserons ce discours à travers plusieurs instruments que nous avons mis en place, en rapport avec le traitement médiatique de l'objet de recherche, notamment *via* Internet, la presse écrite française (voir *supra*) et la rencontre avec des journalistes impliqués sur cette thématique.

1) Veille médiatique – Internet :

Les médias (communication « médiatisée ») résument, le plus souvent, le seul dispositif permettant d'obtenir des informations sur le phénomène de la cybercriminalité. Ainsi, tenant compte de cette importance, notre étude propose d'établir une partie de veille technologique de l'objet, appliquée à l'information de type presse grand public, notamment véhiculée *via* Internet. Nous avons privilégié une recherche indexée sur les mots-clés « cybercriminalité » et « pirates informatiques », *via* un abonnement de type « *Google Search* ». Cette veille a été entreprise depuis début janvier 2006 et a été conduite jusqu'à juin 2006. Nous nous sommes attachés à relever, classer, annexer et analyser cette documentation.

La densité des alertes peut être associée au degré d'importance accordée à chaque thème respectif par les médias qui couvrent le phénomène cybercriminalité pendant la période étudiée. Ainsi, on remarque une prédominance des textes qui portent sur la situation internationale et sur les techniques de piratage. Le thème des condamnations est également bien représenté. Viennent ensuite les études et enquêtes publiées, et le cadre juridique en matière de cybercriminalité. Enfin, quelques alertes portant sur les événements et les tendances sont recensées. Cette distribution quantitative permet de dégager quelques grandes tendances en matière de cybercriminalité caractéristiques de la période concernée. En effet, le phénomène s'internationalise de plus en plus. Avec le développement rapide des technologies numériques, on voit apparaître de nouvelles formes de « cyber-banditisme » encore plus sophistiquées. Les professionnels de la sécurité des systèmes d'information se doivent donc de mettre au point et de proposer aux utilisateurs de nouvelles protections encore plus efficaces pour faire face à une menace grandissante. En même temps, quoique le taux de poursuite judiciaire reste faible par rapport à l'ampleur du phénomène, des peines plus ou moins lourdes selon les pays sont appliquées aux délinquants.

Par ailleurs, des spécialistes s'engagent davantage à mener des études et des enquêtes avec l'objectif de mieux connaître le phénomène de la cybercriminalité. En outre, pour faire face aux infractions liées aux technologies de l'information et de la communication, des lois nationales spécifiques se mettent en place et une volonté de coopération internationale s'affirme. Enfin, la grande majorité des alertes est rédigée dans un style informatif et descriptif qui permet de se tenir au courant en « survolant » les faits, sans approfondir. Un seul texte fait exception en adoptant une forme analytique pour proposer une réflexion sur les fondements d'une contre-culture des années 1990 connue sous le nom de *cyberpunk*. Les détails de notre analyse de cette veille médiatique sont les suivants :

- Alertes Google sur les mots clés « pirate informatique » et « cybercrime » (Cf. annexe 10)[158]

Janvier à juin 2006

Pour la période janvier – juin 2006, on relève 68 alertes Google sur les mots clés « pirates » et « cybercrime ». Les textes se distribuent dans les rubriques suivantes : contexte international (17 alertes) ; techniques de piratage (17 alertes) ; paroles d'experts en cybercriminalité (3 alertes) ; condamnations à travers le monde (10 alertes) ; événements nationaux et internationaux en matière de cybercriminalité (4) ; études et enquêtes menées dans le domaine de la cybercriminalité (7 alertes) ; cadre juridique national et international (6 alertes) ; tendances (2 alertes) ; divers (2 alertes).

- Tableau 15. Classement des alertes Google (mots clés « pirates » et « cybercrime »)

Thème	Nombre d'alertes
Contexte international	17
Techniques de piratage	17
Condamnations à travers le monde	10
Études et enquêtes menées dans le domaine de la cybercriminalité	7
Cadre juridique national et international	6
Événements nationaux et internationaux en matière de cybercriminalité	4
Paroles d'experts en cybercriminalité	3
Tendances	2
Catégorisation - divers	2

[158] Note : chaque numéro entre-parenthèse renvoie vers le numéro de l'article concerné.

Textes relatifs à la situation internationale :

Les ordinateurs sont une porte ouverte aux fraudeurs. Chaque année, les PME du Québec perdent des milliers de dollars pour ne pas avoir sécurisé leurs recherches et leurs produits (4). Dans le même temps, des centaines de citoyens sont victimes d'escrocs du commerce électronique. Que faire ? C'est pour répondre à cette problématique qu'est né l'Institut de sécurité de l'information du Québec (ISIQ) dont la mission est de donner aux Québécois des outils et des moyens de se protéger de la cybercriminalité. Le Gouvernement du Québec a investi 250 000 $ pour soutenir l'organisme.

La Bourse russe a été attaquée par un pirate au moyen d'un virus. Selon la compagnie *Kaspersky*, la machine infectée était contrôlée à distance pour lancer une attaque de type *Denial-of-Service* contre d'autres machines du réseau (7). Selon les experts, c'est une attaque spécifique et il reste à déterminer si celle-ci visait à extorquer des fonds ou simplement vandaliser le réseau. Suite à la publication de douze caricatures mettant en scène le prophète Mahomet par le quotidien danois Jyllands-Posten, des centaines de sites danois ont été pris d'assaut par des pirates informatiques. Ils détournent leur contenu et les remplacent par des pages à la gloire de l'islam ou des menaces à l'encontre de ceux qui profaneraient l'image de la religion coranique (13).

Pour faire face à une criminalité, sous toutes ses formes, qui va en s'amplifiant, les pouvoirs publies en Algérie ont créé un Comité national de coordination des actions contre la criminalité. Cette initiative concerne également la formation spécialisée de plus en plus pointue des personnels pour pouvoir combattre la cybercriminalité (17). La lutte contre le commerce illégal de médicaments sur Internet n'est pas suffisamment organisée. L'Organe international de contrôle des stupéfiants alerte sur le développement de cette cybercriminalité très profitable (23).

Lors d'une réunion de travail entre Pascal Clément, Garde des Sceaux, Ministre de la justice en France, et son homologie américain, Alberto Gonzales, Secrétaire à la Justice, Attorney General des Etats-Unis, des thèmes d'intérêt commun et sensibles ont été abordés dont la cyberciminalité. La France venait effectivement de ratifier la convention du Conseil de l'Europe, cet instrument novateur qui permet de lutter contre les atteintes aux systèmes informatiques, ainsi que les délits commis par le biais d'un

système d'information, notamment la pornographie enfantine et l'atteinte à la propriété intellectuelle. Dans le protocole additionnel que la France a également ratifié, les comportements à caractère raciste ou xénophobes sont également concernés. La France et les Etats-Unis partagent effectivement un intérêt commun, celui de promouvoir, sur le plan international, et dans les relations bilatérales, des instruments juridiques efficaces et opérationnels (25).

La police australienne arrête à Victoria un *hacker* de 22 ans grâce aux informations de la *Federal Computer Crime Unit belge* (FCCU) (36, 41, 43).

La police cantonale valaisanne poursuit son action préventive contre la pédocriminalité sur Internet. En collaboration avec d'autres organismes, elle s'adresse directement au grand public par sa présence à la foire valaisanne Sion-Expo (45). Garry McKinnon, un Anglais, développeur au chômage, avait été arrêté, soupçonné d'avoir pénétré illégalement le système informatique du *Pentagone*, de *l'US Navy*, de la *NASA*, engendrant 900 000 $ de dommages dans les serveurs. L'affaire remonte à la fin 2001 et depuis, les Etats-Unis cherchent par tous les moyens à faire extrader l'individu (54, 60).

Des pirates informatiques dérobent sur des sites bancaires britanniques mal protégés des données concernant des cartes bancaires et les mettent en vente sur Internet. Les prix de vente varient entre un et dix dollars (56). Un réseau de criminalité transnationale opère en Russie. L'accent est mis sur le trafic de stupéfiants et sur la cybercriminalité. Les terroristes sont recrutés et formés *via* Internet (57).

La Sûreté du Québec doit se doter de moyens afin de contrer la cybercriminalité, un fléau en pleine expansion (61). Les Etats-Unis dénoncent le piratage de jeux vidéo par des militants islamistes férus d'informatique et appartenant à *al Qaïda* ou à d'autres groupes. Selon les autorités américaines, ces militants veulent délivrer un message politique et idéologique (63, 64).

Sur les techniques de piratage :

Plusieurs textes – 8 au total - concernent les différentes affaires de *phishing* qui ont marqué le semestre (46, 47, 48, 49, 50, 51, 52, 53). En France, les victimes ne sont pas nombreuses, mais la menace est tout de même grandissante. En effet, en février et en mars 2006, des escroqueries en ligne ciblant les clients des banques *LCL*, *Société*

générale et *BNP Paribas* ainsi que les clients de la société *Visa* ont été perpétrées. Le nombre de clients touchés reste limité, mais les attaques ont tendance à s'améliorer et des variantes plus sournoises apparaissent même si le procédé est toujours le même. L'originalité de ce type d'attaque sur Internet n'est pas d'exploiter une quelconque vulnérabilité informatique, mais la faille humaine à savoir un client crédule, peu méfiant, trop curieux. Le bilan chiffré des victimes de *phishing* est difficile à obtenir, les banques préférant rester discrètes sur le sujet. Le premier signalement de ce type d'attaque en France, par le CLUSIF, a eu lieu en 2003. Depuis, le mode opératoire n'a pas changé. La seule vraie évolution est effectivement la qualité des faux mails expédiés et des faux sites. En France, on connaît deux condamnations d'auteurs de *phishing*, des individus isolés agissant sur le territoire français : en janvier 2005 (un faux site du *Crédit Lyonnais*) et en septembre 2005 (un faux site de *MSN (Microsoft)*). Cependant, la plupart des attaques émane de groupes malfaiteurs organisés depuis l'étranger. Dans ce cas, si les banques déposent plainte, l'action judiciaire sera compliquée et dépendra des accords internationaux passés par la France. De plus, il y aurait deux phases essentielles : d'abord la fermeture des sites et puis ensuite, l'identification des auteurs pour engager des poursuites.

Les réseaux de PC détournés par des pirates informatiques ont connu, en 2005, un essor sans précédent. Selon l'éditeur *Panda-Software*, les « *botnets* », ces réseaux fantômes de PC piratés, ont vu leur nombre exploser par rapport à 2004. En 2005, *Panda-Software* a dénombré plus de 10 000 variantes différentes de ces techniques de piratage, dont 6 000 pour le seul « *Gaobot* » connu encore sous le patronyme « *Agobot* » (1). Après le *phishing*, les cybercriminels attaquent avec l' « e-gène » (9). A l'occasion du salon Solutions Linux, Marc Blanchard, directeur de *l'European Antivirus Scientific* Center chez *Kaspersky Lab*, explique les dernières tendances antivirales. L'empoisonnement du DNS, ou l'attaque informatique totale : le « *pharming* » plus redoutable que le *phishing* (16).

Un article clair, lisible et instructif a pour but de sensibiliser le public aux dangers inhérents à l'ère numérique. Est offert un aperçu du piratage informatique et des motivations des pirates tout en donnant quelques conseils pour se protéger (26)

Selon la société *Lexsi*, le *phishing* est une fraude « nouvelle génération » qui n'a de cesse de discréditer les services en ligne des institutions bancaires (27). La force du *phishing* est la faille humaine. Les techniques mises en œuvre dans ces attaques évoluent continuellement afin de faire face aux systèmes de protection des banques. Les établissements français sont relativement épargnés dans ce type de fraude et l'impact global est inférieur à 5 millions d'euros chaque année. La particularité linguistique française et les moyens d'authentification mis en œuvre par les établissements français sont des facteurs clés pour la protection de leurs clients.

La société *Sophos*, spécialisée dans la sécurité informatique, dévoile qu'un site russe vend le nécessaire du parfait petit pirate pour 15$ (28). « *Googlebot* » était déjà connu pour ses nuisances à la confidentialité de certains données et rapports. Mais, pour la première fois, on donne l'exemple d'une suppression de site (37).

Le *phishing* devient de plus en plus subtil. Après une opération de *hacking* conduite sur les serveurs mêmes des banques visées, les pirates ont glissé des mécanismes de redirection capables de détourner les clients et de les orienter vers un tout autre site dont on devine la finalité (42). A l'instar de la « *Hackacademy* » parisienne, l'éditeur spécialisé dans le domaine de la sécurité informatique McAfee présente son programme de formation aux techniques de *hacking* principalement pour les directeurs des services informatiques (DSI). L'objectif de ces cours est de montrer aux responsables informatiques des entreprises petites et grandes, comment se protéger de façon proactive contre les méthodes utilisées par les *hackers* (62).

Paroles d'experts en cybercriminalité :

Une interview avec J-P Ney (3) – auteur, entre autres, du livre « *Souriez, on vous espionne* » - permet de savoir quel est le rôle d'un journaliste de défense, à savoir traiter à 100 % de son temps des questions de ce domaine, de sécurité internationale et de terrorisme. L'*Association des Journalistes de la Défense* réunit des spécialistes de la défense et des journalistes en leur permettant d'échanger des points de vue et des expériences. J-P Ney est un autodidacte passionné qui pratique l'investigation à l'anglo-saxonne, un investissement personnel très important, peu populaire en France. En tant que membre de l'*Institut International des Hautes Etudes de la Cybercriminalité*, il

entreprend une série de recherches dès 1998. Selon J-P Ney, le souci, en France, c'est que les policiers qui font partie de l'OCLCTIC se forment tout seuls et que généralement, ils ne connaissent pas de l'intérieur le monde des *hackers* et autres cybercriminels qui eux dépendent fréquemment d'organisations mafieuses et/ou terroristes. L'administration devrait donc collaborer plus souvent avec des sociétés privées et des groupes de recherches civils et/ou militaires. En France, il s'agit de développer une culture du renseignement plus poussée. J-P Ney est également à l'origine d'une association dénommée « Centre International de Recherches et d'Etudes sur le Terrorisme & l'Aide aux Victimes du Terrorisme » (CIRET – AVT) dont le but est de partager des connaissances sur le terrorisme et sur les moyens à mettre en œuvre pour combattre ce fléau. Le CIRET – AVT est affilié au programme *Search for International Terrorist Entities*.

Dans le cadre d'une interview accordée par des représentants de *Microsoft*, le point est fait en matière de terminologie. Il s'agit de faire la différence entre des notions de base telles que « logiciel gratuit », « logiciel *Open source* » et « logiciel libre ». ce dernier respecte effectivement les quatre libertés définies par la *FSF* : la liberté d'exécuter le programme, la liberté d'étudier le fonctionnement du programme, la liberté de redistribuer des copies, la liberté d'améliorer le programme et de publier ses améliorations (15). Lors d'une conférence, le directeur du FBI Robert Mueller, invité par la *Business Software Alliance* (BSA) a déclaré qu'en matière de cybercriminalité les entreprises piratées doivent porter plainte. La coopération entre les entreprises et l'administration doit être systématique pour combattre la menace (20).

Condamnations :

La condamnation par le Tribunal correctionnel de Bastia de « *Dany Corsica* », auteur de plusieurs sites de téléchargement illicites a été saluée par la *Business Software Alliance* (BSA, regroupant Microsoft, Adobe et d'autres éditeurs) (5). L'auteur du site 2bcalvi.com proposait un grand nombre de logiciels, accompagnés des cracks adéquats permettant de contourner les protections. La peine appliquée est non négligeable : 24 mois de prison, dont 9 avec sursis et 10 000 € d'amende.

L'inculpation par la justice américaine d'un groupe de pirates nommé RISCISO, pour vol massif de logiciels. Les accusations concernent notamment deux personnes vivant à l'extérieur des Etats-Unis. Chacun risque un maximum de 5 ans de prison et 250 000 $ d'amende. Un pirate condamné à deux ans de prison pour cyberattaques qui auraient perturbé des millions d'internautes espagnols (8). Le jugement du tribunal espagnol prévoît également le paiement d'une amende conséquente de 1,8 millions d'euros. D'après le site *Outlaw.com*, 19 membres d'une importante équipe de pirates - dénommée RISCISO - spécialisés dans le *warez* ont été arrêtés aux USA, au terme d'une longue enquête. D'après le site *The Register*, ils encourent trois à cinq ans de prison et une amende de 250 000$ (11).

Deux membres d'un réseau britannique de *hackers* spécialisés dans la falsification des cartes bancaires de paiement ont été présentés devant le juge d'instruction près le Tribunal de première instance de Tanger sous les chefs d'inculpation de falsification de documents bancaires et usurpation d'identité (12). Même dans un contexte pédagogique, l'intrusion sur des comptes utilisateurs protégés par des mots de passe cryptés est une infraction constituée. Quatre étudiants ont été condamnés par le Tribunal de grande instance de Vannes pour avoir accédé frauduleusement au système de traitement automatisé de données du réseau pédagogique de leur université (38).

Yahoo pourrait être poursuivie pour avoir fourni des informations ayant mené à la condamnation d'un journaliste chinois qui purge maintenant une peine de 10 ans de pénitencier (39). La saisie du matériel informatique et 1 500 euros d'amende ont été requis devant le tribunal correctionnel d'Avignon contre un jeune homme qui avait piraté par « vengeance » le « blog » de son ex-petite amie (44). Un jeune internaute de 25 ans est accusé de s'être introduit illégalement dans le système informatique de l'université de Californie du Sud (USC), et d'avoir récupéré des données personnelles sur les étudiants. Il risque 10 ans de prison (58). Un Californien de vingt ans condamné à 57 mois de prison ferme, suivis de trois ans de liberté surveillée pour avoir monté, loué et exploité des botnets. Au total, plus de 400 000 PC « *zombies* » ont été contrôlés par ce *botmaster* (65).

Evénements en matière de cybercriminalité :

Le président égyptien Hosni Moubarak s'entretient, en février 2006, avec le directeur du FBI, Robert Mueller, de la coopération contre le terrorisme, dans le domaine pénal. La cybercriminalité tout comme le terrorisme et la drogue sont considérés comme de « grands dangers » qu'il faut combattre en commun (14).

Une conférence régionale de deux jours sur la lutte contre la cybercriminalité se tient à Beyrouth. Les débats portent sur les moyens technologiques de répression du cybercrime, le rôle de la société civile dans la consécration de l'éthique sur le net et les effets de la cybercriminalité sur le secteur des affaires (18).

A l'occasion d'un dîner – débat du *Cercle Européen de la Sécurité et des Systèmes d'Information*, DG Consultants rassemble plus de 130 DSI (Directeurs des Systèmes d'Information), experts et partenaires. C'est le rendez-vous incontournable des professionnels de la sécurité informatique. Le thème de cette réunion porte sur la cybercriminalité et plus particulièrement sur trois aspects : l'état de la législation en cours, les méthodes d'intervention des autorités et les profils des cybercriminels (30).

La deuxième semaine nationale de la sécurité informatique - qui s'est tenue à la Sorbonne - s'inscrit dans le cadre du projet Confiance, programme de sensibilisation aux risques d'Internet, lui-même soutenu par la Commission européenne (66)

Etudes et enquêtes menées dans le domaine de la cybercriminalité :

Une enquête menée par le cabinet *Braun Research* pour le compte d'*IBM* indique que plus de 60 % des 2400 DSI ou responsables informatiques interrogés dans 16 pays différents estiment que le coût du cybercrime est désormais supérieur aux malversations du monde réel (2). Les DSI, quelle que soit leur origine, partagent les mêmes préoccupations : les coûts résultants d'attaques sur le Web. La perte de revenus est le risque cité en premier. Cette enquête a été conduite au sein des pays de la zone *BRIC*, des pays européens, d'Amérique latine, au Canada, en Australie et au Japon. Elle met en lumière des différences sensibles en fonction des pays. Ainsi, les DSI américains semblent beaucoup plus confiants vis-à-vis des systèmes de protection qu'ils ont mis en place que leurs homologues dans les autres pays. En revanche, les conséquences sur

l'image et la réputation de leur entreprise sont considérées davantage par les DSI non américains. Les coûts juridiques afférents au cybercrime constituent une préoccupation beaucoup plus importante aux Etats-Unis.

Les dernières études américaines sur la cybercriminalité révèlent que le *spam* est désormais ancré dans le quotidien des utilisateurs d'Internet (10). Selon « *Security Decision Makers* », les entreprises craignent d'abord et à 40 % les *spywares*, ensuite à 29 % les infections de vers, puis à 24 % les attaques par déni de service. Une enquête de la société *Top Layer Networks* démontre que 60 % des responsables d'entreprise ayant répondu ont augmenté en 2005, leurs dépenses pour la sécurisation de leurs systèmes d'information. En 2006, ce qui les incite à investir dans la sécurité des systèmes c'est la protection des données (66 %), la fiabilité du système (63 %) et les performances (40 %).

Une étude du groupe *Lexsi* sur les réseaux de cybercriminalité montre que plusieurs types de menaces sont en recrudescence dont la contrefaçon, l'espionnage économique, ainsi que les vols et pertes de données. Cette situation est la conséquence d'un changement radical des motivations des cyberdélinquants ; alors qu'auparavant ils cherchaient la gloire personnelle, ils sont aujourd'hui motivés par l'appât du gain. Le phénomène s'internationalise et fonctionne par réseaux, grâce à un ensemble de personnes en liaison permanente *via* des canaux d'informations officieux. Le cybercrime à l'image de la mondialisation, ne connaît pas de frontières et n'épargne ni les individus ni les entreprises (22).

Le CLUSIF publie une étude sur les virus informatiques qui propose une typologie des infections et des anti-virus ainsi que le point sur l'étendue de la menace et des parades qui peuvent y répondre. Trois aspects du phénomène sont abordés : l'organisation de la lutte anti-virale, l'aspect juridique et l'assurance contre les virus (31).

Selon une étude des principaux éditeurs de logiciels, la France fait figure de mauvais élève, avec près d'un logiciel sur deux (47 %) piraté sur les ordinateurs personnels. Le piratage français a généré des pertes de 3,2 milliards de dollars. C'est aux Etats-Unis qu'on pirate le moins (21 %), mais pour un montant de 6,9 milliards de dollars qui est le plus important dans le monde. La Chine arrive au deuxième rang avec un manque à gagner de 3,9 milliards de dollars (69). Chaque semaine, *Panda Software* publie un rapport résumant les événements les plus marquants dans le secteur des

intrusions et des virus informatiques. En l'occurrence, le rapport examine un code malveillant qui peut infecter tout autant les plateformes Linux que Windows, ainsi que les vulnérabilités corrigées par *Microsoft* dans ses derniers bulletins de sécurité (55).

Websense (spécialiste de la sécurité web et des logiciels de filtrage web) a réalisé une enquête internationale (110 participants de 20 pays). Selon les résultats, 45 % des experts en cybercriminalité affirment que la plus grave menace à laquelle sont exposées les données d'une organisation vient de l'intérieur de l'entreprise. Seulement 11 % des personnes interrogées pensent que les menaces extérieures (cybercriminalité organisée, pirates) posent un problème plus grave, tandis que 44 % estiment que les risques sont autant internes qu'externes (59).

Cadre juridique national et international :

L'Algérie n'enregistre pas un fort taux de cybercriminalité, mais il n'en demeure pas moins que les pouvoirs publics doivent s'en prémunir et être prêts pour une éventuelle coopération internationale en la matière. Un groupe de travail chargé d'élaborer des textes de loi pour lutter contre la cybercriminalité a donc été mis en place (19).

En France, la Commission des Lois de l'Assemblée nationale a adopté des amendements modifiant le projet de loi controversé DADVSI (Droit d'auteur et droits voisins dans la société de l'information). Jusqu'à présent, les internautes qui téléchargeaient illégalement des œuvres protégées s'exposaient à la prison. Désormais, ils ne devraient plus être sanctionnés que par des contraventions de 38 à 150 Euros.

Après la loi française DADVSI, l'Allemagne vote aussi une loi pour réguler le téléchargement pirate sur la toile. Le texte est l'un des plus durs en Europe (29).

En Europe, la guerre au téléchargement gratuit est déclarée. Avec des peines de prison ferme, l'Allemagne montre l'exemple. La loi française DADVSI déjà adoptée par l'Assemblée nationale soulève une autre question : l'obligation d'interopérabilité qui semble séduire le Danemark (32).

L'Algérie prépare une loi contre la cybercriminalité. Le pays met l'accent sur l'importance de la coopération internationale en matière de lutte contre le cybercrime.

L'Algérie avait déjà signé, en 2003, un accord de coopération avec la France pour lutter contre la criminalité organisée, particulièrement la cybercriminalité (35).

Des experts internationaux plaident pour une loi spécifique sur la cybercriminalité en Algérie. La nécessité d'une coordination internationale en matière de lutte contre la cybercriminalité est mise en avant (40).

Des tendances en cybercriminalité :

La cybercriminalité devient de mieux en mieux organisée. A l'occasion des *Assises régionales à Villeneuve-d'Ascq,* les entreprises ont été alertées des risques encourus de plus en plus importants. Lille accueillera en mars 2007, un colloque international sur la cybercriminalité afin de favoriser l' « amorce d'une coopération mondiale » (68). Les parents ont du mal à assurer un contrôle efficace sur les activités informatiques de leurs enfants. Face à une multitude de dangers existants, les solutions sont trop complexes à mettre en œuvre (34).

Divers :

Dès les années 80, on se rend compte que le cyberespace présente de nombreuses zones frontières où gravitent des bandits de type différent. Le *cyberpunk* est considéré comme une contre-culture des années 90 aux USA (21). C'est une vague de lutte contre le système en place. Les adeptes de cette nouvelle contre-culture voient la technologie comme une arme de choix. Ils se tiennent à l'écart de l'activisme politique, de la désobéissance civile et des marches de protestation. Leur slogan est « *l'information doit être libre* » et ils font référence à tout type d'information. Selon les pirates informatiques des années 90, les ordinateurs contrôlent trop d'aspects de nos vies. Infecter un ordinateur gouvernemental avec un virus n'est donc pas juste un divertissement. C'est du terrorisme politique. L'*underground* informatique fonctionne comme une « confédération libre d'organisations criminelles ». Aucune forme de solidarité ou de coopération n'y a été identifiée. Il n'y aurait aucune finalité commune pour le mouvement. Les *cyberpunks* sont connus pour s'espionner les uns les autres et pour s'opposer les uns aux autres. La plupart d'entre eux sont des solitaires. Peut-on parler d'une cyberpolitique ? Le système

de valeurs de base des *cyberpunks* est le libertarisme. L'intimité (*privacy*) est une question importante. Cette culture est nourrie par des tendances comme la théorie du chaos, le postmodernisme, le dadaïsme, le situationnisme. Le « noble » objectif des *hackers* consiste à rendre la technologie accessible à tous et à décentraliser l'information. On fait la distinction entre le *hacker* (ouvert, conscient, honnête, constructif) et le *cracker* (méchant, dangereux, destructeur). Les *cyberpunks* peuvent représenter un danger non seulement pour les pouvoirs constitués mais aussi pour la société au sens large, car ils possèdent le potentiel pour la changer.

A l'« affaire *Clearstream* », organisme financier luxembourgeois, s'est greffée une affaire de dénonciation anonyme, un corbeau lisant les comptes bancaires dont bénéficieraient des personnalités françaises. Ainsi, le domicile de Philippe Rondot, ancien de la DST et de la DGSE, a-t-il été perquisitionné (33).

(Rappel : les références des documents étudiés sont disponibles en annexe 10).

2) Veille médiatique – Presse écrite :

En rappel à l'historique établi en première partie, nous proposons de détailler un *focus* sur la presse française de 1995 à nos jours traitant du phénomène de la cybercriminalité[159] (Echantillon utilisé pour notre étude presse écrite & cybercriminalité (Cf. liste des articles en annexe 9)) :

Construction du Corpus :

Le cybercrime est un phénomène croissant fort médiatisé. Les informations provenant des divers médias, Internet par exemple, ayant traité ou traitant de ce phénomène constituent un ensemble de documents trop vaste pour être traité de manière correcte et exhaustive. Nous avons souhaité rendre compte de ce qui a été diffusé par la presse quant à notre étude, ce qu'elle en a dit, en effet, quel type d'informations diffuse-t-elle à ce sujet, et non comment elle l'a diffusé ; nous ne ferons pas d'analyse sémiologique, car ce n'est pas le sens de notre étude. Nous considèrerons la presse écrite

[159] *La cyberdélinquance, un risque pour Internet ?* (Humbert, 2003).

uniquement comme une source d'information ; elle conserve une place déterminante dans le système médiatique. Nous avons choisi de rendre compte de manière synthétique de cette transcription d'informations à destination du grand public, à partir d'articles que nous avons stockés de manière empirique dans un cadre professionnel. Nous avons réuni les articles de la presse française, collectés, depuis fin 1994 à nos jours, en relation avec notre étude, et avons retenu, après un tri sélectif, un échantillonnage d'articles traitant principalement de la cyberdélinquance sur Internet. Nous disposons d'environ cinq-cent documents en relation avec le sujet, en tant qu'archives privées, et avons souhaité le mettre à profit au cœur de notre recherche. Le choix et la sélection parmi ces écrits fait office d'enquête générale (relativement stable) de l'existant du phénomène cyberdélinquance sur Internet. Nous procèderons à la synthèse de ces informations divulguées par la presse sur ce sujet. Notre but est de tirer les informations essentielles véhiculées de 1995 à 2003. Vingt-huit articles constituent ce corpus, dix-sept éditions sont représentées.

De fait, nous considèrerons comme exhaustive l'information extraite, car croisée sur un période conséquente de huit ans et à travers un large spectre d'éditions de nature diverse. L'étude de ces articles ne nous permettra pas de vérifier la réalité des faits évoqués quant à la cyberdélinquance ; cependant, nous pouvons conclure à une forte médiatisation de l'existence du phénomène qui s'est amplifié et généralisé sur la période étudiée, corrélativement à la croissance d'Internet. Récemment une presse spécialisée, traitant exclusivement de cyberdélinquance, a vu le jour ; elle tend même à se développer rapidement. Nous pouvons donc mettre en lumière, à travers cette revue de presse, la corrélation entre le développement d'Internet et la croissance du traitement médiatique de la cyberdélinquance. Concrètement, corrélativement à l'essor du médium, la source d'information du corpus presse montre qu'Internet, donne matière à l'envolée de la cyberdélinquance. Les faits, tels que présentés par la presse écrite française de 1995 à nos jours, traduisent l'éclairage de la Sociologie juridique, validant l'approche de J. Carbonnier : l'évolution des mœurs et des techniques donne, effectivement, matière à de nouvelles formes de délinquances (cf. *infra*).

Le « terrain de jeu » Internet est devenu la matière première de la cyberdélinquance. Cette source d'information rend bien compte de l'évolution d'un

nouveau type de délinquance appliquée à Internet. Nous garderons une distance critique quant à la pertinence des informations véhiculées. Cependant, l'étude, telle que nous l'avons constituée, au fil des évènements relatés, provenant de sources diverses, nous permet de valider globalement les faits traités (nous avons traité de 1994 à 2001, soit sur le plan judiciaire, soit sur le plan administratif, environ 300 enquêtes de terrain, et la plupart des piratages et faits relatés par la presse écrite française). Cependant, nous sommes tenus à un devoir de réserve et de confidentialité quant à ces affaires traitées et notre démarche de recherche nous impose aussi un devoir d'objectivité. Cela nous permet globalement de retenir ce corpus comme source d'informations pertinentes.

Un lien de corrélation transparaît donc entre le développement du médium Internet et le développement d'une nouvelle délinquance appliquée spécifiquement à la société de l'information. Plus qu'une instabilité du système Internet, cette délinquance est présentée, à travers la presse, comme une perte de crédibilité pour ce médium alors que l'intérêt et le besoin de la sphère de communication universelle Internet est entendue. La presse relaie, en effet, la cyberdélinquance en tant que risque véritable pour Internet, à travers les actes illicites d'acteurs spécifiques dénommés *hackers*, *crackers* ou pirates informatiques, sans distinction véritable.

La presse écrite française, sur la période choisie, constitue en la matière un vecteur exhaustif et synthétique des faits importants et marquants. Nous procèderons à la synthèse de ces informations et communications divulguées par la presse sur ce sujet. Notre but est de tirer les informations essentielles véhiculées de 1995 à 2003 (Nous avons, à partir de 2003, stoppé l'indexation de ce type d'articles de presse, relatif à la cybercriminalité, pour nous consacrer plus spécifiquement au champ de la sécurité de l'information, au niveau professionnel. Les derniers développements ont tout de même été suivis, notamment *via* l'analyse médiatique par Internet (Cf. analyse « *Google Search* » *supra*)). Vingt-huit articles ont été sélectionnés, dix-sept éditions sont représentées : *Courrier International, Joystick, Le Monde, Le Monde Diplomatique, L'Ordinateur individuel, Libération, La Tribune DESFOSSES, L'Evénement du Jeudi, Le Figaro, Le Quotidien de Paris, Net@scope, Hackmania, Le manuel de Hackers Voice, Hackerz Voice, Pirat'z, Science et Vie, et Zataz Magazine*.

- Analyse du corpus de presse sur la cybercriminalité recueilli durant la période 1995-2002

Nous proposons une analyse des discours médiatiques dans le domaine de la cybercriminalité, à partir des articles recueillis, précédemment décrits. Le corpus est constitué de 28 références dont 18 titres parus dans la presse généraliste et 10 dans la presse spécialisée. Les articles se distribuent comme suit :

- Tableau 16. Répartition des articles de presse portant sur le domaine de la cybercriminalité

Année de parution	Nombre de références	Nombre de références presse généraliste	Nombre de références presse spécialisée
1995	7	6	1
1996	2	2	0
1998	6	5	1
1999	3	2	1
2000	2	1	1
2001	4	2	2
2002	4	0	4
Total références	28	18	10

Le tableau ci-dessus permet de constater une prédominance en nombre des articles parus dans la presse généraliste (18 contre 10 références de la presse spécialisée), pour toute la période 1995-2002. Nous notons la tendance suivante : entre 1995 et 2000, les articles publiés dans la presse généraliste sont plus nombreux que ceux parus dans la presse spécialisée (16 contre 4). En revanche, pour la seule période 2001-2002, la tendance est inversée au profit des articles publiés dans la presse spécialisée (6 contre 1) ;

si bien qu'en 2002, tous les articles portant sur la cybercriminalité – au nombre de quatre - ont été publiés dans la presse spécialisée et aucun dans la presse généraliste.

Ces statistiques sont intéressantes dans la mesure où les discours médiatiques possèdent une force structurante avérée. Ainsi, les publications dans la presse généraliste seraient destinées à un public très vaste, tandis que les textes de la presse spécialisée concerneraient plutôt un public initié. Cette étude est sans doute incomplète, d'autres textes ayant pu paraître dans la presse nationale pendant la même période. Toutefois, l'échantillon analysé permet de dégager quelques grandes tendances concernant notamment les thèmes traités et le vocabulaire utilisé par les journalistes. En effet, nous nous proposons de réfléchir sur les questions suivantes : Quels sont les thèmes liés à la cybercriminalité traités par les journalistes de façon prioritaire? Quel message les journalistes veulent-ils transmettre aux lecteurs ? Quelle image des cybercriminels les médias construisent-ils ?

Nous proposons une grille de lecture thématique et chronologique à la fois. Les textes sont classés par année de parution et les tendances dans l'information sur la cybercriminalité sont enregistrées pour chaque année. Cette approche permet de voir l'évolution des thèmes et du vocabulaire journalistique à travers les années.

Sont analysés les supports suivants :

1) pour la presse généraliste – *Le Monde, Le Monde diplomatique, Libération (Cahier multimédia), Le Figaro, La Tribune Desfossés, L'Evénement du Jeudi, Le Quotidien de Paris, Le Courrier international, Sciences et vie* ,

2) pour la presse spécialisée – *Hackerz Voice, Le manuel de Hackerz Voice, Hackmania, Pirat'z, L'Ordinateur individuel, Joystick, Net@scope.*

Année 1995 (7 articles dont 6 dans la presse généraliste et 1 dans la presse spécialisée)

Les thèmes traités dans la presse généraliste : la sécurité des systèmes informatiques est mise en avant. Etant donnée la montée des risques liés à l'utilisation des réseaux numériques, il s'agit d'une véritable prise de conscience : nul ordinateur n'est inviolable, tout le monde est exposé au risque des attaques. Ainsi émerge une idée développée dans la presse qui consiste à créer des systèmes ultra protégés, mais on serait alors en présence d'un monde informatique à deux vitesses : les ordinateurs personnels et ceux des entreprises resteraient transparents alors que les machines de l'Etat deviendraient de véritables coffres-forts. Il est question également de l'apparition des organes répressifs en matière de fraude informatique en France. Le public est informé des causes des fraudes, du dispositif juridique et de la panoplie des assureurs. Il est recommandé de faire preuve de bon sens face à la menace. Cette même année, les lecteurs sont également mis au courant de l'existence d'un véritable *lobby* des *hackers* aux Etats Unis qui prône la liberté sur les réseaux informatiques. On définit – à travers une approche sociologique et idéologique - les différentes castes de *hackers*, *cyberpunks*, etc. Les qualificatifs et les termes utilisés par rapport aux *hackers* sont : *libertaires, mi-requins mi-entrepreneurs, communauté virtuelle, attachés à une liberté d'expression totale, hostiles à la propriété intellectuelle des œuvres* (« L'Odyssée des pirates dans la jungle d'Internet », *Le Monde diplomatique*, juin 1995). Dans la presse généraliste (*Le Monde*), on annonce parfois des faits graves qui ont eu lieu : le site Internet de l'école polytechnique qui dépend du Ministère de la défense a été fermé à la suite d'intrusions. Le même quotidien national aborde le sujet du *« jeu dangereux du piratage informatique »* en proposant un historique du projet de réseau informatique mondial et mettant l'accent sur le lien existant entre débit et sécurité. Le piratage informatique distingue mal la délinquance, du « sport » (au sens de l'activité ludique).

Les thèmes traités dans la presse spécialisée : le piratage informatique serait une affaire de « passionnés » le but étant de trouver la faille. On fait la différence entre les « *hackers* » qui explorent les systèmes par soif de connaissances, et les « *crackers* » qui eux cherchent à pénétrer le système avec l'objectif de nuire. Il est cependant impossible

de départager l' « espion » du « passionné ». Des techniques utilisées par les pirates sont décrites. La question des organes répressifs en France et leurs compétences en la matière est également abordée. Les journalistes français sont fascinés par la situation aux Etats-Unis : *« …terreur des services secrets, les hackers sont invités à la conférence OSS à Washington qui réunit responsables de l'armée, de l'espionnage et industriels américains … »*. Les pirates sont considérés comme *« l'une des richesses nationales »* de l'Amérique (*Joystick* 34-40, du 9 décembre 1995).

Année 1996 (2 articles dans la presse généraliste)

Les thèmes traités dans la presse généraliste : Internet est décrit comme « *le théâtre d'un jeu de cache-cache* » entre les pirates informatiques et les services de renseignement. Dans la presse, on se pose des questions : Les pirates informatiques peuvent-ils agir à leur guise au nom de la liberté sur le net ou doivent-ils être utilisés comme des vigies dans le cyberespace pour le compte d'intérêts nationaux ? On fait toujours la différence entre les « gentils » *hackers* qui utilisent l'ordinateur pour visiter ce qu'il y a dedans sans autorisation, pour le plaisir, et les *crackers* « noirs » dont l'objectif est de causer des dégâts. Le monde des *hackers* est celui de la culture « *underground* » ou « anti-culture ». Dans la presse française, on propose le point de vue stratégique d'experts américains (Robert Steel, président de l'agence américaine *OSS* cité dans *La tribune Desfossés*, le 21 février 1996) *: « …la guerre de l'information est une guerre totale qui exige une intégration complète de tout le capital national de l'information »*. Trois idées phares sont mises en avant : le cyberespace est une nouvelle frontière où les lois nationales et internationales ne s'appliquent pas ; il faut établir les standards d'un comportement approprié au cyberespace ; les « terroristes de l'information » et les criminels doivent être physiquement appréhendés et condamnés de la même façon que tout criminel dans n'importe quel pays.

Les thèmes traités dans la presse spécialisée : aucun article n'a été recensé pour l'année 1996.

Année 1998 (6 articles dont 5 dans la presse généraliste et 1a dans la presse spécialisée)

Les thèmes traités dans la presse généraliste : des affaires sont médiatisées : des pirates français ayant visité le réseau de l'*US Air Force* sont poursuivis par les Etats-Unis ; un jeune Israélien a visité les ordinateurs du Pentagone. En Israël, ce pirate connu sous le pseudonyme « *Analyser* » est promu « techno héros ». Le pays se prend de sympathie pour « ce gamin », ce « génie séduisant qui n'a rien volé ni abîmé », symbole d'une « compétence toute neuve dans les domaines de pointe » ; « sans intention de nuire, par seul goût du challenge ». On voit là la construction d'une image très positive qui rejoint en tous points celle que nous renvoie la presse nationale par rapport à un jeune *hacker* français ayant visité le réseau des forces aériennes des USA (*Le Figaro* du 30 avril 1998). On parle du « profil type du jeune pirate », passionné d'informatique, poursuivant des études spécialisées auxquelles il renonce parce que « le niveau est trop bas ». Il force les sécurités des serveurs par « goût de la performance ». Néanmoins, à côté de cette image certes anecdotique mais plutôt agréable des jeunes *hackers*, la presse nationale n'omet pas de parler des « menaces de la cybercriminalité » (*Le Figaro*) et d'enquêter sur la lutte contre la délinquance informatique sur le plan international. Il est également question de cryptologie. On rencontre de nouveau la dichotomie bien connue proposée cette fois par *Sciences & Vie* : *hackers* (« justiciers qui veulent purifier Internet ») à l'opposée de *crackers* (« mercenaires »). On fait état des motivations d'ordre pécuniaire, politique ou même militaire des pirates, et des techniques de piratage.

Les thèmes traités dans la presse spécialisée : définition du terme « *hacker* » (« bidouilleur » dont les activités sont illégales mais dont « l'état d'esprit n'est pas malsain »).

Année 1999 (3 articles dont 2 dans la presse généraliste et 1a dans la presse spécialisée)

Les thèmes traités dans la presse généraliste : l'information est au cœur des conflits modernes ; sur le plan stratégique, il s'opère un changement d'époque. « *Penser*

la cyberguerre » titre le *Monde diplomatique* ; il propose toute une série de concepts en la matière, inventés par des auteurs américains : « cyberguerre », « politique de la connaissance », etc. Les profondes transformations de la société bouleversent la façon de faire la guerre. L' « intangible » caractérise le temps présent. Une autre conception de la puissance, et donc de la guerre s'impose. Le pouvoir est désormais affaire de relations entre les gens. Il devient immatériel… l'information devient une des dimensions de la stratégie. Elle peut être employée au lieu des armées et des sanctions économiques. Protection des achats, lutte contre la cybercriminalité : le 26 août 1999, Lionel Jospin annonce la deuxième grande étape de son « programme d'entrée de la France dans la société de l'information ». La France est le seul pays au monde à proposer une loi globale sur la société de l'information.

Les thèmes traités dans la presse spécialisée : un nouveau métier émerge outre atlantique – cyberdétective. En France, cette profession n'existe pas encore, mais des agences spécialisées se consacrent à la veille technologique au profit d'autres entreprises. En France, la CNIL (Commission Nationale de l'Informatique et des Libertés) veille sur les réseaux d'autant que l'utilisation des données nominatives est soumise à des lois ce qui n'est pas le cas aux Etats-Unis.

Année 2000 (2 articles dont 1 dans la presse généraliste et 1a dans la presse spécialisée)

Les thèmes traités dans la presse généraliste : les contestataires de la mondialisation sont rejoints par des pirates informatiques qui mettent à profit leur savoir-faire pour s'en prendre aux symboles de l'ordre établi. Il s'agit des « *hacktivistes* » (néologisme) ou cybermilitants et cyberrésistants qui mobilisent leurs connaissances informatiques contre la mondialisation, les multinationales et en faveur de la défense des internautes. Le Courrier international dans un dossier spécial « Internet contre l'ordre établi » invite à réfléchir de manière approfondie sur ce nouveau phénomène. Un glossaire est proposé : « *hacker* », « *hacktiviste* », « *cracker* », … Internet est le rêve des activistes ; les réseaux protestataires se mondialisent à la même vitesse que les grands groupes qu'ils dénoncent. Mais, ce qui manque c'est le pouvoir de cohésion des

communautés « réelles ». Les *hackers* sont très attirés par la politique, mais il leur reste à trouver les bonnes méthodes pour réussir. En matière de cyberrésistance se pose la question de l'espace physique. Le vocabulaire des journalistes s'enrichit par rapport aux années précédentes. Les thèmes se diversifient. De nouvelles nuances sémantiques et thématiques apparaissent qui correspondent au développement de nouveaux phénomènes socio politiques et économiques.

Les thèmes traités dans la presse spécialisée : pas de définition précise du concept cybercrime, mais il s'agit plutôt de crime étant en rapport avec une intrusion sur le réseau. De nombreux crimes traditionnels sont en partie perpétrés par voie informatique et sur Internet, mais on enquête de la façon traditionnelle.

Le projet de Convention sur la cybercriminalité du Conseil de l'Europe, un dispositif légal qui prévoit des mesures radicales, préoccupe les journalistes spécialisés.

Année 2001 (4 articles dont 2 dans la presse généraliste et 2 dans la presse spécialisée)

Les thèmes traités dans la presse généraliste : le Monde diplomatique titre « *Nous sommes tous des cybercriminels* ». L'auteur du texte, un haut fonctionnaire international, s'insurge face au projet de convention sur le cybercrime du Conseil de l'Europe. Cette convention serait le *« premier instrument juridique multilatéral à traiter des problèmes liés aux activités criminelles sur les réseaux globaux de communication »*. Mais, en même temps, ce texte serait inquiétant à plusieurs titres : il donnerait accès aux données personnelles ; le Conseil de l'Europe est accusé de servir les intérêts spéciaux de certains éditeurs et groupes de communication, et de rester fermé aux intérêts des pays en développement.

Les thèmes traités dans la presse spécialisée : le piratage est interdit, mais la solution légale est proposée par les « challenges » et les « *wargames* ». L'organisation « *2600 France* » est un groupement non officiel *underground* qui n'a pas de chef ni de groupe dirigeant attitré ; le but des réunions mensuelles est de partager des connaissances, de rechercher et de solutionner des failles de sécurité.

Année 2002 (4 articles dans la presse spécialisée)

Les thèmes traités dans la presse généraliste : aucun article n'a été recensé pour l'année 2002.

Les thèmes traités dans la presse spécialisée : un portrait du « *hacker* » est dressé. Les avis sont controversés sur les *hackers* : s'agit-il de personnes dangereuses et nuisibles ou bien d'un modèle à suivre ? Même si la définition du terme « *hacker* » est très succincte, un développement est proposé concernant l'idée d'une culture, de l'attitude, et de la motivation des *hackers*. Ce serait finalement des personnes « anti-autoritaristes » dont l'objectif est de combattre la censure, le secret et l'usage de force ou de la ruse pour dominer. Les *hackers* résolvent des problèmes, construisent et croient en la liberté et l'entraide volontaire. C'est encore une image très positive et idéaliste des pirates informatiques construite par les journalistes spécialisés. Elle est renforcée par l'histoire particulière d'un « *hacker* brillant » qui a infiltré Matignon …et qui attend son jugement. *Alone Trio* - c'est son pseudonyme - est présenté comme quelqu'un d'honnête, de bienveillant et de sérieux. L'appel est lancé par la presse : « *hacker* brillant cherche emploi stable ». Mais la question fondamentale est toute autre ; en effet, est-ce là un crime que de signaler aux responsables système les failles du serveur ministériel pour qu'ils réagissent ? La loi française répond par l'affirmative. Décidément, le terme « *hacker* » est très controversé. Pour les « puristes » c'est un passionné spécialiste des ordinateurs, des réseaux, de la programmation. Pour l'opinion publique formée par le discours des médias, un *hacker* est forcément un pirate informatique. Pour les journalistes spécialisés qui proposent des publications sur le sujet, le véritable *hacker* est une personne très compétente en informatique et en programmation, passionnée de sécurité informatique et qui aime à chercher comment on peut la contourner. Les premiers *hackers* - puristes ou pionniers – prônent la libre diffusion de l'information, le logiciel libre. L'information est si fondamentalement libre qu'il est du droit de chacun d'y accéder. S'introduire dans un serveur protégé est donc pour eux un acte légitime. Ce principe va de pair avec l'idée de la liberté universelle de l'information. Un pur *hacker* ne commet aucune action malveillante.

Bilan de l'analyse du corpus de presse

Entre 1995 et 2002, on relève deux grandes tendances dans les discours médiatiques sur la cybercriminalité. D'une part, il y a cette vocation de la presse d'informer et cette volonté d'instruire au sujet d'un phénomène nouveau que les journalistes découvrent en même temps que le public. En effet, au début de la période étudiée, il est question de prendre conscience face à la menace et de se doter de systèmes d'information sécurisés. On fait état d'une situation nouvelle engendrant la mise en place progressive d'organes répressifs spécialisés. On identifie les acteurs principaux de cette pièce de théâtre à l'échelle internationale dont le dispositif scénique n'est autre qu'Internet. Au fur et à mesure, des affaires sont médiatisées. La presse française rapporte l'expérience américaine en matière de cybercrime. Peu à peu, dans la presse généraliste des articles engagés commencent à être publiés. On voit apparaître des analyses stratégiques sur la nature des conflits modernes. On émet des opinions concernant le futur cadre juridique multilatéral proposé par le Conseil de l'Europe pour traiter les problèmes liés aux activités criminelles sur les réseaux globaux de communication. Le vocabulaire des journalistes s'enrichit. Les thèmes se diversifient.

De nouvelles nuances sémantiques et thématiques apparaissent qui correspondent au développement de nouveaux phénomènes socio politiques et économiques liés à la cybercriminalité (« *hacktivistes* » et « cyberrésistance »). Cette tendance à la diversification des sujets est très marquée surtout au niveau de la presse généraliste qui aborde des thèmes variés et privilégie les commentaires et les analyses. En ce qui concerne la presse spécialisée, elle s'en tient plutôt aux aspects techniques et pratiques de la question tout en essayant de fournir une définition du phénomène cybercrime et de ses acteurs principaux. La deuxième grande tendance dans les discours médiatiques est l'approfondissement de la connaissance sur le sujet à travers une réflexion sur le profil type du « *hacker* », et de la philosophie et de la culture « *underground* ». Tous les journalistes, quel que soit leur médium de rattachement, s'y intéressent. On fait la différence entre les « gentils *hackers* » et les « *crackers* noirs». L'image des « *hackers* » est mise en valeur : ce sont des passionnés qui aiment les défis et maîtrisent à la perfection les moindres détails des systèmes d'information. Leur activité est certes

illégale, mais ils respectent une certaine éthique. On reconnaît qu'ils ont des mérites et on ne cherche pas à les discréditer.

Au final, nous constatons une contradiction au sein du discours journalistique qui doit sans doute refléter la nature d'un phénomène complexe, dangereux et fascinant à la fois. En effet, à côté des appels alarmistes mettant l'accent sur la menace et l'ampleur que prend la fraude informatique ces dernières années, on voit se construire une image des « *hackers* » plutôt agréable et débarrassée de connotations négatives. Ainsi, il appert spécifiquement que cette représentation médiatique est parallèle aux significations sociales relevées par notre sondage (Cf deuxième partie - I - 2), révélant la conscience de l'illégalité du cybercrime, mais tout en affichant une « espèce de sympathie » paradoxale pour ses auteurs, allant jusqu'à prôner des actions judiciaires faibles, à l'inverse de ce qui est appliqué en matière de répression actuellement.

Pour terminer cette analyse des représentations médiatiques, nous proposons de rendre compte du monde journalistique en regard de notre objet de recherche.

3) Veille médiatique – Monde du journalisme :

Nous avons veillé, au cours de l'étude, à mener des échanges avec différents intervenants du milieu journalistique traitant du monde de la cybercriminalité. A ce titre, plusieurs retours permettent de relever des mécanismes de construction journalistique de la thématique cybercriminalité, souvent identiques. Ainsi, plusieurs entretiens ont eu lieu avec les co-fondateurs du portail francophone dédié au piratage informatique (ZATAZ[160]), par mail et en direct, notamment au Grand-Duché de Luxembourg, le responsable de ce serveur d'information francophone a permis, notamment, la mise en ligne dans le cadre de notre thèse libellée « *Monde de la Cyberdélinquance et images sociales du pirate informatique* »[161], d'un questionnaire de type sondage sur cette problématique, et récemment des résultats issus de ce dernier. Cette collaboration a pu

[160] http://www.zataz.com.
[161] http://jph.cases-cc.org.

montrer l'ouverture d'esprit journalistique vis-à-vis du phénomène que nous étudions, la clairvoyance, mais aussi la volonté de faciliter la recherche en cours sur le sujet. Les résultats de ce sondage ont été présentés lors d'une rencontre SPIRAL[162] le 26 septembre 2006 : « *S'il te plaît… dessine-moi un pirate informatique !* », dont le sujet était le suivant : « *Si vous deviez dessiner un pirate informatique, comment le représenteriez-vous ? Les caricatures, plus effrayantes les unes que les autres, ne manquent pas. Escroqueries, espionnage, spamming, abus de confiance... Les différentes formes de délinquance informatique sont devenues une réalité indéniable. Chiffres inquiétants et cas d'écoles médiatisés sont là pour l'attester. Mais qui est ce mystérieux pirate, caché dans les ténèbres de la grande toile ? Au cours de cette rencontre, les intervenants apporteront des éléments objectifs permettant de caractériser précisément les différents types de « hackers » et les menaces qu'ils représentent. On se placera également du point de vue des pirates et de leur culture, pour entrevoir des représentations différentes d'une même réalité... Parfois, le dessein n'est pas aussi sombre que l'image.* »

Le programme était le suivant :

- « *Les mondes de la cyberdélinquance et images sociales du pirate informatique* » par Jean-Philippe Humbert - Centre de Recherche Public Henri Tudor.

- « *What the hack ?* » - ? (Anonyme).

- « *Panorama cybercrime 2005 - CLUSIF* » par Danielle Kaminsky – CLUSIF.

- « *Observation des différentes attaques IT au Grand-Duché de Luxembourg* » par Alexandre Dulaunoy et Fred Arbogast – CSRRT.

- « *Prospective nationale de l'observation des menaces IT au G-D de Luxembourg* » par François Thill - Ministère de l'Economie et du Commerce Extérieur.

Cette conférence était couverte par deux journalistes : un du journal « *Le Jeudi* » et un du magazine « *Paper Jam* », chacun ayant produit un article à l'issue. La pratique de mettre les supports à disposition du public, mais aussi en ligne, n'a pas suffi aux journalistes. En effet, ces derniers nous ont directement contacté pour un entretien-interview téléphonique, aux fins de rédiger « correctement » leur article, le domaine du cybercrime étant difficile à traiter. De plus, une fois rédigés, les articles nous ont été

[162] Réseau des professionnels de l'IT au Grand-Duché de Luxembourg – http://www.spiral.lu.

soumis pour vérifier l'adéquation des propos avec le sujet traité et la véracité du rendu correct de la rencontre SPIRAL.

Les membres de ZATAZ ne sont pas en reste, puisqu'une fois la conférence terminée, ces-derniers ont annoncé sur leur site la tenue de cette conférence et la disponibilité des résultats du sondage d'origine dans le cadre de cette thèse, notamment sur le portail de la sécurité de l'information du Grand-Duché de Luxembourg (http://www.cases.public.lu). La pratique de relecture par expert lors de la construction d'un article dédié au cybercrime, semble être une bonne pratique ; en effet, cela avait déjà été le cas pour un article publié en 2004 par le journal *Luxemburg Gemengen*, et dédié aux acteurs de la cybercriminalité. La pratique consistait à nous interviewer, et ensuite à rédiger l'article, puis à nous le soumettre pour relecture et validation. Il appert, cependant que cette pratique n'est pas légion et que la plupart des journalistes ne font pas ainsi. Certains parce qu'ils disposent de connaissances et compétences suffisantes sur la problématique, surtout pour la presse spécialisée, d'autres parce qu'ils pensent en disposer. Ces derniers posent problème car ils ne tiennent pas forcément compte correctement des différentes catégories, culture, législation, tendances du phénomène et de l'importance du champ de la sécurité de l'information. Ils risquent ainsi de tenir un discours décalé par rapport à la réalité, et souvent empreint d'empathie, de surcroît s'ils souhaitent tenir un rôle d'«éducateur » sur cette thématique.

Nous avons, à ce titre, rencontré le responsable « *awareness raising* » (amélioration à la sensibilisation de la sécurité de l'information) de l'ENISA (Agence Européenne de la Sécurité de l'Information de l'Union Européenne[163]) qui nous a clairement indiqué, que cette agence allait mettre en place un programme de sensibilisation au domaine des menaces IT et de la sécurité de l'information à destination des journalistes au niveau européen, afin de tenir compte de toutes les subtilités du discours associé à la problématique cybercrime. Cela afin de faciliter la rédaction objective des articles de presse vis-à-vis du phénomène.

Enfin, nous avons pu rencontrer également Mme Danielle Kaminsky (journaliste indépendante, membre du CLUSIF) qui nous a confirmé le fait que le traitement de cette

[163] http://www.enisa.eu.int.

problématique est difficile pour le monde journalistique réagissant sur l'instant et aimant le sensationnel (En fait, le traitement du « temps qui passe »), ce qui peut parfois orienter le discours, sans l'objectiver. Ainsi, la communication médiatique pourrait ne pas tenir compte du contexte, en évitant toute vérification ou investigation, et par conséquent nuire au sujet de la cybercriminalité, et à ses acteurs. Il est évident que les journalistes tiennent peu souvent compte de la différence existante entre les « *hackers* » et les « *crackers* », ce qui, vis-à-vis de la communauté « *underground* », pose de grosses frustrations, engendrant souvent une « cassure » entre ces mondes. En effet, le pouvoir des journalistes est primordial, quant à la problématique des acteurs du cybercrime, vis-à-vis du citoyen. Ce dernier, ne rencontrant pas ce type de personnage en réel, s'en fera souvent une représentation à partir du vecteur médiatique. Ce que nous avons décrit précédemment, en constatant que l'image médiatique (prédominante) se superpose avec l'image sociale « devenant » dominante (par inspiration).

Nous avons également pris attache avec le responsable de la première revue spécialisée de sécurité informatique en France : MISC. Nous avons produit trois articles sur la période 2006-2007 pour ce magazine (voir annexe 13) et avons rencontré son responsable notamment au salon hack.lu (http://www.hack.lu - 19-21 octobre 2006), et durant la phase de relecture des articles scientifiques soumis pour ce colloque (dont nous étions relecteur). Proche du monde de la sécurité informatique, le responsable du magazine MISC, nous a plusieurs fois indiqué qu'il privilégie la sécurité informatique, les dossiers techniques et les aspects de vulnérabilités effectives pouvant atteindre un système ou réseau, pouvant être exploité par tout agent menaçant, qu'il teste, et qui nécessite donc réflexion en matière de sécurité informatique. Son engagement est relativement moins marqué pour le domaine large de la sécurité de l'information, trop vaste et trop organisationnel à son sens.

La construction des articles tient ainsi compte de cette importance (quelques articles traitent tout de même de sécurité de l'information de type organisationnel). Tout en respectant les aspects de respect des lois, il privilégie les aspects techniques de la sécurité avec en toile de fond de réflexion les principes d'un « *hacking* » qui fourni l'innovation et l'amélioration des systèmes et réseaux en terme de sécurité et fiabilité. Les articles sont proposés par les auteurs au responsable de la publication, qui le valide

ou non, puis l'article rédigé est soumis à relecture de deux pairs, tant sur le fond que sur la forme, puis enfin publié.

Les images du pirate informatique sont, *via* MISC, sous-jacentes, et rarement présentées ; elles se justifient *via* l'innovation et la pertinence des articles rédigés au cœur du magazine, très bien côté en Europe. Le responsable de MISC insiste sur le fait que l' « *underground* » n'existe pas et que seulement des passionnés des TIC existent. Parallèlement à cet état de fait, ce dernier indique que certains personnages dépassent les lois, et sont alors punissables. Il a précisé que MISC n'a jusqu'à présent édité qu'un seul article traitant du sujet, il a ajouté que pour qu'un nouvel article de ce type puisse « passer », il faudra qu'il soit de niveau élevé, explicitant notamment de la prise en compte de tous les points de vue du phénomène.

Note : autre aspect non négligeable, en lien avec le cadre de notre étude, *The HacAckhademy* (Paris), journalisme spécialisé dans le piratage informatique a récemment fermé, pour cause d'absence d'entrée d'argent. L'éditeur de *Hacker Voice-Hackademy* fut donc contraint de fermer. « *Il faut dire aussi que plusieurs pigistes, professionnels ou non, commençaient à montrer le bout de leurs avocats pour tenter de se faire payer des articles commandés et édités par le fondateur de DMP France (Publia, ...), Olivier Spinelli* »[164]. En fait, l'information est apparue au registre du commerce et des sociétés : la société éditrice d'origine, *DMP France*, est en liquidation judiciaire. La date de fin d'exercice comptable avait été changée en juin 2006. Un autre signe. Cette liquidation a été précédée de peu par celle d'une troisième société d'édition « cousine » *Publia* (*Pirat'z* et autres). Ce secteur presse a donc subi des « perturbations » récemment, notamment dans la presse spécialisée, ce qui préfigure d'une certaine vitalité, mais aussi d'un secteur en construction constante, évoluant aussi en fonction de l'évolution des images sociales attachées au pirate informatique. En effet, la représentation sociale « sédimentée » de la cyberdélinquance, par amélioration de la connaissance sociale globalisée du phénomène, peut aussi entraîner une baisse d'intérêt pour la thématique et la presse « hyper » spécialisée.

[164] http://www.zataz.com.

La compréhension de la véritable menace est primordiale, notamment de ses véritables protagonistes, qui n'engendrent pas les mêmes conséquences.

Il conviendrait que les médias puissent établir définitivement cette distinction lors d'articles traitant de cybercriminalité. La participation constructive des *hackers* pour Internet est largement relayée et expliquée ; de fait il semble évident que ces derniers sont des techniciens d'Internet ; leurs actes de progrès technique appliqués au médium s'opposent, logiquement, à ceux des pirates informatiques ou *crackers*. Nier cette dichotomie entre eux serait faire un amalgame réducteur. Les *hackers* peuvent alors être véritablement considérés comme des faciliteurs de la libre communication, n'appartenant pas au monde de la cybercriminalité, tandis que les pirates informatiques sont à l'origine des entraves informationnelles et communicationnelles volontaires du réseau de réseaux Internet. Globalement, certains médias devraient éviter cet amalgame réducteur entre les qualifications de ces protagonistes. « *Pourquoi les hackers sont-ils perçus comme des individus n'utilisant leurs connaissances que pour s'introduire illégalement dans les serveurs informatiques? La raison principale provient sûrement de l'image diffusée par les médias, particulièrement les journaux et la télévision alors que le cinéma glorifie bien souvent leurs activités »*[165].

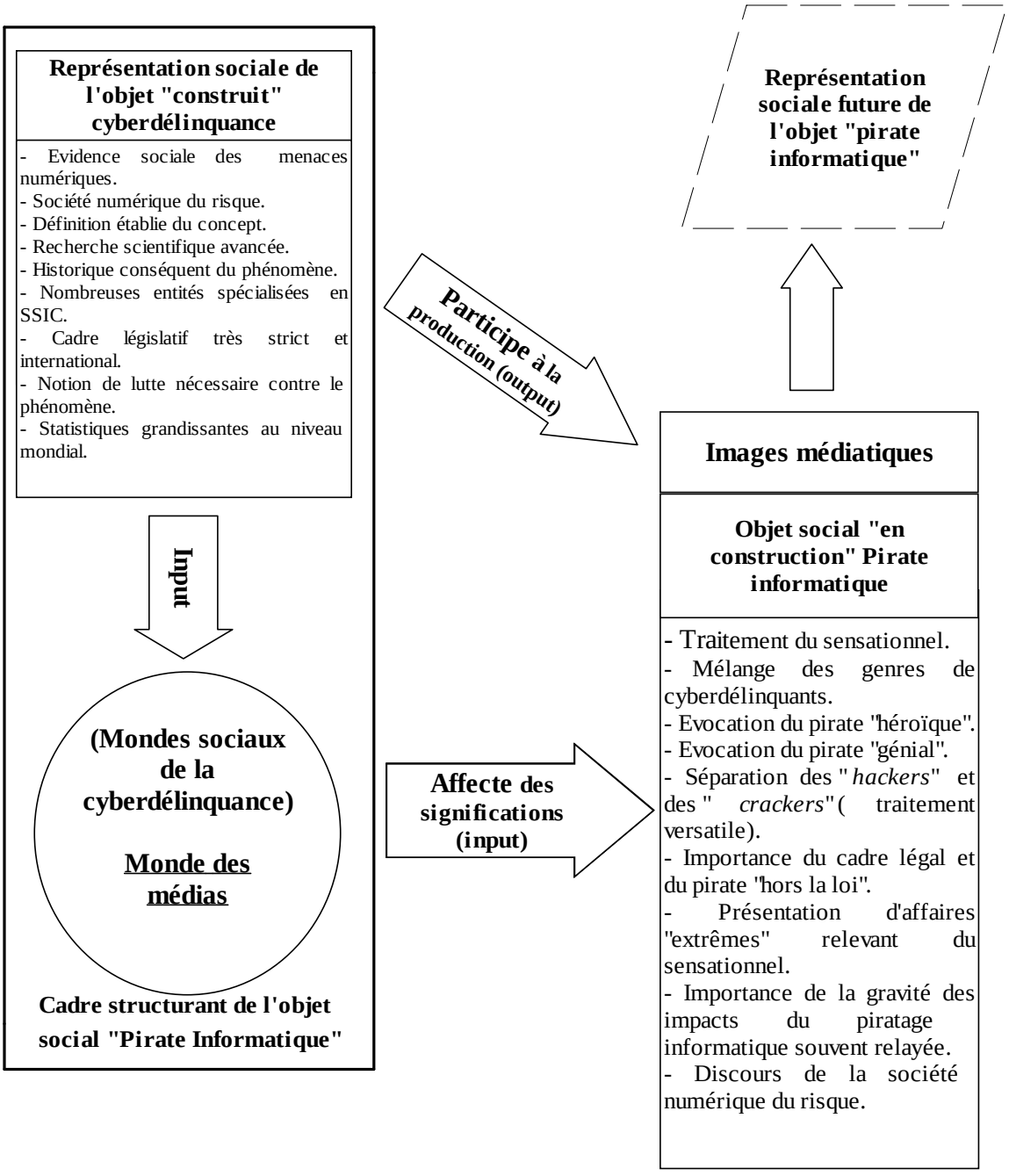
Au sein des TIC, les *hackers* revendiquent au plus haut point Internet en tant qu'espace de démocratie. « *Commençons par dire clairement ce qu'est la culture hacker, puisque l'ambiguïté du terme est source de malentendu. Les hackers ne sont pas ce qu'en disent les médias – des trublions de l'informatique qui ne penseraient qu'à percer à jour les codes secrets, s'infiltrer illégalement dans les systèmes et répandre le chaos sur le réseau. Ceux qui se comportent ainsi sont les crackers, et en général la culture hacker les rejette*»[166]. Une véritable opposition distingue les *hackers* des *crackers* quant au risque qu'ils représentent pour le système Internet (Les *crackers* en tant que risque réel, les *hackers* en tant que risque fantasmé). Il convient de le retenir dans toute réflexion et diffusion d'information relative à la sécurité des systèmes d'information et de communication, mais également dans toute démarche de réflexion relative à la régulation

[165] http://denislabrosse.net/articles/index.php.
[166] *La galaxie Internet* (Castells, 2001).

d’Internet. Plus que jamais, l’ensemble des médias doit aussi clarifier son discours et tenir compte de cette différence effective.

Au-delà de cette mise en évidence de la représentation médiatique de l’objet de recherche, nous proposons de déterminer, justement afin de les confronter, les significations d’autres mondes aussi attachés à la construction de l’objet. En effet, la représentation médiatique, nous l’avons vu, est dominante et influence fortement l’image sociale dominante de l’objet, cependant d’autres mondes participent aussi à l’édification des significations du pirate informatique, et peuvent apparaître masqués par cet état de fait.

- Figure 2. Modélisation graphique de la représentation médiatique du pirate informatique



III – D'autres mondes « bâtisseurs » d'images du pirate informatique

Il appert que l'image dominante est guidée par les représentations médiatiques de l'objet. Cependant, ce monde n'est pas le seul à fournir une vue significative du pirate informatique. Ainsi, le monde des experts sécurité de l'information formalise également une image singulière de l'objet de recherche, et pas forcément reprise par les médias. Nous avons pu vérifier dans la deuxième partie de notre recherche, que le second questionnaire utilisé vers le monde des experts SSIC, formalise des résultats de recherche parfois fortement différents sur les éléments de valeurs généraux attribués aux pirates informatiques. De plus, le monde des pirates informatiques construit également des significations particulières qu'il convient d'étudier. Nous traiterons, ainsi, dans un premier temps, de la sécurité de l'information et de la communication comme domaine d'expertise participant aussi à la génération des significations sociales de l'objet de recherche. Puis, nous nous intéresserons également au monde des acteurs principaux de la cyberdélinquance, concernés au premier chef de la construction de leur propre représentation sociale.

1) La sécurité de l'information et de la communication pour domaine d'expertise

Le domaine de l'expertise, quant aux mondes de la cyberdélinquance, repose principalement sur le monde de la sécurité de l'information. Ce dernier est composé des professionnels spécialisés sur les différents référentiels de la sécurité de l'information, qu'ils développent et qu'ils reconnaissent ensuite comme solution requise pour pallier notamment aux risques de sécurité (le sous-comité ISO/JTC1/SC27[167] : « *IT Security Techniques* » représente, par exemple, une composante essentielle de ce monde des experts sécurité). Pour ce faire, les experts sécurité sont à l'origine de nombreuses bases de connaissances de menaces ciblées permettant, par exemple, de prendre conscience des

[167] http://www.jtc1.org.

profils des attaquants. Ainsi, une analyse des référentiels de sécurité des systèmes d'information et de la communication permet de faire une synthèse homogène de l'ensemble des risques de sécurité qu'il semble important de connaître et de comprendre pour l'utilisateur. Ces risques sont le plus généralement classés suivant différentes catégories de menaces qui constituent l'origine primaire du risque. Les principales catégories de risques de sécurité, définies à l'aide des menaces, sont donc les suivantes : phénomène naturel ou environnemental, défaillance technique, acteur humain non-malveillant, et enfin acteur humain malveillant (notre objet de recherche).

Au cœur du risque de sécurité, les experts estiment que la menace constitue certainement l'élément le plus difficile à cerner, du point de vue de son identification et de son niveau de dangerosité. Ceci est dû, comme expliqué précédemment, à son caractère purement probabiliste (on ne sait jamais quand une attaque peut se réaliser) et totalement incontrôlable. En effet, autant la vulnérabilité peut être contrôlée et diminuée par des contre-mesures (techniques ou non) à appliquer sur un système, autant il est difficile d'agir sur la menace généralement hors de portée de l'utilisateur (mais aussi de l'expert sécurité). C'est une des raisons pour laquelle la gouvernance des menaces relève de l'autorité des pouvoirs publics qui s'organisent en fonction des tendances ou de l'état global constaté de la menace. Le Conseil de l'Europe a, à ce titre, rédigé la Convention Cybercrime[168], ratifiée à ce jour[169] par 15 états membres et signée par 28. Elle est également entrée en vigueur dès janvier 2007 aux Etats-Unis.

Les experts sécurité ont procédé à la définition d'une catégorisation des menaces qui permet d'identifier de manière théorique toutes les possibilités pouvant atteindre un utilisateur, et pouvant être véritablement de nature diverse, pas uniquement en provenance de l'univers des TIC, mais aussi *via* des menaces humaines. Ces experts les décrivent sous le vocable globalisé de « cyberdélinquance » recouvrant à la fois les menaces, les attaques, les éléments dangereux, les préjudices générés par des « armées de pirates » structurées en organisations diverses. Ces derniers offrent notamment une classification des différentes typologies de pirates informatiques tels que les *hackers*, les *crackers*, et les *script-kiddies*.

[168] http://conventions.coe.int.
[169] Données juillet 2006.

La structure CASES (*Cyberworld Awareness & Security Enhancement Structure*)[170], portail national luxembourgeois de la sécurité de l'information, faisant partie intégrante du monde des experts sécurité, a récemment structuré cette approche des trois profils catégorisés des cyberdélinquants, en rédigeant une fiche didactique complète de l'objet social de notre étude : « *Les cyberdélinquants se définissent, communément, soit comme acteurs visant l'intégrité d'un site informatique déterminé, soit comme acteurs menant un délit ou crime conventionnel à l'aide d'un outil informatique. La différence se décline selon l'utilisation faite, par le cyber-délinquant, du médium informatique* ». Ainsi, si tout *hacker* peut être « étiqueté » en tant que cyberdélinquant, tous les cyberdélinquants ne sont pas des *hackers*. Les *hackers* se démarquent des *crackers* et des *script-kiddies* par leur sens de l'éthique. Contrairement à ces derniers, ils n'attaquent pas leurs cibles, mais se contentent d'enfreindre la sécurité de leurs systèmes pour en souligner les failles. Il s'agit pour le *hacker*, à travers des moyens, illicites, il est vrai, de relever un « challenge » technologique tout en agissant pour le bien des organisations attaquées, puisqu'il permet l'amélioration de la sécurité du système d'information concerné. Le *cracker* ou « chapeau noir », souvent confondu avec le *hacker*, pénètre les systèmes informatiques avec l'intention de nuire. Les *scripts-kiddies*, quant à eux, forment le « bas de gamme » du piratage informatique. Si les deux communautés précédentes se focalisent sur des cibles spécifiques, les *script-kiddies* eux, lancent leurs attaques de manière totalement aléatoire en utilisant des listes de commandes groupées dans un *script* (programme exécutable), d'où leur nom. Ce type d'attaque ne demande pas un très haut niveau de connaissance informatique ; c'est pourquoi le *script-kiddy* est souvent un adolescent voire parfois un enfant. Ce dernier utilise des logiciels « prêts à l'emploi », ne maîtrisant nullement les conséquences de l'action entreprise, ni même son fonctionnement. Cette classification est largement développée et utilisée comme référence au sein du monde professionnel des experts de la sécurité de l'information.

[170] http://www.cases.public.lu.

Pratiques courantes des attaques numériques retenues par l'expertise sécurité

Les risques appliqués aux systèmes d'information, connectés à des réseaux ouverts notamment, font l'objet d'une méthode d'analyse qui répond, nous l'avons vu, à l'équation suivante : Risque = Vulnérabilité*Menace*Impact.

La « *Risk Equation* » (équation du risque) est connue du monde des experts ; S. Bosworth et M.E. Kabay dans *Computer Security Handbook*, la reprennent dans le détail et en précise le fondement : « *Les critères d'évaluation et de mise en place de la sécurité informatique semblent très peu efficaces. Ce chapitre présente l'équation du risque en tant que nouveau moyen de vérifier les éléments principaux permettant une approche sécurité. Elle est utile pour les administrateurs systèmes, les gestionnaires de sécurité, et permet de prévoir et de garantir la sécurité à appliquer : Risque = Menace*Vulnérabilité*Coût*[171] ».

Il y a beaucoup de manières de voir le risque et beaucoup de différences dans l'utilisation même du terme. L'équation est simple : Risque = Menace*Vulnérabilité*Coût. Ainsi, « *Tel un guide, les spécifications des normes contiennent des critères qui ne conviennent pas forcément à toutes les organisations. « Risque = Menace*Vulnérabilité*Coût », est une équation qui fournit la base permettant de cibler les risques réels affectant les ressources ainsi que le moyen de le réduire et de les atténuer* ».[172]

Tout système d'information et de communication possède des vulnérabilités qui peuvent être plus ou moins facilement exploitées par une menace. Une vulnérabilité est

---

[171] *« Many of the past and present criteria for evaluating and implementing computer security have proven to be only marginally effective, at best. This chapter presents the risk equation as another way to view the major elements of a sound computer security approach. The risk equation is useful to network administrators and security managers because it, better than anything else known can clarify thinking and help to maintain a well-directed, effective security course well into the future. There are many ways to look at risk and many subtle and subtancial differences in the use of risk-related terms. In the following simple approach, developped at TruSecure – ICSA Labs, just four terms are tied together as simple equation :*
*Risk = Threat*Vulnerability*Cost. »*
Computer Security Handbook (Bosworth, Kabay, 2002).

[172] « *Just as in the Code of Practice, the specification standard contains a variety of criteria, not all of which will be applicable to every organization. Risk = Threat * Vulnerability * Even Cost which provides the foundation for focusing resources on real risk reduction and mitigation.* »
Equation du risque également reprise dans ISO/IEC 17799 :2005, norme internationale de sécurité organisationnelle des systèmes d'information et de communication.

difficile à détecter, même pour un spécialiste. Pour cette raison, des listes de vulnérabilités triées par systèmes d'exploitation sont répertoriées par les CERT (*Computer Emergency and Response Team*), le CSI (*Computer Security Institute*) (Institut de Sécurité Informatique), et d'autres encore.

Pour pouvoir bien informer toutes les personnes concernées de la présence de nouvelles vulnérabilités, les experts de la sécurité de l'information et de la communication déterminent l'importance de mettre en place un réseau d'information et de veille qui est capable de diffuser rapidement des informations importantes. Même si les vulnérabilités ne sont découvertes que « post-incident », un tel réseau peut réduire considérablement le nombre d'incidents. Les vulnérabilités peuvent exister au niveau du logiciel, du matériel, du personnel, auprès de la politique de sécurité, des procédures de sécurité, des programmes de sensibilisation, des plans de secours et/ou de réponse.

S. Bosworth et M. E. Kabay définissent les vulnérabilités tel que : « *Une vulnérabilité est la probabilité de succès d'une catégorie de menaces particulières contre une organisation ciblée* »[173]. Contrairement aux vulnérabilités, une organisation n'a pas d'influence directe sur les menaces, mais elle peut se protéger en agissant sur ses potentielles vulnérabilités. S. Bosworth et M.E. Kabay, définissent les menaces de la sorte : « *La menace est la fréquence ou le taux de probabilité d'évènements potentiellement défavorables* »[174].

Toutes les menaces sont également une cause potentielle de perte. Nous avons vu *supra* qu'elles appartiennent à deux catégories : « intentionnelles » ou « non intentionnelles ».

Les pirates informatiques utilisent également toute une panoplie d'outils malveillants, décrite spécifiquement par les experts de la SSIC :

- <u>cheval de Troie</u> **:** programme espion déposé par un pirate dans un système victime. Le but est d'avoir accès à la machine et aux informations confidentielles stockées. Le principe est simple, une machine infectée par un programme de type cheval de Troie, va,

[173] « *Vulnerability is the likelihood of success of a particular threat category against a particular organization* ».
Computer Security Handbook (Bosworth et Kabay, 2002).

[174] « *Threat is the frequency, or occurrence rate, of potentially adverse events* »
Computer Security Handbook (Bosworth et Kabay, 2002).

lorsqu'elle se connecte à Internet, indiquer au pirate que la porte (port de communication spécifique) est ouverte. Le pirate peut alors se connecter sur la machine victime, *via* le cheval de Troie, et accéder aux fichiers de la personne piégée.

- virus : programme informatique qui vise l'intégrité d'un système sur lequel il est exécuté. Ce type de programme correspond à une instruction ou suite d'instructions susceptibles d'entraîner diverses perturbations dans le fonctionnement de l'ordinateur visé.

- vers : certains virus appelés vers (worms) se reproduisent à travers les réseaux et ont comme but d'infiltrer le système et de détruire ou modifier des données voire d'exécuter des commandes.

- bombes logiques : petits programmes laissés inactifs au sein d'un système visé aussi longtemps qu'une condition spécifique n'est pas remplie. Une fois la condition remplie, comme par exemple une date déterminée à l'avance, une suite de commandes est exécutée dans le but de faire un maximum de dégâts.

- trappes **:** ou « backs doors » sont généralement envoyées par téléchargement à partir d'un site web. Les trappes sont souvent déguisées en programmes inoffensifs. Une fois ouverts, les programmes s'installent sur l'ordinateur victime à l'insu de son propriétaire. Une back door ainsi installée constitue ensuite un point d'entrée pour le pirate.

- *TCP-SYN Flooding* **:** l'attaque de type « *syn-flood* » est une inondation par paquets SYN d'une machine cible. Les fichiers en attente de connexion sont alors inondés, ce qui empêche le traitement des demandes de connexions entrantes. L'hôte est inondé par des centaines de requêtes, un temps considérable s'écoulera avant qu'il ne puisse à nouveau traiter les requêtes de connexion.

Enfin, il est important de savoir que les menaces intentionnelles peuvent être également véhiculées hors réseaux par les pirates informatiques :

- *social engineering* : dans ce cas précis la victime n'est pas confrontée à une manipulation technique mais à un pirate qui se fait passer pour une personne identifiée pour avoir accès à des informations tel qu'un mot de passe par exemple. Ce scénario est pratique courante ; les pirates agissent souvent par pression psychologique ou invoquent l'urgence pour obtenir les renseignements rapidement.

- craquage de mot de passe : il fournit une aide précieuse aux pirates pour pénétrer les réseaux cibles. En effet, la méthode consiste à récupérer un fichier de mots de passe qu'il faut deviner par combinaisons. Les programmes de craquage de mots de passe essaient chaque combinaison jusqu'à découverte du bon mot de passe. Une fois le mot de passe découvert, le pirate peut pénétrer les réseaux cibles.

Le *National Institute of Standardization Technology* (N.I.S.T), s'est, très tôt, intéressé aux risques, ayant défini les rôles « clef » en matière de sécurité dont l'étude des risques. Au sein des « agents menaçants » sont repris les *hackers* (pour le challenge, l'ego…), les *crackers* et les criminels informatiques pour tout ce qui est destruction, altération de données, divulgation d'information, gain monétaire.

Quant à l'impact ou le coût, S. Bosworth et M. E. Kabay estiment « *Le coût de l'incident de sécurité correspond au dommage global subi par l'organisation victime* »[175].

Une « délinquance globale » assistée par ordinateur

De la littérature pléthorique consacrée à la criminalité contemporaine, quelques indications peuvent être, dès-à-présent, retenues quant au pirate informatique. Elles concernent en particulier les corrélations susceptibles d'être établies entre les formes actuelles de la délinquance et les modes de croissance et de fonctionnement des sociétés économiquement développées. Des causes générales sont identifiées dans les bouleversements produits par le passage de l'économie agricole à l'économie industrielle, et dont le développement du capitalisme n'a cessé d'aggraver les effets ; à savoir la dislocation des anciens ordres communautaires ayant entraîné une destructuration des représentations collectives de l'unité sociale et de la famille en particulier. A tout le moins, ce principe est vérifiable sur Internet qui ne présente pas véritablement de vecteur central et reconnu veillant à la respectabilité du réseau de réseaux.

[175] « *Event cost is the total cost in both real and soft dollars related to the total ramifications of a particular exploit experienced by a vulnerable target company or system* »
Computer Security Handbook (Bosworth et Kabay, 2002).

L'industrialisation s'est par ailleurs accompagnée de processus démographiques qui ont modifié la structure de la population délinquante et les formes de criminalité. L'accélération spectaculaire de l'urbanisation, outre l'anonymat qui en a résulté pour les habitants des grandes villes, a créé des problèmes inédits dans les domaines du logement, de la circulation, de l'ordre public, et déterminé la formation de zones ou d'anneaux favorables au développement de la délinquance juvénile. Transposé à la « société de l'information », le développement de la délinquance a suivi le même parcours avec le développement d'Internet, profitant de l'anonymat de la toile pour développer des actes de trouble à l'ordre public et à la circulation de l'information.

L'universalisation du système de production et de consommation de masse a, dans le même temps, généralisé les occasions d'infractions contre les biens, liées structurellement à l'extension du chômage et à la permanence des inégalités de revenus, mais aussi aux disparités devant la santé et la scolarité. Parallèlement à la petite délinquance s'est développée la « *white collar criminality* » étudié par Sutherland (considéré comme le fondateur de la sociologie criminelle américaine, il voit dans la criminalité un processus socioculturel inhérent à chaque société) c'est-à-dire la délinquance des « cols blancs » propre aux milieux économiquement élevés et qui est le fait d'individus parfaitement intégrés.

Cela semble particulièrement vrai pour la délinquance assistée par ordinateur qui est le fait de personnes ayant les moyens d'avoir un ordinateur, une connexion Internet, acquis des connaissances techniques et le temps de les mettre en pratique. L'amélioration d'ensemble des conditions sociales d'existence s'est ainsi accompagnée d'un accroissement et d'une diversification de la délinquance, mais aussi de sa banalisation, qui se traduit par un effacement progressif du clivage séparant le délinquant du non délinquant. Ainsi, il n'est pas rare d'entendre en réaction à la diffusion médiatique de certains piratages, des réflexions du type : « *c'est un vrai génie…il faut être fort pour faire cela…ce n'est pas grave il n'a tué personne…* » (SIC – opinion publique).

Par ailleurs, si le progrès technique, telle l'informatisation a contribué à perfectionner les instruments de répression du crime, elle n'en a pas pour autant favorisé l'efficacité, parce qu'elle a tout aussi bien profité à des catégories de criminels dont le

rendement s'est ainsi accru. De nouveaux types de crimes ont même vu le jour (voir première partie).

Quant à la notion de réseaux de *hackers*, les menaces actuelles proviennent plus de l'exploitation d'outils à caractère malveillant disponibles sur Internet, que d'experts développant un savoir-faire personnel. Alors que les groupes d'attaquants sont actifs et nombreux, les victimes potentielles sont d'ordinaire passives et isolées. Une généalogie du cybercrime[176] est également mise au jour. Le premier délit informatique identifié est commis aux Etats-Unis en 1966 (nous l'avons vu, il s'agissait alors d'une altération des comptes d'une banque de Minneapolis), mais la criminalité des réseaux est globalement un phénomène plus récent, en expansion constante depuis le début des années 1980, qui s'est généralisée en France, depuis l'avènement d'Internet, fin 1994. R. Trégouët donne en 1997 une définition du terme *hacker* : « *une personne qui aime comprendre et utiliser les finesses techniques des programmes* »[177]. Il qualifie ainsi aujourd'hui les délinquants pénétrant par effraction des sites informatiques ; le terme, *hacker*, néologisme de sens assez large, n'est cependant pas si facilement applicable pour toute situation de délinquance informatique.

Le principe d'une nouvelle délinquance semble bien correspondre à Internet : « *la croissance exceptionnelle de cet univers de communication s'accompagne évidemment de son cortège de méfaits : les nouvelles technologies de l'information et de la communication sont à la fois l'objet et l'outil de nouvelles délinquances. On peut classer ces délinquances en fonction de l'objet technologique concerné ou en fonction de l'usage qui en est fait : si c'est un outil utilisé par le criminel pour commettre son forfait ou s'il en est l'objet même* »[178]. Les TIC sont, soit les armes de l'activité criminelle (outils de la délinquance) soit les victimes d'actes criminels, notamment l'objet virtuel : « *une taxe téléphonique, un programme informatique, des données personnelles ou de la monnaie électronique. Dans cette perspective, on a introduit une nouvelle notion pénale, l'atteinte à un système informatique, sa perturbation ou le fait de s'y introduire par les réseaux,*

[176] *La criminalité sur* l'Internet (Pansier, Jez, 2000).
[177] *Des pyramides du pouvoir aux réseaux de savoirs* (Tregouet, 1997/1998).
[178] *L'internet* (Capul, mars-avril 2000).

lorsqu'on n'y est pas autorisé »[179]. Ce sont les crimes et délits informatiques réprimés en France par la loi Godfrain de 1988. Mais nous ne pouvons nous contenter du rendu « historique » des acteurs du cybercrime, de plus le rapport de l'objet de recherche avec le phénomène de la cyberdélinquance (sa représentation sociale) est complexe, il convient aussi, à ce titre, d'en rendre compte de manière participante (Cf. *infra*).

Risque et acteurs de la cyberdélinquance

« *La manipulation des peurs sert tous ceux qui font des affaires avec la sécurité.*

L'insécurité ne veut rien dire, comme la délinquance dont il existe des genres différents, dans tous milieux professionnels, sociaux, à tout âge. Idem pour la violence, a fortiori, lorsqu'aujourd'hui, sous le même vocable, on désigne aussi bien un regard dur qu'un meurtre, une gifle ou une injure. Ces mots renvoient à des peurs, pas à des phénomènes précis » [180]. De plus, D. Duclos affirme que les discours sur les dangers peuvent avoir des effets nocifs : « *Remplaçant les peurs de la damnation ou de la famine, le risque est d'abord un outil d'influence* ».

« *Il ne s'agit pas seulement de rééquilibrer les reproches adressés aux collectifs et accusations envers des individus imprudents : l'intensité du thème du risque doit être globalement atténuée, car le seul climat de peur surchage chacun de culpabilité tout en multipliant les barrières techniques et administratives à la liberté, à commencer par celle de penser. Il faut alors distinguer risque réel et risque fantasmé. Les deux sont liés puisqu'un fantasme peut devenir dangereux, mais leurs traitements sont inverses : nous attaquons directement les « causes objectives » du risque réel, tandis que le risque fantasmé n'est diminué que si l'on enraie la spirale des indignations et des répressions, en apaisant l'effroi sans rapport avec le danger prétexté. Or les risques fantasmés passent pour des risques réels dans la bouche des « crieurs-au-loup »* »[181].

Le risque réel porte sur des faits patents, survenus ou potentiels, affectant de vastes populations, ce qui est le cas pour les attaques recensées sur Internet, considérées comme des accidents majeurs. La cyberdélinquance est un risque pour Internet.

[179] *L'internet* (Capul, mars-avril 2000).
[180] *Violence et insécurité, fantasmes et réalités dans le débat français* (Mucchielli, 2001).
[181] *Le grand théatre des experts du risque* (Duclos, in Le Monde Diplomatique (06/2002)).

Cependant, « *Quant au risque fantasmé, il s'attaque souvent injustement à des « boucs émissaires* »[182]. L'élargissement de notre étude montre que les menaces sont réelles. Ce qui nous permet de valider la cyberdélinquance en tant que risque pour le système Internet. Cependant, les articles de presse semblent généraliser les acteurs de la cyberdélinquance. Notre étude précise, en effet, que ces acteurs font partis des menaces, il appert que les entraves communicationnelles sont le fait surtout de ces sujets particuliers. Qui sont-ils et que revendiquent-ils ? Leur catégorisation permet-elle de qualifier un risque réel ou bien relevant du fantasme ? Existent-ils des acteurs réellement délinquants et des boucs-émissaires au sein de la cyberdélinquance ?

Finalement qu'en pensons-nous ? Par nous-mêmes ou bien comme pensent les autres ? Peut-on mettre en évidence un conformisme qui se présente avant tout comme la détermination par la majorité non du jugement de l'objet mais de l'objet du jugement ?

Catégorisation des menaces au cœur des risques de sécurité

La croissance des réseaux informatiques à l'échelle internationale entraîne corrélativement une aggravation des risques et des menaces associées. Ces dernières sont multiformes, ne connaissent pas de frontières, ne se limitant pas au périmètre de l'organisation, ni d'une cible déterminée. Chacun peut être concerné par la menace, dans son sens général, particulièrement l'utilisateur final. Cette dernière peut s'attaquer à n'importe quel système pour autant que ce dernier soit interconnecté. Les attaques peuvent par exemple reposer sur des techniques de « *scanning* » aléatoire. A ce titre, la menace se présente alors comme un état générique qui concerne l'ensemble de la société.

Elle devient particulière et dangereuse lorsqu'elle trouve un récepteur, c'est-à-dire un système vulnérable en réponse à une attaque. Souvent, l'utilisateur final n'est pas celui qui paraît le mieux armé, le plus conscient, finalement, le plus sensibilisé au fait. En termes de risque, la société de l'information n'est finalement qu'une transposition de la société traditionnelle : « *la production sociale de richesses est systématiquement corrélée à la production sociale de risques* ». U. Beck précise, en effet, « *A la différence de toutes les époques qui l'ont précédée, la société du risque se caractérise avant tout par un*

[182] *Le grand théatre des experts du risque* (Duclos, in Le Monde Diplomatique (06/2002)).

manque : l'impossibilité d'imputer les situations de menaces à des causes externes. Contrairement à toutes les cultures et à toutes les phases d'évolutions antérieures, la société est aujourd'hui confrontée à elle-même ». Ainsi, les sociétés mêmes sont devenues des manufactures du risque. U. Beck défend la thèse de ces sociétés qui produisent, à travers leurs systèmes productifs et scientifiques, de nouveaux risques devant lesquels les individus ne sont pas égaux. Ces risques peuvent être alors considérés comme un phénomène sociétal.

Cependant, les représentations sociales des menaces effectives et reconnues de manière détaillée sur les réseaux d'information et de la communication sont encore peu développées (De manière générale la cyberdélinquance est reconnue, mais l'existence et les valeurs des acteurs responsables demeurent floues). Elles ne sont en effet, pas instinctives, ni automatiques, comme elles peuvent l'être dans la société traditionnelle. De plus, pour un système d'information et de communication elles ne se réduisent pas uniquement aux technologies et à l'outil informatique. Ces menaces peuvent être analysées dans un cadre beaucoup plus large *via* le concept de sécurité de l'information, atteignant à la fois les structures physiques, organisationnelles, humaines, ou encore techniques. Une analyse des référentiels de sécurité des systèmes d'information et de la communication permet de faire une synthèse homogène de l'ensemble des risques de sécurité qu'il semble important de connaître et de comprendre pour l'utilisateur final. Ces risques sont le plus généralement classés à l'aide des différentes catégories de menaces, ces dernières constituant l'origine primaire du risque. Les principales catégories de risques de sécurité, définies à l'aide des menaces, par les experts SSIC, sont donc les suivantes :

- Phénomène naturel ou environnemental : Ces risques ont pour origine soit des évènements naturels, par exemple liées aux conditions météorologiques (foudre, inondation, tempête…), soit à l'environnement de l'utilisateur et de son système (incendies, dégâts des eaux, coupures de courant, etc.). Leur cause est généralement accidentelle, beaucoup plus rarement intentionnelle.

- Défaillance technique : Les risques de cette catégorie sont issus de problèmes du système informatique, comme les pannes matérielles ou les dysfonctionnements logiciels, qui sont accidentels et qui entraînent souvent la perte du service offert par le SI (disponibilité). Y sont également compris l'ensemble des logiciels malveillants comme les vers, virus, *spyware*…, mais qui sont regroupés sous le terme anglais couramment utilisé de *malware*. Ces derniers agents techniques ont quant à eux une cause intentionnelle et entraînent des problèmes techniques au sein du système.
- Acteur humain non malveillant : Les risques liés à des acteurs humains non malveillants ont généralement pour origine des erreurs d'utilisation ou des oublis. Leur cause est accidentelle. L'erreur humaine n'a pas la dimension d'un piratage informatique mais peut être à l'origine de sinistres informatiques graves. L'erreur peut consister en une distraction, une négligence, qui ne correspond pas au rythme ou procédure de travail régulier dans une sphère de sécurité donnée (dictée par exemple par une politique de sécurité de l'information).
- Acteur humain malveillant : Cette catégorie de risque regroupe l'ensemble des attaques volontaires sur un système donné. On y retrouve des attaques distantes (*via* les réseaux) ou des actes malveillants réalisés par un attaquant ayant un accès physique au système (vol, modification d'information). Leur cause demeure toujours délibérée, généralement malveillante, il s'agit d'une menace très orientée vers l'utilisateur qui devient une cible finale privilégiée, sans en être généralement conscient (*phishing*, *botnets* ou réseaux de robots, chevaux de Troie, *rootkits*…). Ces menaces intentionnelles peuvent être passives (ne modifiant pas le comportement du système et étant parfois indétectables) ou bien actives (modification du contenu de l'information).

Au cœur du risque de sécurité, la menace constitue certainement l'élément le plus difficile à cerner, du point de vue de son identification et de son niveau de dangerosité. Ceci est dû, comme expliqué précédemment, à son caractère purement probabiliste (on ne sait jamais quand une attaque peut se réaliser) et totalement incontrôlable. Les experts SSIC recourent aussi à la catégorisation pour expliquer le pirate informatique, mais pas toujours par retour d'expérience même d'interactions de terrain avec les acteurs de la cyberdélinquance, masquant aussi, *de facto*, un aspect de sa réalité sociale.

2) Les acteurs principaux de la cyberdélinquance

Nous avons indiqué que ce monde « *underground* » des pirates informatiques (connu aussi sous le vocable globalisé de monde du « *hacking* ») est celui qui est le plus difficile à percevoir ; en effet sa dénomination détermine toute l'opacité de ce milieu. Nous le qualifierons comme tout individu se revendiquant de ce milieu. Elle se situe hors de la vision du grand public dans le but avoué de conserver son « identité culturelle » héritée des origines, et d'autre part par des valeurs véhiculées souvent considérées comme n'étant pas politiquement correctes, voire illégales. Cependant, cette communauté se mobilise notamment pour combattre l'image négative qui tend à s'instaurer, la concernant, et souvent au niveau médiatique. Ainsi, Rop Gonggrijp (professionnel d'Internet et un des organisateurs de « *Galactic Hacker Party* » – 1989), indique qu'il est important que les réunions dédiées au « *hacking* » se tiennent en plein air, et se passent dans une ambiance « relaxe » (sic), totalement ouverte. Ce dernier indique que l'idée est de casser le stéréotype des « *hackers* », qui est réellement à l'inverse d'un « vandale ». Rejoignant, par le fait, la catégorisation du monde des experts de la sécurité de l'information.

La volonté de faire connaître et reconnaître ses talents est un élément constitutif de la culture du *hacking*. Un piratage de système informatique qui ne serait pas connu d'autres que soi-même n'a finalement que peu de valeur, sauf pour ceux qui décident d'en profiter pour en retirer de l'argent. Pour les autres, à la recherche d'un challenge informatique, le *hacking* nécessite la reconnaissance des pairs. Pour ce faire, les lieux de meeting dédié à cette culture du « *hack* » demeurent des espaces de connaissance et de reconnaissance des différentes parties prenantes. La conférence *Black Hats*[183], par exemple, offre un dispositif de visibilité et de confrontation, où même les autorités légales de lutte contre la fraude informatique admettent les performances exposées. Parfois, certains *Black Hats* d'origine, finissent par changer de bord et se font employer par des sociétés spécialisées dans la sécurité informatique. Un exemple récent est celui de Sven Jaschan, auteur du virus *Sasser*, recruté en 2005, par la PME allemande *Securepoint*. Sven Jaschan est désormais considéré comme un *traître* par certains *Black*

[183] http://www.blackhat.com.

Hats (« Chapeaux noirs ») qui considèrent qu'il ne devait pas se vanter à ce point de ses actions douteuses…

Il semble convenu que le milieu du « *hack* » souhaite rester « *underground* », de plus, il est clairement impossible de se proclamer de ce monde ou encore « *hacker* », puisque généralement se sont les « pairs » (ceux de la « scène » : vocable du terrain de jeu « *underground* ») qui vous reconnaissent en tant que tel, et qui vous qualifient en fonction de vos développements et actions reconnues. Dans ce cadre, le regard de la communauté donne son identité sociale ; l'identité de *hacker* se mérite, elle est le fruit d'un processus apparenté à une forme d'initiation, avec la réalisation de performances informatiques et le respect d'une certaine éthique. Associée à cette reconnaissance, l'expertise technique est indissociable, et doit être de très haut niveau. La notion de partage, de confrontation est manifestement constitutive de cette activité et confère un vrai sens à l'idée de communauté, fut-elle virtuelle. De fait, actuellement, les travaux de recherche sont difficiles dans ce milieu, notamment en s'affichant « officiellement » en tant que chercheur, et sans appartenance à ce monde social.

Finalement, ce monde se présente comme un état d'esprit, celui du « *hack* » véritablement opposé au cybercrime. Cela rend possible la distinction entre les *hackers* et les « véritables cybercriminels ». Pour ce monde « *underground* », les motivations de ces différentes classes sont diverses : la recherche d'identité, des codes, des valeurs, l'éthique, une culture singulière proche d'un idéal libertaire, un fort ego, le besoin de reconnaissance, la soif de progresser et la nécessaire existence de moyens de regroupement. Il ressort que la lutte pour la diffusion d'une image positive de leur action et de leur philosophie est un enjeu important pour ce monde qui refuse toute labellisation comme criminel. Leur lutte ne semble pas vaine, car on retrouve plutôt bien la dichotomie souhaitée « *Hackers / Crackers* » dans divers écrits journalistiques ou grand public (cela restant tout de même versatile en terme de représentation), mais aussi au sein du monde des experts de la sécurité de l'information. Cependant, seule la catégorisation peut apparaître une piste fédératrice, les aspects de légitimité des actes de piratages informatiques n'étant pas partagés par l'ensemble des mondes.

« *C'est au début des années 60 qu'un groupe de programmeurs passionnés du MIT décide de se nommer hackers. Le terme va assez rapidement servir à désigner une*

élite informatique et constituer ce que l'on a appelé le clergé de l'informatique. Ce n'est que récemment que le terme hacker – devenu en français pirate – a commencé à désigner une personne capable de pousser un programme informatique au-delà de ses capacités supposées ou encore d'optimiser le code source d'un programme au maximum. Quant au hacking dans son acception la plus moderne, elle apparaît au début des années 80 dans la presse informatique pour désigner, désormais, toutes les atteintes aux systèmes de traitement automatisé de données : manipulations de programmes, falsifications de données, intrusions malveillantes dans les systèmes informatiques… »[184].

E. S. Raymond[185] oppose les *hackers*, chevaliers de l'innovation, aux *crackers*, qualifiés de pirates. Si cette différenciation était chose aisée dans les années 60 et 70, elle ne l'est plus de nos jours, notamment à travers la diffusion médiatique. « *Aux termes : to hack, hacker, E. S.Raymond, a consacré un article complet. Il s'agit de l'action de comprendre comment les choses fonctionnent, de vouloir savoir ce qui se cache dans les mécaniques diverses, et de les réparer ou de les améliorer. En aucun cas, ce terme ne doit être confondu, avec les pirates de l'informatique, ou crackers. J'ai choisi de traduire ce terme par « bidouille », et je vous demande de ne pas y attacher d'a priori négatif. Un bidouilleur construit des choses parfois très belles et très compliquées, alors qu'un pirate cherche à détruire* »[186]. De même, en introduction à l'enquête du *Boston Consulting Group* est présentée une définition classique du « *hacker* » (voir *supra*).[187]

---

[184] *Hackers ! : Le 5ème pouvoir – Qui sont les pirates de l'Internet* (Chatelain, Roche, 2003).
[185] *The Cathedral and the bazaar* (Raymond S., 2001).
[186] *The Cathedral and the bazaar* (traduit de Blondeel s., 1998).
[187] *« Hackers not crackers » : « hacker. 1. A person who enjoys exploring the details of programmable systems and how to strech their capabilities, as opposed to most sers, who prefer to learn only the minimum necessary.*
2. One who programs enthusiasticaly (even obsessively) or who enjoys programming rather than just theorizing about programming.
3. A person capable of appreciating hack value.
4. A person who good at programing quickly.
5. An expert at a particular program, or one who frequently does work using it for on it ; as in « a Unix Hacker ». (Definition 1 through 5 are correlated, and people who fit them congregate).
6. An expert or enthusisast of any kind. One might be an astronomy hacker, for example.
7. One who enjoys the intellectual challenge of cratively overcoming or circumventing limitations.
8. (deprecated) A malicious meddler who tries to discover sensitive information by poking around. Hence « password hacker », « network hacker ». The correct term for this sense is cracker ». *Hacker Survey* (The Boston Consulting Group, 2002).

Cette définition, reprise mondialement, est en fait issue du *Jargon file*[188] qui définit les *hackers* comme des « *individus qui programment avec enthousiasme, croyant que le partage de l'information est un bien influent et positif et qu'il est de leur devoir de partager leur expertise en écrivant des logiciels libres et en facilitant l'accès à l'information ainsi qu'aux ressources informatiques autant que possible.* ». R. Russell en reprend littéralement la traduction dans *Stratégies anti-hackers*[189] : « *Hacker* : *[Désigne à l'origine un individu maniant une hache pour construire des meubles.] 1. Individu éprouvant un intérêt particulier pour l'exploration en détail des systèmes programmables et la manière d'étendre leurs capacités, contrairement à la plupart des autres utilisateurs, qui préfèrent se contenter du strict minimum. 2. Individu développant des programmes de manière enthousiaste (voire obsessionnelle) ou éprouvant un intérêt particulier pour la programmation au lieu de se contenter d'émettre des théories sur celle-ci. 3. Individu capable d'apprécier la valeur du hacking. 4. Individu maître dans l'art d'écrire des programmes rapidement. 5. Expert dans un programme en particulier : individu utilisant fréquemment ce programme pour effectuer ses tâches ou travaillant directement sur ce programme. On parle par exemple de hacker Unix. (Les définitions 1 à 5 sont en corrélation et les populations appartenant à ces catégories forment un tout.) 6. Désigne tout individu expert ou passionné par un domaine particulier. On peut par exemple être un hacker de l'astronomie. 7. Individu aimant le défi intellectuel qui consiste à dépasser ou à contourner des limites. 8. [sens contesté] Touche à tout malveillant qui tente de découvrir des informations confidentielles en fouinant : password hacker (hacker de mot de passe), network hacker (hacker de réseaux) etc. Dans le cas présent, le terme adéquat est cracker »*[190].

L'idéologie reconnue aux *hackers*, permet également de les qualifier correctement : « *L'idéologie hacker, pour sa version la plus exigeante, repose sur le principe que toute information doit être libre et l'accès aux ordinateurs illimité et total*[191] *[…] L'esprit du*

[188] Dictionnaire des hackers rédigé collectivement sur Internet : http://www.tuxedo.org/~esr/jargon/html/entry/hacker.html.
[189] *Stratégies anti-hackers* (Russell, 2001).
[190] Dictionnaire des hackers rédigé collectivement sur Internet : http://www.tuxedo.org/~esr/jargon/html/entry/hacker.html.
[191] *Hackers : Heroes of the Computer Revolution* (Levy, 1984).

hack : tous se doivent d'y adhérer – c'est d'ailleurs cet esprit qui les distingue définitivement de la criminalité informatique et du terrorisme, comme d'ailleurs de toute industrie liée à la sécurité informatique. Parmi les valeurs de cet esprit du hack qui, en quelque sorte fonde le code des hackers, on trouve : la gratuité de l'information sur Internet, la propriété intellectuelle doit appartenir à tous ceux qui en ont la compréhension, les grandes entreprises ne sont pas dignes de confiance, les grands gouvernements le sont encore moins, toute tentative de légiférer et donc de restreindre le cyber-espace doit être combattue, le savoir-faire technique est la vertu qui doit être la plus valorisée »[192]. L'ouvrage pionnier en matière de détermination du sujet *hacker* est celui de S. Levy qui mentionne que le terme hacker aurait vu le jour au *M.I.T.* (*Massachusetts Institute of Technology*) dans les années 50. Il aurait été utilisé pour la première fois au *MIT Model Railroad Club* (club de modélisme du M.I.T). Le M.I.T. est généralement considéré comme le point de départ de l'usage moderne du terme *hacker*. La définition « acceptable » de ce terme, à travers ces nombreuses réflexions, éclaire notre étude, notamment le dictionnaire *The Jargon File* qui distingue en effet le *hacker* malveillant – qu'il nomme *cracker* – des autres *hackers*. « *Crackers : individu qui enfreint la sécurité d'un système. Terme créé vers 1985 par des hackers en réaction à l'usage impropre que faisaient les journalistes du mot hacker. […] L'apparition de ces deux néologismes reflète le profond dégoût général envers les vols et le vandalisme perpétrés par les réseaux de crackers. Il est légitime que tout hacker digne de ce nom ait effectué des petits cracks et connaisse plusieurs techniques de base ; en revanche tout individu outrepassant ce stade « larvaire » est considéré comme franchissant les bornes excepté si sa conduite est justifiée par des raisons pressantes, justes et pratiques (par exemple s'il est indispensable de contourner un système de sécurité pour pouvoir effectuer une tâche utile. Par conséquent, le hacking et le cracking se ressemblent beaucoup moins qu'on ne le pense : les non-initiés ont été induits en erreur par le journalisme à sensation. Les crackers ont tendance à se rassembler en petits groupes unis et très secrets ; ce comportement n'a pas grand-chose à voir avec le pluralisme culturel revendiqué par les hackers. Bien que les crackers aiment à se définir comme des*

[192] *Hackers le 5ème pouvoir* (Chatelain, Roche, 2002).

hackers, la plupart des véritables hackers les considèrent comme une forme de vie bien distincte et primitive »[193].

Une note de la revue Réseaux[194] précise cette différence : « *Le hacker, lui, essaye pour la beauté du sport d'atteindre un ordinateur distant sans intention frauduleuse. […] Les crackers quant à eux cherchent désespérément à nuire, à effacer les fichiers, implanter des bombes logiques* ». Enfin les « Cahiers français » apportent confirmation en définissant également le terme *hacker* en opposition à celui de *cracker* : « *On établit classiquement une distinction entre ces deux catégories de « bidouilleurs ». « Les hackers peuvent être définis comme des passionnés de programmation qui trouvent leur plaisir dans le décorticage des programmes écrits par les autres, afin d'y apporter des améliorations, d'en corriger les erreurs, cela pour le bien de tous. Les années 80 ont vu l'avènement des « crackers » même si la frontière entre ces deux catégories est parfois ténue. Les crackers utilisent les failles d'un système, sans forcément les avoir dénichées eux-mêmes, à des fins ludiques, destructives ou malhonnêtes* »[195].

Une thèse récente de M. K. Rogers (doctorat en philosophie) : « *Théorie d'étude sociale et analyse du détachement social du comportement du pirate informatique : une étude préliminaire* », août 2001, Département of Psychology University of Manitoba Winnipeg, Manitoba fait état également de cette dichotomie entre *hackers* et *crackers*[196] : « *Beaucoup d'individus utilisant l'informatique à des fins criminelles sont dénommés hackers. Il y a eu beaucoup de controverses et de confusion dans l'usage des termes hackers, et crackers […] Les Hackers déterminent uniquement des personnes intéressées par les réseaux et les ordinateurs. Les crackers tentent de pénétrer à l'intérieur des systèmes ou les détruire* ».

---

[193] *Stratégies anti-hackers* (Russell, 2001).
[194] *Guerres dans le cyberespace, services secrets et Internet* (de J. Guisnel par Wolkowicz, note de lecture in Réseaux (1996, N°75)).
[195] *L'internet* (Capul, 2000).
[196] « *A social learning theory and moral disengagement analysis of criminal computer behavior : an exploratory study* » : « *Many of the individuals who are using computer technology for criminal purposes have been termed hackers. There has been some controversy and confusion over the use of terms like hackers and crackers. […] Hackers are thought to be solely interested in networks and computers. Crackers attempt to break into systems or crack into them (Parker, 1998)* ».

Les *hackers* à l'origine d'Internet ?

« *Qui sont les premiers concepteurs d'Arpanet ? Désolé pour ceux qui s'accrochent à la légende, mais ce ne sont pas des hippies, ni des anarchistes, et encore moins des philosophes ou des idéologues*[197]*. Ce ne sont pas non plus des hackers, ni des sommités scientifiques de l'époque. « Le premier groupe de travail chargé de débroussailler le domaine de la communication des ordinateurs en réseau, le Network Working Group, missionné par la DARPA*[198]*, est un mélange d'ingénieurs tranquilles, d'étudiants de troisième cycle et de représentants des différents départements universitaires appelés à participer au projet* »[199]. Ces derniers vont, tout au long de la genèse d'Internet, favoriser l'échange et l'enrichissement de chacun qui s'accomplit grâce à la libre circulation et la gratuité de l'information, véritable culture d'entraide permettant de faire progresser le réseau de réseaux.

En France le sénateur R. Trégouêt a popularisé *ce concept par la formule « réseaux de savoirs » qui s'opposent aux « pyramides du pouvoir* »[200]. Au sein de cette communauté du développement du réseau de réseaux que nous connaissons aujourd'hui, l'idée dominante était l'absence de contrôle sur le contenu des discussions, concept propice au développement. Le concept d'*Open Source*, garant de la communauté du logiciel Libre, est né de cette mouvance défendant un idéal de transparence et de liberté d'information et de communication. La « récupération » récente du monde économique du médium Internet, n'a pas convaincu la communauté ayant participée à son développement. Leur concept reposait sur un réseau ouvert et neutre. Il est désormais commercial, propriétaire et contrôlé.

Des marginaux s'y opposent, parmi lesquels de nombreux *hackers.* R. Stallman, considéré comme le fondateur du mouvement du logiciel libre, en est une figure marquante. Depuis l'origine de leur travail de développement de la structure d'Internet, tant au niveau logiciel que matériel, les *hackers* n'ont cessé de permettre au réseau de réseau de progresser, permettant le développement d'outils facilitant son utilisation. « *La*

[197] *Le Culte de l'Internet* (Breton, 2000)
[198] Usuellement dénommée DARPA soit *Defense Advanced Research Projects Agency.*
[199] *Les Maîtres du Réseau, les enjeux politiques d'Internet* (Mounier, 2002)
[200] *Des pyramides du Pouvoir aux Réseaux de savoirs* (Trégouët, 1998).

culture techno-méritocratique se spécifie en culture hacker en élaborant certaines règles et habitudes à travers des réseaux de coopération d'intérêt technologique. La culture des communautés virtuelles ajoute au partage de la technologie une dimension sociale : elle fait d'Internet un instrument d'interaction choisi et d'appartenance symbolique. La culture des entrepreneurs s'associe à celle des hackers et des communautés pour diffuser les pratiques d'Internet dans toute la société, à des fins lucratives »[201]. Les *hackers* exécutent leurs travaux avec passion visant à améliorer sans cesse les interactions informatiques, tout cela animé par de fortes revendications.

« *Le culte actif de la transparence, de l'ouverture, de la suppression du secret explique de tels comportements* »[202]. Ceux que D. Weinberger appelle les « *longbeards* », les pères fondateurs, furent, il y a maintenant trente ans, les véritables mécanos du réseau de réseaux, et en même temps, « *les maîtres d'un média qui n'intéressait pas grand monde* »[203]. Aujourd'hui les nouveaux maîtres des réseaux (les acteurs économiques, mais également les régulateurs au sens de P. Mounier[204]) n'ont plus l'état d'esprit de ceux qui l'ont conçu. Les *hackers* revendiquent aujourd'hui, le partage de l'information, le caractère ouvert et le statut public d'Internet, la définition de standards communs et accessibles au plus grand nombre : ce sont devenus de véritables dogmes selon P. Mounier. « *Les biographies des passionnés d'Internet font souvent ressortir ces deux traits, bien au-delà du monde des pirates : d'une part, ils ont un goût prononcé et précoce (souvent dès l'enfance) pour les choses et surtout les objets matériels, goût qui se traduit précisément par une volonté de démontrer ces objets, de les rendre transparents au regard pour en comprendre le fonctionnement […] De ces points de vue, nos pirates sont bien à l'image du monde des croyants d'Internet*»[205].

Le *hacker* cherche véritablement à construire pour une motivation cernée. Il est difficile selon la dichotomie des classifications de sujets de P. Breton de le positionner en tant que « technophobe » mais bien en tant que « technophile ». « *Contrairement aux crackers qui déplombent les logiciels, et aux codeurs, dont la spécialité est la réalisation*

[201] *La galaxie Internet* (Castells, 2001).
[202] *Le culte de l'Internet, une menace pour le lien social ?* (Breton, 2000 : 61).
[203] *Les Maîtres du Réseau, les enjeux politiques d'Internet* (Mounier, 2002).
[204] www.homo-numericus.net.
[205] *Le culte de l'Internet, une menace pour le lien social ?* (Breton, 2000).

et la diffusion de virus, tous les hackers cherchent à construire quelque chose [206] »[207]. « *Le courant principal de la culture hacker est très irrité par les crackers, car ils marquent l'ensemble de la communauté du stigmate de l'irresponsabilité, amplifié par les médias* »[208]. Les *hackers* tendent véritablement à atteindre l'idéal de « cyberdémocratie »[209], en effet P. Lévy spécifie dans son essai : « *Les médias intéractifs, les communautés virtuelles déterritorialisées et l'explosion de la liberté d'expression permise par Internet ouvrent un nouvel espace de communication, inclusif, transparent et universel, qui est amené à renouveler profondément les conditions de la vie publique dans le sens d'une liberté et d'une responsabilité accrues des citoyens* ». Ces revendications ne semblent pas menaçantes, mais relèveraient d'une éthique particulière.

Une éthique des *hackers*

L'éthique est un terme de philosophie, et peut être considérée comme la science de la morale. Peut-il y avoir une éthique des *hackers* ? Les travaux de P. Himanen[210] à travers son exposé « *L'éthique hacker* » semble nous le démontrer. Cependant, ce dernier ne se contente pas de l'éthique *hacker* informatique mais la considère dans un sens plus large, l'éthique *hacker* pouvant s'appliquer à tous à partir du moment ou l'implication des actes, quels qu'ils soient, est passionnée. Telle est l'éthique *hacker* depuis qu'un groupe de programmeurs passionnés du M.I.T.[211] a commencé à se nommer *hackers* au début des années 60.

Beaucoup plus tard, les médias ont appliqué ce terme aux pirates informatiques. Afin d'éviter toute confusion les *hackers* ont, eux-mêmes, baptisé ces personnages destructeurs des *crackers*. Interview de D. Martin : « *Pour vous, le hacker, est-il un cyber-criminel ?Pour moi, le hacker est un bidouilleur. Le vrai hacker n'est pas heureux. Il passe sa vie devant sa machine à tenter de percer les secrets qui l'entourent. Son*

[206] *How to become a hacker* (Raymond, Internet).
[207] *Hackers ! : Le 5ème pouvoir – Qui sont les pirates de l'Internet* (Chatelain, Roche, 2003).
[208] *La galaxie Internet* (Castells, 2001).
[209] *Cyberdémocrati*e (Lévy, 2002).
[210] *L'éthique hackers et l'esprit de l'ère de l'information* (Himanen, 2001).
[211] *Massachussetts Institute of Technoloy*.

bonheur est fugace, il trouve et puis il recommence. Avec l'âge, il change et comprend qu'il risque beaucoup. Pour ce qui est des pirates, ceux qui utilisent le savoir des autres pour s'enrichir, ceux-là sont des cybercriminels. Ce sont eux qui doivent avant tout être mis hors d'état de nuire »[212].

M. Castells fait également référence aux travaux de P. Himanen : « *Selon Pekka Himanen, l'éthique hacker caractérise l'ère de l'information. Je le pense aussi […] La culture hacker joue un rôle pivot dans la construction d'Internet, et ce pour deux raisons : c'est tout d'abord elle qui, tel un milieu nutritif, entretient les percées technologiques par la coopération et la libre communication ; et c'est ensuite à travers elle que le savoir de la «techno-méritocratie » passe dans la sphère des marchands, qui, à leur tour, vont diffuser Internet dans toute la société »*[213]. P. Himanen traduit véritablement à travers son essai le principe de la « *hacker attitude* ». Il considère les *hackers* comme les véritables moteurs d'une profonde mutation sociale. Leur éthique, leur rapport au travail, au temps ou à l'argent sont fondés sur la passion, le plaisir ou le partage. Cette éthique est radicalement opposée à l'éthique protestante, telle qu'elle est définie par M. Weber, du travail comme du devoir, comme valeur en soi, une morale qui domine encore le monde aujourd'hui.

Les *hackers* répondent donc à un code de conduite, guidé par une éthique particulière qui vise à construire plutôt qu'à détruire. Ils se battent pour la liberté de la toile et son usage démocratique. F. Latrive a interviewé P. Himanen qui a répondu à la question : « *Quel est votre hacker préféré ?* » : « *Socrate. Toute son attitude, sa relation passionnée et modeste le désignant, son ouverture d'esprit, sa quête de directions intellectuelles non prévues ; l'attitude des Grecs anciens est très similaire à celle des hackers d'aujourd'hui. Platon, son disciple, a fondé la première académie du monde occidental, et c'est le modèle de la recherche scientifique aujourd'hui. C'est aussi celui des hackers passionnés d'ordinateurs…* »[214]. Le risque qu'ils sont susceptibles de représenter est réellement fantasmé car il ne peut correspondre au risque réel des actes de

[212] *Hackers le 5ème Pouvoir* (Chatelain, Roche, 2002). Daniel Martin est ancien Commissaire Divisionnaire de la D.S.T. Il est aujourd'hui responsable du Service de Sécurité de l'O.C.D.E. (Organisation de Coopération et de Développement Economique).
[213] *La galaxie Internet* (Castells, 2001).
[214] Propos recueillis par Florent Latrive, *Libération*, 25 mai 2001.

piratage, qui parfois sont calqués sur l'appropriation des compétences développées par des *hackers*.

L'impact des *hackers* sur Internet est double : des revendications « légitimées » visant la liberté et la transparence numérique, traduisant le « fantasme » de la menace relayée, mais également, amenant par extension, des actes de piratages répréhensibles, qualifiant réellement la menace. La diffusion de l'information par tout média, vu par l'étude de la presse écrite, fait souvent l'amalgame, et situe la réalité du risque au plus haut point (la « société de l'information du risque »). Le danger concernerait tout le monde, et tous les *hackers* sont dangereux. Alors qu'il conviendrait de modérer ce type d'affirmation et de faire la part des choses.

A ce titre, D. Labrosse, doctorant en sociologie, à l'Université de Québec à Montréal, émet pour hypothèse principale que les *hackers* représentent actuellement le plus important mode de régulation sociale dans les réseaux informatiques. D'après D. Labrosse, il serait impossible de maintenir l'ordre social et la libre circulation de l'information sans mettre en place des structures et des règles qui empêcheraient la libre circulation de l'information sans garantir un ordre sur les réseaux. « *La solution du problème repose sur les hackers. Ils seraient actuellement le plus important mode de régulation sociale dans les réseaux informatiques mondiaux. Ils imposent en quelque sorte un équilibre. Les exploits des hackers, en ce qui concerne les systèmes de sécurité, la confidentialité et les enjeux liés à la cryptographie, sont le meilleur moyen de régulariser les réseaux. Il ne faut donc pas les considérer comme des malfaiteurs mais comme la façon d'empécher que les grandes entreprises comme Microsoft ne soient pas les maîtres des réseaux et donc de l'information* »[215]. Avant de développer cette hypothèse principale, D. Labrosse, pose les bases de sa réflexion qui converge avec les résultats de notre étude : « *Pourquoi les hackers sont-ils perçus comme des individus n'utilisant leurs connaissances que pour s'introduire illégalement dans les serveurs informatiques? La raison principale provient sûrement de l'image diffusée par les médias, particulièrement les journaux et la télévision alors que le cinéma glorifie bien souvent les activités des hackers. Dans un article intitulé « Discourses of Danger and the*

[215] http://pages.infinit.net/cybersoc/hackers/consequencestxt.htm.

Computer Hacker » (The Information Society, 13:361-374, 1997), D. Halbert traite du rôle des médias dans la construction négative de la représentation sociale des hackers. Les médias utilisent les termes « pirates informatiques », « terroristes informatiques » et « hackers » comme synonyme pour parler des activités d'intrusion informatique et des dangers que représentent les pirates informatiques. Or, les hackers, contrairement aux terroristes et autres pirates informatiques, légitiment leurs activités par une éthique particulière qui se négocie dans les différentes communautés de hackers. La base de cette éthique est la libre circulation de l'information, ainsi que la gratuité et l'échange réciproque de l'information. De ce fait, leurs activités sont bien souvent annoncées publiquement par les hackers eux-mêmes»[216].

Les *hackers* recherchent, avant tout, la libre circulation de l'information, tandis que les *crackers* recherchent la destruction et l'entrave de la circulation de l'information. Nous pourrions convenablement ôter les *hackers* de la thématique cyberdélinquance. Le choix des mots et sa compréhension au sein de l'espace public est important et peut entraîner des conséquences néfastes tant pour l'évolution d'Internet que pour la communauté des *hackers*. L'analyse des acteurs de la cyberdélinquance, « enfants » d'Internet, permet donc de mettre en avant le danger réel représenté pour le système d'information et de communication Internet à travers la dichotomie entre pirates informatiques et *hackers*.

Les mondes ne semblent pas construire de la même façon l'image sociale du pirate informatique. Les significations également attachées ne sont véritablement pas les mêmes. La source d'information, constituée par le corpus de la presse écrite étudié (voir partie II – II – 2)), diffuse l'existence d'un véritable phénomène de perturbations du système Internet. Ces actes sont d'origine humaine, les machines ne se perturbent pas entre elles, à moins d'avoir été programmées pour le faire. Ces auteurs d'infractions ont d'ailleurs été catégorisés voire hiérarchisés. De l'analyse des mondes de la cyberdélinquance, ressort-il des dénominations qui ne permettent pas d'obtenir une vision claire ? Se mélangent à la fois les pirates, les *hackers*, les *crackers*, car souvent pour caractériser les mêmes individus, le même objet…

[216] http://denislabrosse.net/articles/index.php.

L’amalgame a été et demeure général. Rares sont les personnes faisant aujourd’hui la distinction entre pirates informatiques et *hackers*. Pour aller au-delà des diverses significations « réductrices » n’est-il pas, finalement, plus judicieux de concevoir la possible réalité sociale de l’objet de recherche de manière constructiviste, en tenant compte de l’existence des significations des différents mondes de la « cyberdélinquance » et favoriser ainsi l’intégration, à terme, de ces dernières, permettant de formaliser la construction de la représentation sociale du pirate informatique ?

TROISIÈME PARTIE

Titre III - Approche intégrée des significations du pirate informatique : un ensemble d'images sociales

Nous avons vu qu'une image dominante du pirate informatique se dessine principalement *via* les médias, notamment en tant que vecteur d'information et de communication principal, eu égard, aussi, à la difficile pénétration du milieu « *underground* » des pirates informatiques. Notre approche vise à aller plus loin que cette vue singulière, en prenant en compte les significations de l'ensemble des mondes de la cyberdélinquance identifiés par notre étude. Ainsi, nous avons privilégié l'observation participante afin de rendre compte au mieux des significations de l'objet *via* ces mondes, à savoir les experts de la sécurité de l'information et les pirates informatiques eux-mêmes, après avoir spécifiquement traité de l'image médiatique dominante.

Pour ce faire, nous rendrons ainsi compte, dans un premier temps de la vision des experts de la lutte contre la cybercriminalité, avec pour terrain d'analyse la France (espace que nous avons longtemps investigué), données que nous pourrons corroborer avec notre vision experte de la sécurité de l'information au Grand-Duché de Luxembourg. Ensuite, nous établirons le rendu de son image sociale du point de vue même de l'acteur principal de la cyberdélinquance : le pirate informatique lui-même. Pour ce faire, nous montrerons l'intérêt de l'observation participante au cœur de ce milieu « *underground* » et ce qu'il est possible d'en retirer comme significations ; nous mettrons en regard de ces informations, le rendu même des individus qui y participent. Enfin, nous focaliserons notre propos sur un exemple précis d'intégration des significations de l'ensemble de notre recherche *via* la réalisation et la présentation du déroulement d'une étude récente que nous avons menée : « *Etude de la mise en place d'un observatoire des menaces IT au Grand-Duché de Luxembourg* ».

I – Significations du pirate informatique du point de vue de l'expertise sécurité

Afin de rendre compte de la vision des experts de la lutte contre la cybercriminalité, il nous est apparu important de considérer la France pour terrain d'analyse, à savoir, l'espace même que nous avons longtemps investigué, et sur lequel

repose notre socle d'expérience concrète quant à la cyberdélinquance. Dans un second temps, nous rendrons compte, en termes d'observation participante, de notre immersion professionnelle et du retour d'expérience au cœur du réseau « sécurité de l'information » luxembourgeois. Il sera ensuite intéressant de corroborer ces données entre elles pour dégager les significations globales du pirate informatique du point de vue de l'expertise sécurité.

1) Construction des significations des acteurs de la répression en France

En 2000, D. Dufresne et F. Latrive, auteurs de Pirates et flics du Net[217], avaient déjà souligné le nécessaire développement de la régulation face à la multiplication des affaires de cybercriminalité. « *Dans l'ombre, ils manipulent les fichiers informatiques comme personne. En solo, ou en bandes, ils traquent les failles qui leur permettront de fouiller dans tous les ordinateurs connectés. Ce sont les pirates informatiques, hackers, héros négatifs d'un monde du réseau-roi et du tout-électonique* ». L'oxymore « héros négatifs » montre que même pour des auteurs qui appellent à combattre cette délinquance, le cliché de « petit génie de l'informatique », de « héros » a la vie dure, puisqu'il faut y accoler l'adjectif « négatifs » pour les caractériser et en dévaloriser l'image.

Face au défi croissant de la cybercriminalité, les pouvoirs publics français se sont donc organisés et ont mis en place de nombreux organismes pour lutter contre ces formes nouvelles de délinquance. Le rapport sur la lutte contre la cybercriminalité présentée par T. Breton, remis au Ministre de l'Intérieur, le 25 février 2005, suivis des récents travaux de la « mission Lasbordes » (P. Lasbordes – Député), donnant lieu au rapport « *La sécurité des systèmes d'information – Un enjeu majeur pour la France* », daté du 26 novembre 2005, formalisent la prise en compte forte de la problématique des menaces TIC, traitée au plus haut niveau national.

Le « Rapport Lasbordes » est axé sur l'importance de la sécurité de l'information comme solution organisationnelle de contre-mesure aux menaces qui nous concernent ;

[217] *Pirates et Flics du Net*, (Dufresnes, Latrive, 2000).

ce rapport reprend les mêmes principales caractéristiques des acteurs de la problématique, que nous avons définies. Il propose six recommandations pour renforcer la position de l'Etat en matière de technologies de l'information et de la communication, et de SSI (Sécurité des Systèmes d'Information), et pour assurer la mise en œuvre opérationnelle des politiques et des décisions de l'Etat en matière de sécurité de l'information :

- Sensibiliser et former à la SSI.
- Responsabiliser les acteurs.
- Renforcer la politique de développement de technologies et de produits de SSI et définir une politique d'achat public en cohérence.
- Rendre accessible la SSI à toutes les entreprises.
- Accroître la mobilisation des moyens judiciaires.
- Assurer la sécurité de l'Etat et des infrastructures vitales.

En amont, le chantier sur la lutte contre la cybercriminalité caractérise plus particulièrement le domaine concerné par notre étude : « *La cybercriminalité est l'une des nouvelles formes de criminalité et de délinquance, dont les conséquences peuvent être particulièrement graves pour notre sécurité collective, pour notre économie et, bien sûr, pour les citoyens qui peuvent être personnellement atteints, dans leur personne, dans leur dignité et dans leur patrimoine* ». Le rapport reprend, pour tout acte de cybercriminalité : la dichotomie de l'ordinateur objet ou cible du crime ou délit, tel que nous l'avons décrit dans la première partie. La France a ainsi été un des premiers pays européens à constituer une force de Police visant à la répression de la criminalité informatique. Plusieurs entités ont depuis vu le jour dans ce pays où la cybercriminalité n'est pas considérée comme une fatalité. « *La police et la gendarmerie ont pris conscience des nouvelles menaces liées au cyberespace. Pour ces deux institutions, la cybercriminalité constitue déjà aujourd'hui et sera demain davantage encore un champ d'action renouvelé et ouvert* »[218]. L'entretien mené avec le lieutenant-colonel Joël Ferry (Officier représentant la Gendarmerie Nationale à la Direction des affaires criminelles et des grâces – Ministère de la Justice) a permis de mettre en évidence la matrice des services de répression du cybercrime en France (conférence CESCTI (27/11/2006 -

[218] *Chantier sur la lutte contre la cybercriminalité* (Breton, 2005).

« Cybercriminalité, comment la gendarmerie et la justice travaillent-elles sur le terrain ? ») – cf. annexe 8).

Le chantier sur la lutte contre la cybercriminalité propose de nombreuses mesures tel que :

- une meilleure connaissance statistique de la cybercriminalité,
- un doublement des capacités opérationnelles des services de police et de gendarmerie,
- un développement d'actions de formations communes,
- un renforcement des capacités juridiques d'investigation,
- un renforcement de la veille technologique et de la recherche et développement,
- un meilleur contrôle des contenus illicites,
- un renforcement de la protection des mineurs,
- le développement de la protection des mineurs,
- le développement d'une politique de prévention,
- la création d'un certificat citoyen.

Mais comment évaluer l'ampleur du phénomène criminel ? De quels outils d'évaluation dispose-t-on ? Comment mettre en perspective l'étude sur les représentations journalistiques de la cybercriminalité (la visibilité sociale que la presse donne du phénomène) avec la réalité des actes ? L'OCLCTIC collecte les données d'infractions numériques auprès des services de police et de gendarmerie. En 2003, nous l'avons vu, 1280 atteintes aux systèmes de traitement automatisé de données (piratage) sont relevées (+9 %), tandis que 792 diffusions de programmes informatiques permettant de fabriquer de fausses cartes bancaires sont identifiés (+149 %). Il faut spécifier que ces chiffres ne tiennent pas compte du « chiffre noir » du cybercrime (infractions commises mais non portées à la connaissance des forces de polices ou de gendarmerie) qui serait très important, par absence de relevé des incidents de sécurité, par négligence, par crainte des représailles, ou encore par crainte d'atteinte à l'image de marque.

Par ailleurs, deux rapports en lien avec la cybercriminalité sont attendus chaque année, en effet, ces derniers permettent de donner le « pouls » de cette problématique. Il s'agit du rapport « Computer Crime and Security Survey » du CSI/FBI (Computer Security Institute/Federal Bureau of Investigation (San Francisco Federal Bureau of

Investigation's Computer Intrusion Squad)) et du « Panorama Cybercrime » du CLUSIF (CLUb de la Sécurité de l'Information France). Ces deux rapports sont rendus publics chaque début d'année, en regard des activités de type « menaces IT » relevées l'année précédente (cf. première partie – III – 2)).

Notre étude menée pour l'INHES, a permis de rencontrer plusieurs responsables de la lutte contre la cybercriminalité, afin de tester auprès d'eux leurs perceptions du phénomène. C'est la synthèse de ces entretiens que nous proposons dans les pages qui suivent, sous forme d'abord d'une synthèse globale, puis d'une présentation synthétique des propos tenus par chacun. Afin, de relever des significations alors spécifiques quant à l'objet de recherche.

Synthèse des entretiens menés avec des représentants des organes répressifs en matière de cybercriminalité en France

Cinq officiers représentant les principaux organes de lutte contre la cybercriminalité en France ont pu être rencontrés, à travers l'étude menée. Deux d'entre eux font partie du système de la Police judiciaire (PJ) au sein du Ministère de l'Intérieur[219], deux autres représentent la Gendarmerie Nationale relevant du Ministère de la Défense[220] et un appartient au Secrétariat Général de la Défense Nationale[221]. Ainsi nous tenons à les remercier tout particulièrement pour leur disponibilité, pour leur accueil et pour les réponses détaillées qu'ils ont bien voulu fournir à toutes les questions constituées pour notre enquête.

Nous proposons une synthèse analytique des discours d'expertise tenus par ces fonctionnaires de haut niveau chargés de la conception et de la direction au sein de leurs services respectifs. L'appartenance des personnalités interviewées à des institutions

[219] C. Aghroum, Commissaire divisionnaire, Chef de service Office Central de Lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), Direction centrale de la police judiciaire (DCPJ) ; Yves Crespin, Commissaire principal, Chef de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), Direction de la Police judiciaire.

[220] J. Ferry, Lieutenant-colonel, Officier représentant la Gendarmerie nationale à la Direction des affaires criminelles et des grâces – Ministère de la Justice ; Eric Freyssinet, Chef d'escadron à la Direction générale de la Gendarmerie nationale, Service des opérations et de l'emploi, Sous-direction de la Police judiciaire, Bureau de la PJ, Cybercriminalité.

[221] S. Piallat, Commissaire divisionnaire, Direction centrale de la Sécurité des systèmes d'information (DCSSI), Secrétariat général de la Défense nationale.

distinctes et les méthodes de travail qui en découlent viennent expliquer les nuances sémantiques quant à l'approche conceptuelle du phénomène étudié. Les entretiens s'organisent autour de sept grands axes qui permettent de dégager des tendances. Existe-t-il une définition univoque de la cybercriminalité ? Est-il possible d'établir une typologie des cyberdélinquants ? Où en est-on en matière de coopération internationale concernant la lutte contre la cybercriminalité ? Peut-on parler de crime organisé en matière de cybercriminalité ? Quelles sont les méthodes de travail des différents services répressifs ? Quel est le taux de poursuite dans ce domaine en France ? Quels comportements et attitudes faut-il adopter face à cette menace ? Ce sont les questions qui nous préoccupent ici et auxquelles nous proposons de réfléchir.

- Vers *une* définition de la cybercriminalité ?

Il semble difficile de proposer une définition univoque de ce terme. Chaque officier offre une approche différente reflétant la réalité du travail qu'accomplissent les services concernés sur le terrain et les différences historiques et sociales dans la définition de leurs fonctions respectives au sein de l'appareil répressif français[222]. Ainsi, au niveau de la Gendarmerie nationale on évoque tantôt une subdivision de grandes catégories d'infractions commises au moyen TIC (Joël Ferry), tantôt une stratégie qu'il s'agit d'appliquer face à une typologie de comportements (Eric Freyssinet). À la P.J., certains experts défendent la dichotomie suivante : cybercriminalité (concernant l'attaque de l'ordinateur) versus cyberdélinquance (les technologies numériques sont utilisées comme moyen pour commettre d'autres actes graves (Yves Crespin, BEFTI). Un autre (Christian Aghroum, OCLCTIC) situe la notion de cybercriminalité à deux niveaux conceptuels distincts (au niveau mondial/à la française), et la présente comme un terme organisationnel permettant d'aborder les infractions liées aux TIC sous deux angles différents : les infractions générées par le système numérique ; l'utilisation des TIC pour faciliter une délinquance préexistante.

Enfin, signalons le cas particulier de la DCSSI (Stéphane Piallat) dont les

[222] *La police : une réalité plurielle* (Monjardet, Ocqueteau, 2004).

objectifs en matière de cybercrime diffèrent sensiblement de ceux poursuivis par les autres organes répressifs évoqués plus haut, où on ne cherche pas à définir ce qu'est la cybercriminalité. La connaissance des milieux des *hackers* et des cybercriminels ne préoccupe pas cette direction de la Défense nationale. L'objectif n'est pas de combattre la cybercriminalité, mais de mener une réflexion au niveau interministériel et de fournir des analyses concrètes en la matière concernant surtout le degré de complexité de l'outil informatique conçu et utilisé par les auteurs d'une éventuelle attaque.

- Est-il possible d'établir une typologie des cyberdélinquants ?

Selon les officiers, une typologie rendrait les délinquants sympathiques. De plus, on doute de l'utilité d'une telle démarche qui, en matière d'enquête, ne contribuerait pas à améliorer l'efficacité des interventions des services de police (Christian Aghroum). Il est impossible de créer des catégories dans ce domaine, car les personnes concernées viennent de tous les horizons. Le seul point commun entre les auteurs de ce type de crimes est leur accès à l'internet[223]. Malgré ces observations d'ordre pragmatique, une réflexion a abouti à des conclusions qui font l'unanimité. Le cybercriminel est défini comme quelqu'un de foncièrement individualiste, exprimant à travers ses actes une forte volonté de mise en valeur de soi. L'image du « techno héros », cet adolescent passionné d'informatique qui défie la sécurité des systèmes pour s'amuser n'est plus d'actualité. Ce profil existe toujours, mais il n'est pas le plus dangereux. En outre, la dichotomie classique « gentils *hackers* » vs « méchants *crackers* » est maintenant dépassée. En effet, on cherche simplement à savoir qui a commis le crime. Les officiers mettent tous en garde par rapport à une vision romanesque assez répandue au niveau du grand public concernant le cybercriminel. Une confusion se produit dans les représentations des victimes potentielles. On s'attache au côté mythique du phénomène sans se rendre compte de l'existence d'une véritable criminalité organisée en réseaux internationaux.

[223] Un raisonnement très intéressant quant à l'impossibilité de définir un profil type de ces « praticiens de l'informatique » « à cheval entre l'ordre et le désordre » est proposé par Breton, Bertrand et Heilmann (Breton P., Bertrand I., Heilmann E. : « *Entre l'ordre et le désordre des valeurs paradoxales du monde de l'informatique* », *Réseaux* n°48/1991, pp. 19-21).

- La dimension transfrontière du phénomène et la coopération internationale en matière de lutte contre la cybercriminalité

Le développement de l'internet a permis l'avènement d'un nouveau monde où il n'y a ni territoires, ni frontières. Nous nous trouvons désormais dans une logique mondialiste où un acte malveillant peut infecter le monde entier. Les réseaux organisés de cybercriminels font l'objet d'une attention particulière de la part des services d'enquête. Force est de le constater, la législation et l'approche de travail de la police judiciaire diffèrent d'un pays à l'autre ce qui peut limiter l'investigation. Néanmoins, on se félicite d'une très forte volonté de coopération internationale notamment avec les organes répressifs au sein des pays considérés comme des foyers potentiels ou réels de cybercriminalité. Pour les officiers français, les échanges avec des experts des différents pays européens rendent la recherche et la réflexion très intéressantes. Ce partage de connaissances et d'expérience permet également de mieux se connaître et de mieux se comprendre (Eric Freyssinet, Christian Aghroum). En revanche, on note une harmonisation insuffisante des pratiques judiciaires. Les raisons en sont d'ordre culturel et idéologique ce qui a des répercussions sur l'application des lois dans les différents pays du monde (Eric Freyssinet, Yves Crespin).

- Peut-on parler de crime organisé en matière de cybercriminalité ?

Actuellement, la cause primordiale des cyber-infractions est l'intérêt financier. Une délinquance organisée, au niveau international, arrive à manipuler d'importantes sommes d'argent. Le but des actions malveillantes est donc surtout lucratif et tend vers le crime organisé. Ce fait est la conséquence de l'effet pervers d'Internet qui devient de plus en plus rentable grâce à des schémas de plus en plus massifs (Eric Freyssinet). Les officiers que nous avons rencontrés évoquent l'existence d'une « *véritable criminalité organisée en réseaux internationaux* », et mentionnent ouvertement des « réseaux ou groupes organisés de cybercriminels » (Christian Aghroum, Joël Ferry). Cependant, il semblerait qu'en France, paradoxalement, ce ne soit pas encore perçu comme du crime organisé. Pourtant, il ne fait aucun doute que la cyberdélinquance se professionnalise et que le crime organisé l'a largement intégrée à ses pratiques. Pour exemple, le procureur

antimafia italien, Pier Luigi Vigna, a récemment souligné que le crime organisé « *se sert de managers et de cols blancs pour gérer les affaires illégales à travers le système informatique* ». En effet, les différents types de criminels n'agissent donc pas en autarcie, mais interagissent, multipliant les effets négatifs, illégaux et dangereux de la cyberdélinquance. Le récent rapport *Symantec* « *Le cybercrime s'organise pour vider les caisses* »[224] précise la généralisation de ce phénomène. Globalement ce rapport fait état d'une cyberdélinquance internationale de mieux en mieux organisée, les pirates informatiques « pensant réseau » avant tout, et coordonnant leurs actions. La cyberdélinquance s'organise donc, avec par exemple des outils de type « *crimewares* » (programmes informatiques conçus spécialement à des fins malveillantes), se professionnalise et perfectionne tout type d'escroquerie comme le vol d'informations sur Internet.

- Les méthodes de travail des organes répressifs

L'évolution rapide des TIC permet l'apparition de nouvelles formes de délinquance, mais les cyber-policiers travaillent toujours de manière traditionnelle : en considérant en premier lieu le facteur humain. Les objectifs des services de police sont de rester proches du terrain, de mener une enquête efficace et de vérifier toutes les hypothèses. Une enquête s'ouvre suite à une plainte déposée (dans la majorité des cas). Les données qu'on possède en terme de nombre d'enquêtes par an ne sont pas représentatives à cause notamment de la fameuse réticence des grandes entreprises de déposer des plaintes de peur de nuire à leur propre image. Quant aux PME, il est difficile d'évaluer la situation, car les petites structures possèdent rarement de serveurs spécialisés permettant de garder les traces d'une éventuelle intrusion. Une des solutions consisterait alors en l'initiative de susciter des plaintes auprès des entreprises sur la base de quelques indices précis.

Du point de vue du profil psychologique des délinquants, le travail de

[224] *Pirates, phishing virus...le cybercrime s'organise pour vider les caisses*, guide de la sécurité informatique, (Symantec, 2006).

« *profiling* » en matière de cybercrime semble être peu porteur et rejoint un fantasme des journalistes spécialisés. Le vrai *profiling* à la police est représenté par l'analyse criminelle effectuée de manière tactique et stratégique à la fois. Enfin, au niveau de la DCSSI, on ne s'intéresse pas au contenu mais aux moyens techniques mobilisés pour commettre un acte malveillant. On privilégie une approche très opérationnelle. On cherche à connaître le degré de complexité de l'outil informatique conçu et utilisé par les auteurs d'une attaque ce qui renseigne sur le degré d'expertise des criminels.

- Quelles sont les raisons du faible taux de poursuite en matière de cybercriminalité en France ?

Il est vrai qu'en France, le taux de poursuites en matière de cybercriminalité est très faible. Les raisons en sont multiples : faiblesse des plaintes déposées et enregistrées, difficultés rencontrées pour trouver les auteurs, éléments de preuve difficiles à obtenir, etc. En outre, les peines appliquées sont très faibles, car en France, la cybercriminalité n'est pas considérée comme du crime organisé, elle fait partie des infractions non violentes et des actes moins graves en tant qu'atteinte aux biens et non pas aux personnes. Contrairement aux États-Unis où les peines doivent être additionnées et sont généralement très lourdes, en France on est jugé pour l'ensemble des faits et ce de façon moins sévère. Pour approfondir la connaissance sur la cybercriminalité en France, il serait judicieux de contacter des magistrats qui pourraient émettre des avis intéressants en la matière.

- Une nécessité : changer les mentalités, les attitudes et les comportements …

a) du grand public face à la menace. Derrière cet outil puissant constitué par Internet générant un monde virtuel sans frontières, se cache parfois un risque réel. On insiste donc sur la nécessité absolue de faire prendre conscience d'une menace existante. L'état d'esprit de l'opinion publique doit évoluer (Christian Aghroum).

b) mais aussi des utilisateurs d'Internet. En effet, on doit faire face à plusieurs problèmes liés au développement de l'Internet : les comportements nuisibles et le plaisir de nuire encouragés par la dématérialisation des faits, le sentiment d'impunité de ceux qui nuisent, etc. Un travail de fond, d'éducation et de culture civique doit être entrepris pour arriver à changer les mentalités. Un acte d'incivilité ou une imprudence risquent d'avoir des conséquences très lourdes (Yves Crespin).

Certains services en France (BEFTI) ont justement comme tâche, entre autres missions d'enquête et d'assistance, la sensibilisation concernant les failles techniques et humaines dans l'utilisation des réseaux numériques au sein des entreprises (cible principale des cyber-attaques). L'accent est mis sur la gestion des ressources humaines et sur leur importance pour la sécurité de l'entreprise. Le facteur humain est la première cause de la fraude informatique. L'équilibre parfait entre la technique et l'humain est à la base du bon fonctionnement des entreprises.

2) Immersion et retour d'expérience au cœur du réseau « sécurité de l'information » luxembourgeois

Différents mandats « sécurité de l'information » nous ont permis d'observer de près le réseau adapté au Grand-Duché de Luxembourg, et ainsi valider la génération de la signification principale de l'acteur de notre propos, à savoir le pirate informatique représenté comme une menace réelle, et imposant en réaction des contre-mesures adaptées.

Les différents mandats qui ont été et sont encore exercés à ce jour sont les suivants :

- *Head of Delegation* Luxembourg ISO/SC27 (« Techniques de Sécurité des Technologies de l'Information »).

- Membre du Conseil d'Administration (Vice-Président) ANSIL (Association de Normalisation pour la Société de l'Information Luxembourg).

- Président CNLSI (Comité de Normalisation Luxembourg pour la Sécurité de l'Information).

- Membre du Conseil d'Administration (Administrateur) et du Bureau CLUSSIL (CLUb de la Sécurité des Systèmes d'Information Luxembourg).

- Chargé de cours pour le Master « Sécurité des Systèmes d'Information et de la Communication » depuis 2003 (Responsable Module 48 heures (Méthodologies avancées de la Sécurité) – Université Paul Verlaine de Metz (F-57).

- Chargé de cours pour le Master « Management de la Sécurité des Systèmes d'Information» (depuis décembre 2006) – Université de Luxembourg (G-D de Luxembourg).

Mais le cœur de notre immersion, dans le domaine de la sécurité de l'information et de la communication, est surtout représenté, de 2004 à 2007 (février), au niveau du Centre de Recherche Public Henri Tudor (Centre d'Innovation par les Technologies de l'Information - CITI), par la Plate-Forme d'Innovation « Sécurité des Systèmes d'Information » (PFI Sécurité). En effet, l'ensemble des projets de Recherche et Développement (R&D), ayant pour thématique la sécurité de l'information, au CRP Henri Tudor, a été regroupé au cœur d'un portefeuille particulier, la PFI Sécurité, organe de *management* centralisé. L'intérêt d'un tel regroupement réside dans la haute interaction des projets de R&D traitant des diverses problématiques de la sécurité de l'information, et visant dans ce domaine la production de valeur ajoutée pour le Grand-Duché de Luxembourg. La PFI Sécurité a, en effet, pour objectif la synergie des actions entreprises, la définition de nouveaux axes de travail, de trajectoires d'innovation, de lignes de produits, mais aussi et surtout la suppression de redondances possibles en la matière. La PFI Sécurité se mobilise ainsi, au jour le jour, *via* des relations constantes entre les Chefs et Gestionnaires de chaque projet de sécurité, aux fins de veiller au bon ordonnancement de la stratégie planifiée. Une logique d'innovation anime la PFI Sécurité, *via* des objectifs stratégiques et des objectifs d'impacts définis clairement. Ses objectifs stratégiques sont les suivants :

- identifier et promouvoir le besoin en sécurité des SI auprès des entreprises (particulièrement les PME), des citoyens et du secteur public,
- développer le marché des services autour de la sécurité dans le conseil informatique en optimisant la rencontre avec les besoins des demandeurs,
- investiguer les modèles socio-économiques, juridiques et organisationnels nécessaires à l'adoption de nouvelles technologies de sécurité,

- mettre en contexte des référentiels de sécurité adaptés aux réalités de la Grande Région.

Ses objectifs d'impacts se déclinent ainsi :

- augmenter le nombre et la formation des Responsables de Sécurité des SI (RSSI) dans les entreprises et les services publics,
- augmenter la définition et le déploiement de politiques sécurité dans les entreprises et les administrations,
- augmenter la sensibilisation à la sécurité des usagers « faibles »,
- augmenter en termes quantitatif et qualitatif l'offre de services privés,
- développer une mobilisation concertée des acteurs nationaux pour innover dans cette matière,
- développer et déployer des connaissances, des compétences et un partenariat européen en la matière.

Dans cette logique, la PFI Sécurité définit également des « produits » sécurité, en devenir, qui suivent une marge de développement en lien avec la progression de la recherche sur chaque projet, mais qui tient compte aussi de la réalité de terrain, à savoir les besoins relevés, mais aussi les développements politiques sécuritaires en cours menés au Grand-Duché de Luxembourg, notamment *via* une forte collaboration avec le Ministère de l'Ėconomie et du Commerce extérieur. Ce ministère développe, depuis 2004, le Plan Directeur National de la Sécurité des Réseaux. Un de ses premiers éléments concrets peut être visible *via* cette fenêtre numérique : http://www.cases.public.lu (CASES : *Cyberworld Awareness & Security Enhancement Structure* - Portail de la sécurité de l'information du Grand-Duché de Luxembourg). Pour exemple de produits, la PFI Sécurité veille actuellement à la production et au test d'une démarche complète de préparation à la certification ISO 27001, dans le contexte d'une petite structure économique au Grand-Duché de Luxembourg. Nous pouvons encore citer, par exemple, le développement d'un module *e-learning* « sécurité » développé pour la structure nationale CASES, et la production d'un prototype, en cours de validation, relatif à la thématique de l'« *Identity Management* ».

Aux fins de rejoindre les besoins et exigences du marché, ainsi que les objectifs définis, la PFI Sécurité s'est également dotée d'un Comité d'Accompagnement (CAP

PFI). Ce dernier réunit chaque trimestre des partenaires stratégiques de premier choix, qui veillent à la production scientifique, en la matière et en ligne, avec les axes de développement nécessaires pour le Grand-Duché de Luxembourg. Ses membres sont les suivants : Association de Normalisation pour la Société de l'Information (ANSIL), Ministère de l'Economie et du Commerce Extérieur (CASES), Centre Informatique de l'Etat, *Computer Security Research and Response Team* (CSRRT), Commission de Surveillance du Secteur Financier (CSSF), Club de la Sécurité des Systèmes d'Information du Luxembourg (CLUSSIL), Université du Luxembourg (UL), Commission Nationale pour la Protection des Données (CNPD), Chambre des Métiers, Chambre de Commerce, Luxinnovation, Fédération des Industriels Luxembourgeois (FEDIL), Association des Professionnels de la Société de l'Information (APSI), et le Centre de Recherche Public Gabriel Lippmann.

Plusieurs recommandations sont déterminées lors des réunions du CAP PFI Sécurité ; citons, par exemple, la décision de mener une « *Etude de faisabilité de mise en place d'un observatoire des menaces IT au Grand-Duché de Luxembourg* ». Sujet phare qui montre l'implication des différents protagonistes cités *supra* et qui ont décidé, par consensus, la réalisation de cette étude, en regard de leur expérience de la probable nécessité de mettre en place un observatoire de ce type, par rapport aux nombreuses menaces existantes sur le terrain numérique. Nous avions mené les discussions relatives à la mesure de ce besoin, et les acteurs du CAP étaient clairs quant à la menace représentée par le pirate informatique, et les dégâts engendrés par la cybercriminalité. Ce qui était récurrent dans le discours : les références aux statistiques et études relevant de ce domaine (CSI/FBI, CLUSIF, *Symantec*… (Cf. première partie – III – 2)), et surtout l'incompréhension face au fait que le G-D de Luxembourg ne relève pas d'incidents numérique de la sorte au plan national, alors même que des relevés statistiques montrent clairement le G-D de Luxembourg comme un pays attaquant (souvent il s'agit d'une machine elle-même victime d'un piratage informatique en provenance d'une autre machine, et souvent de l'étranger). Les résultats de cette étude furent présentés en décembre 2006, au CAP PFI Sécurité (voir troisième partie – III). Il est à noter l'importance cruciale de cette étude que nous avons menée et qui répond à un double

besoin à la fois national, et en tant que mesure de terrain des représentations du pirate informatique par les experts de la sécurité de l'information et de la communication.

Cette étude et la majorité de notre travail de recherche, ont été principalement exécutées au cœur du projet R2SIC (*Recherche en Sécurité des Systèmes d'Information et de Communication*) : Projet de Recherche – Partenaire : Ministère de l'Economie et du Commerce extérieur, que nous avons co-rédigé. L'objectif fut notamment d'analyser les comportements et menaces de piratage informatique, d'identifier les vulnérabilités au niveau des PME, de produire un référentiel d'évaluation de la maturité de la sécurité de l'information en PME, ainsi qu'une démarche *e-learning* associée. De plus, récemment des résultats de projets de recherche en cours sur les domaines de la prospective économique en terme de technologies, mais aussi de métiers de la sécurité, ont également été présentés en CAP PFI Sécurité. *Via* ce CAP, la PFI Sécurité tient notamment compte, pour son développement, du riche tissu associatif luxembourgeois de la sécurité, très homogène, et de ses conseils avisés (CLUSSIL, ANSIL (CNLSI), CSRRT…). Ce cadre « transpire » et « vit » les interactions fortes entre les différents membres de la sécurité de l'information au Grand-Duché de Luxembourg. De plus, généralement, les significations attachées à la réalité des attaques techniques s'affichent par consensus au sein de la PFI Sécurité.

De l'expertise de la réalité des attaques techniques

Après avoir montré l'évidence de la réalité quantitative de la cyberdélinquance, notamment dans son acception généralisée de menace préjudiciable, comme un domaine lié au domaine du risque numérique (il apparaît comme preuve d'une évidence contextuelle du domaine), la pertinence des attaques techniques, tant au niveau des méthodes formelles, que des pratiques courantes et récentes de cyberdélinquance est établie. Cependant, identifier les risques ne suffit pas, ainsi un arsenal de méthodes et, plus encore, de concepts, prétend en contraindre ou en supprimer les effets[225].

[225] 2006 : Jean-Philippe Humbert, Nicolas Mayer : « *La gestion des risques pour les systèmes d'information* » - MISC Magazine N°24 – Avril-Mai 2006. France.

2006 : Francine Herrmann, Jean-Philippe Humbert, Nicolas Mayer « *Gestion de la sécurité : les défis* », Mag SECURS, 12, Juin-Juil.-Août 2006, pp. 18-23, France.

En matière de conception, les méthodes de prévention des risques sont relativement formelles. Elles sont destinées à concevoir le produit ou le service pour minimiser l'occurrence des risques susceptibles d'apparaître. Les techniques reposent sur des solutions variées, allant de la réduction du risque par tous les moyens, jusqu'à son contrôle par une conception d'architecture des systèmes qui tolère certaines défaillances (système tolérant aux fautes).

Cependant, nul système n'est parfait, parfois les mécanismes de sécurité permettant de prévenir un risque peuvent aussi contenir des vulnérabilités (*firewall*, routeurs, etc…). Dans le domaine du risque organisationnel (au sens de la mise en place de procédures de gestion globale qui répondent à une politique), les méthodes utilisables en prévention relèvent plutôt de concepts, voire de champs théoriques, certes heuristiques mais reposant sur des outils plutôt peu formalisés.

J. Reason (1993) suggère l'idée de « *défense en profondeur* », le système socio-technique est comparé à une série de couches d'acteurs contribuant à la sécurité finale de ce système et incluant les concepteurs, les « règlementeurs », l'étage directoral de l'entreprise et l'ensemble des exécutants de première ligne. La sécurité résulte de l'empilement des couches (des défenses en profondeur) ; aucune d'entre elles ne peut assurer seule la sécurité, mais chacune protège des défaillances générées par les autres couches. G. Rochlin (1993) propose un autre modèle-cadre très connu : il s'agit de la notion d'organisation sûre – *high reliable organization*. L'organisation est considérée comme sûre quand elle respecte plusieurs critères de base : partage des motivations de sécurité (culture de sécurité), flexibilité des décisions, fonctionnement collégial, recherche active des défaillances, compétence technique et efficacité professionnelle. Rappelant et s'inspirant de ce contexte, une initiative intéressante est à retenir à l'échelle européenne à savoir la réalisation du réseau de prévention aux risques informatiques dénommé CASES (*Cyberworld Awareness and Security Enhancement Structure*). CASES est une initiative de plusieurs pays européens qui prévoit la mise en place d'un réseau opérant dans le domaine de la prévention et de la protection. Le réseau CASES va travailler conformément aux lignes directrices de la *Cyber Security Task Force* (organe de sécurité de l'Union Européenne) dans le domaine de la protection et de la prévention. Le but est d'augmenter la confiance et d'établir une culture de sécurité nécessaire au

développement des N.T.I.C. dans un cadre sécurisé. CASES devra faire la promotion de méthodes d'analyse des risques telle que par exemple la méthode EBIOS[226] (*Expression des Besoins et Identification des Objectifs de Sécurité*) qui est une méthode publiée par la Direction Centrale de la Sécurité des Systèmes d'Information (D.C.S.S.I.) et qui permet, lors de la phase de spécification de besoins d'un système, de les identifier dans la thématique sécurité. Les étapes empiriques sont les suivantes : étude du contexte, expression des besoins de sécurité, étude des risques, identification des objectifs de sécurité, puis des exigences de sécurité. Cette méthode est très utilisée au sein de l'Union européenne et permet surtout aux divers organismes qui l'utilisent de rédiger une politique de sécurité des systèmes d'information rationnelle et adaptée à leurs besoins. Encore une fois la base de données, concernant les menaces pouvant s'appliquer aux systèmes d'information et de communication, met en lumière les *hackers*.

Les méthodes d'analyses des risques informatiques sont apparues vers 1984, date à laquelle les experts SSIC ont perçu la nécessité d'un travail méthodologique. Elles ont pour objet, l'étude, l'évaluation et la réduction des risques liés à l'utilisation de l'informatique. D'autres méthodes que EBIOS sont utilisées par divers organismes ; citons MEHARI, MELISA ou encore MARION, qui chacune utilise une base de connaissances où les pirates informatiques sont clairement identifiés en tant que menaces pour les systèmes d'information et de communication.

Méthode exploratoire et concaténation des significations « expertes » en regard des menaces IT en général et du pirate informatique en particulier

La catégorisation des menaces, permet d'identifier de manière théorique toutes les possibilités pouvant atteindre un utilisateur, et pouvant être véritablement de nature diverse (pas uniquement en provenance de l'univers IT). Dans le but d'en vérifier les aspects pratiques, il convient dès lors de détailler leur réalité technique, notamment *via* les principaux recensements connus de cette activité. Ce travail d'investigation des

[226] 2006 : Jean-Philippe Humbert, Nicolas Mayer : « *La méthode de gestion des Risques de sécurité EBIOS* » - MISC Magazine N°27 – Septembre-Octobre 2006. France.

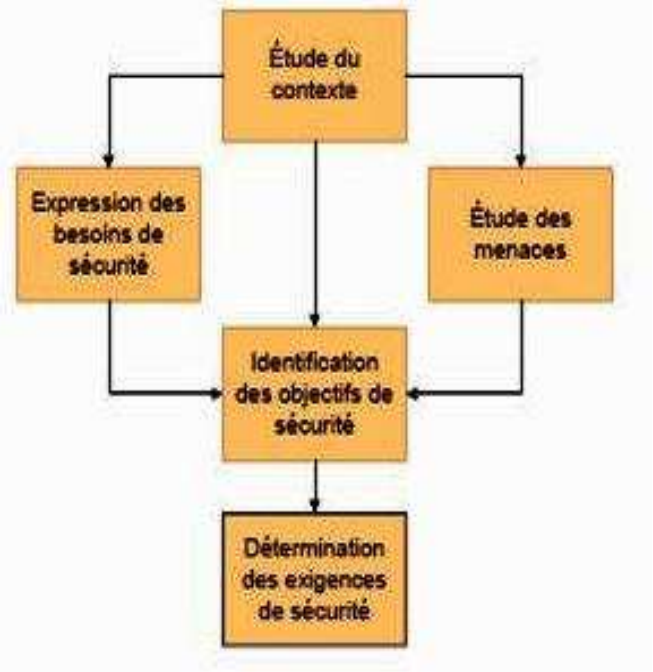
menaces TIC vues *via* l'angle de l'expertise sécurité des systèmes de l'information et de la communication, va permettre de rendre compte du relevé des significations des menaces réelles que représente le pirate informatique, selon ce monde.

Au coeur des méthodologies d'analyse de risques

Actuellement, il existe de nombreuses méthodologies d'analyse de risques qui se dégagent quant au niveau de maturité atteint et quant à leur fréquence d'utilisation. Nous détaillerons EBIOS qui spécifiquement prend en compte de manière détaillée et particulière l'élément menaçant à éviter.

EBIOS

La Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI), qui dépend du SGDN (Secrétariat Général de la Défense Nationale) en France, a publié une série de guides méthodologiques relatifs à la SSI, dont fait partie la méthode d'analyse de risques EBIOS. Cette méthode permet d'apprécier et de traiter les risques relatifs à la SSIC, et de communiquer à leur sujet au sein de l'organisation et vis-à-vis de ses partenaires. Son principe est le suivant : identifier les biens (informations) et services à protéger, analyser les conséquences d'incidents sur ces biens et services, analyser parallèlement les vulnérabilités des architectures techniques pour choisir les objectifs de sécurité appropriés afin de minimiser les risques. Elle présente une approche technique et une approche organisationnelle de la sécurité d'un système d'information. Elle permet d'en exprimer les besoins de sécurité. Le schéma suivant présente l'ensemble des étapes d'une démarche EBIOS :



- Figure 3. La démarche d'analyse de risques EBIOS

La méthodologie déployée par EBIOS repose sur la confiance que l'entreprise peut avoir dans la sécurisation de son système d'information. Cette démarche peut se résumer en cinq points :

1. **L'étude du contexte :**

Un système d'information repose sur des éléments essentiels, fonctions et informations, qui constituent la valeur du système d'information pour l'organisme. Ces éléments sont liés à un ensemble d'entités de différents types : matériels, logiciels, réseaux, organisations, personnels et sites.

2. **L'expression des besoins de sécurité :**

Chaque élément essentiel a un besoin de sécurité. Ce besoin s'exprime selon différents critères tels que la disponibilité, l'intégrité et la confidentialité. Si ce besoin n'est pas respecté, l'organisme en sera impacté. Cet impact peut revêtir différentes

formes : pertes financières, atteinte au bon déroulement des activités, atteinte à l'image de marque, atteinte à la sécurité des personnels, pollution ...

3. L'étude des risques :

Chaque organisme est exposé à diverses menaces, de par son environnement naturel, sa culture, son image, son domaine... Une menace peut être caractérisée selon son type (naturel, humain ou environnemental) et selon sa cause (accidentelle ou délibérée). Elle peut employer diverses méthodes d'attaque qu'il convient alors d'identifier. Une méthode d'attaque est caractérisée par les critères de sécurité (disponibilité, intégrité, confidentialité...) qu'elle peut affecter et par les éléments menaçants susceptibles de l'utiliser. Chaque entité possède des vulnérabilités qui pourront être exploitées par les éléments menaçants selon chaque méthode d'attaque.

4. L'identification des objectifs de sécurité :

On détermine comment les éléments essentiels peuvent être affectés par les éléments menaçants et par leurs méthodes d'attaque : il s'agit du risque. Le risque représente un sinistre possible. Un élément menaçant peut affecter des éléments essentiels en exploitant les vulnérabilités des entités sur lesquelles ils reposent avec une méthode d'attaque particulière. Les objectifs de sécurité consistent à couvrir les vulnérabilités. Il est inutile de protéger ce qui n'est pas exposé. On note aussi que plus le potentiel d'attaque est important et plus le niveau des objectifs de sécurité sera important. Ces objectifs constituent ainsi un très bon cahier des charges de la SSI.

5. La détermination des exigences de sécurité :

L'équipe de mise en oeuvre de la démarche doit spécifier les fonctionnalités de sécurité attendues. Elle démontre la couverture des objectifs par ces exigences fonctionnelles. Elle doit enfin spécifier les exigences d'assurance qui permettent d'obtenir le niveau de confiance requis, pour le démontrer. Au cœur de l'étude des risques, nous nous intéresserons dans le cadre de notre projet plus particulièrement à

l'étude des menaces proposées par EBIOS et à sa base de menaces. Les menaces pertinentes pour le système concerné sont sélectionnées à partir de la liste des menaces génériques proposée dans la base de connaissance. La liste des menaces proposée dans la méthode EBIOS est composée de dix rubriques génériques pouvant toucher tout système d'information. Les nouveaux risques susceptibles d'apparaître pouvant être couverts par l'une ou l'autre des rubriques existantes. Une menace est retenue dans la mesure où sa réalisation a un impact sur le système-cible. L'évaluation s'effectue en proposant le libellé exact de la menace identifiée, le vecteur de cette menace (informatique, physique, personnel, etc.…), la gravité qu'elle génère en terme de Disponibilité, d'Intégrité, de Confidentialité, la nature de l'acte de la menace (malveillance, intentionnel, recherche de renseignement…) ainsi que les commentaires éventuels. EBIOS affecte à l'impact de la menace une valeur de sévérité indépendante de la sensibilité des informations et des fonctions. La base de connaissance fournie par le logiciel d'assistance à la méthode est modifiable en fonction des besoins de l'utilisateur. Elle permet la modification de la base existante, mais en plus offre la possibilité de créer sa propre base de connaissances. Le logiciel dispose pour ce faire d'une interface d'édition de base. Il permet, au cours de la création, ou de l' « implémentation » d'une base existante, de vérifier la cohérence de la base et de déterminer les erreurs éventuelles de conception.

EBIOS : Méthodes d'attaque et éléments menaçants génériques

EBIOS présente des méthodes d'attaque qui sont classées selon un thème représentatif (elles pourraient néanmoins être placées dans plusieurs thèmes).[227]

Thème 1 – Sinistres physiques

1- INCENDIE
2- DÉGÂTS DES EAUX
3- POLLUTION

[227] EBIOS – Section 4 – Outillage pour l'appréciation des risques SSI (Version 2 – 05 février 2004).

4- SINISTRE MAJEUR
5- DESTRUCTION DE MATÉRIELS OU DE SUPPORTS

Thème 2 – Événements naturels

6- PHÉNOMÈNE CLIMATIQUE
7- PHÉNOMÈNE SISMIQUE
8- PHÉNOMÈNE VOLCANIQUE
9- PHÉNOMÈNE MÉTÉOROLOGIQUE
10- CRUE

Thème 3 – Perte de services essentiels

11- DÉFAILLANCE DE LA CLIMATISATION
12- PERTE D'ALIMENTATION ÉNERGÉTIQUE
13- PERTE DES MOYENS DE TÉLÉCOMMUNICATIONS

Thème 4 – Perturbations dues aux rayonnements

14- RAYONNEMENTS ÉLECTROMAGNÉTIQUES
15- RAYONNEMENTS THERMIQUES
16- IMPULSIONS ÉLECTROMAGNÉTIQUES (IEM)

Thème 5 – Compromission des informations

17- INTERCEPTION DE SIGNAUX PARASITES COMPROMETTANTS
18- ESPIONNAGE À DISTANCE
19- ÉCOUTE PASSIVE
20- VOL DE SUPPORTS OU DE DOCUMENTS
21- VOL DE MATÉRIELS
22- RÉCUPÉRATION DE SUPPORTS RECYCLÉS OU MIS AU REBUS

23- DIVULGATION

24- INFORMATIONS SANS GARANTIE DE L'ORIGINE

25- PIÉGEAGE DU MATÉRIEL

26- PIÉGEAGE DU LOGICIEL

27- GÉOLOCALISATION

Thème 6 – Défaillances techniques

28- PANNE MATÉRIELLE

29- DYSFONCTIONNEMENT DU MATÉRIEL

30- SATURATION DU SYSTÈME INFORMATIQUE

31- DYSFONCTIONNEMENT LOGICIEL

32- ATTEINTE À LA MAINTENABILITÉ DU SYSTÈME D'INFORMATION

Thème 7 – Actions illicites

33- UTILISATION ILLICITE DES MATÉRIELS

34- COPIE FRAUDULEUSE DE LOGICIELS

35- UTILISATION DE LOGICIELS CONTREFAITS OU COPIÉS

36- ALTÉRATION DES DONNÉES

37-TRAITEMENT ILLICITE DES DONNÉES

Thème 8 – Compromission des fonctions

38- ERREUR D'UTILISATION

39- ABUS DE DROIT

40- USURPATION DE DROIT

41- RENIEMENT D'ACTIONS

42- ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL

Les méthodes d'attaque sont décrites en fonction des éléments menaçants pouvant les exploiter. Des thèmes développés, il ressort des menaces de types naturels, techniques et humains (Non intentionnels, intentionnels. Cf les thèmes 5, 7 et 8 qualifiant le contexte menaçant de notre objet de recherche).

De nombreuses autres méthodes ont pu être investiguées lors de notre travail de recherche (MEHARI (Méthode Harmonisée d'Analyse de Risques), BSI - *IT Baseline Protection Manual*, NIST – *Risk Management Guide for Information Technology systems*, ISO/IEC FCD 27005…), à ce titre, pour focaliser plus en avant la perception des menaces TIC, par le monde de la sécurité, nous avons repris une synthèse de ces diverses considérations/classifications du monde des experts SSIC, sous forme de tableau.

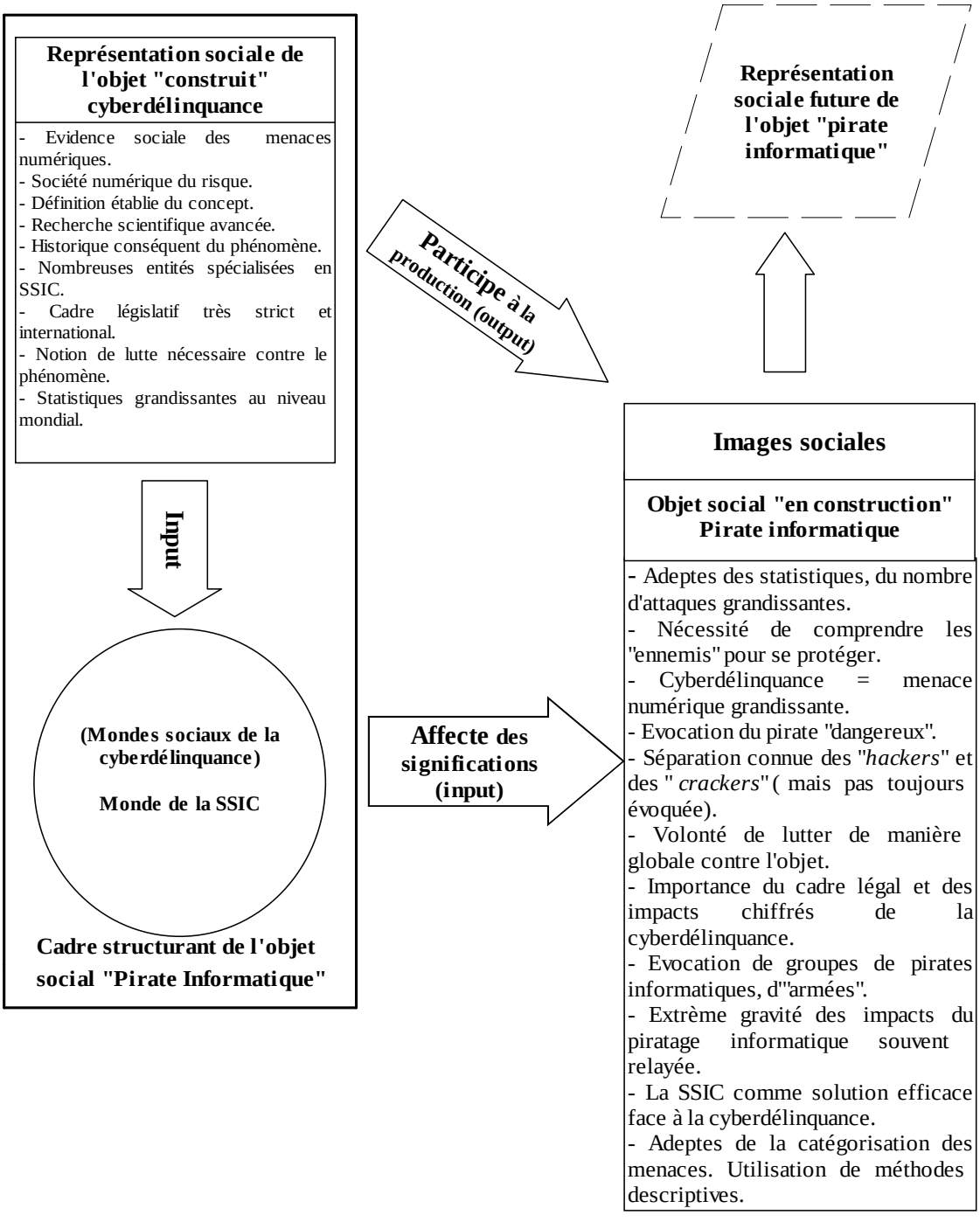
Tableau de synthèse

MENACES DES SYSTEMES D'INFORMATION ET DE LA COMMUNICATION	***INTENTIONNELLES***	***NON INTENTIONNELLES***
NATURELLES & ENVIRONNEMENTALES	(Rares) – Provoquées - Incendie - Dégâts des eaux - Sinistre majeur	- Pollution - Sinistre majeur - Phénomène climatique - Phénomène sismique - Phénomène volcanique - Phénomène météorologique - Crue
TECHNIQUES	Agents techniques : - Chevaux de Troie - Virus - Spywares - Adwares - Rayonnements électromagnétiques - Rayonnements thermiques - Impulsions électromagnétiques (IEM) - Interception de signaux parasites compromettants	Faiblesses : - Défaillance de climatisation - Perte d'alimentation énergétique - Perte des moyens de télécommunication - Panne matérielle - Dysfonctionnement du matériel - Saturation du système informatique. - Dysfonctionnement logiciel.

	- Espionnage à distance - Ecoute passive - Saturation du système informatique.	
HUMAINES	Agents humains : - Pirates informatiques - Vol de support ou de documents - Vols de matériels - Récupération de supports recyclés ou mis au rebus - Divulgation - Espionnage industriel - Espionnage économique - Fraude financière. - Piégeage du matériel - Piégeage du logiciel - Géolocalisation - Saturation du système informatique - Atteinte à la disponibilité du système d'information - Utilisation illicite des matériels - Copie frauduleuse de logiciels - Utilisation de logiciels contrefaits ou copiés - Altération des données - Traitement illicite des données. - Abus de droit - Usurpation de droit - Atteinte à la disponibilité du personnel - Atteinte à la vie privée.	Manquements : - Erreurs (d'utilisation) - Omission

- Tableau 17. Tableau récapitulatif des menaces à la SSIC en regard des bases de menaces des différents référentiels analysés – Compilation des menaces.

- Figure 4. Modélisation graphique de la représentation du pirate informatique par le monde de la sécurité des systèmes d'information



Elément périphérique de la représentation sociale de la cyberdélinquance

II – Construction de l'auto-signification du « pirate informatique »

Nous l'avons vu, le rôle des médias est décisif dans l'évaluation des représentations sociales de la cyberdélinquance et des images sociales du pirate informatique. Le rendu médiatique est souvent prédominant, par manque de possibilité d'intégrer le monde social des pirates informatiques. Pourtant, il est primordial d'en considérer l'importance dans le contexte social de production des images sociales associées. Mais, d'autre part, les tentatives effectuées pour pénétrer directement ce milieu, en qualité d'enquêteur sociologique, se sont révélées peu fructueuses, voire impossible par expérience et reconnaissance dans le milieu, mais aussi par obligation professionnelle. De facto, nous avons pu privilégier la description détaillée des rassemblements organisés par cette communauté et disposer de quelques témoignages parcellaires. Ce qui constitue la jonction du monde « *underground* » et le cadre de ce monde social.

1) L'impossible pénétration sociologique du milieu

En proie à une méfiance qui s'est rapidement transformée en une hostilité, nous n'avons guère pu mener largement le programme d'observation qui était le nôtre. Le monde social de la cybercriminalité se rend volontairement difficilement perceptible, se voulant sciemment situé hors de la société traditionnelle. Il repose sur les principes dits de la « TAZ »[228] (« *Temporary Autonomous Zone* » ou « Zone Autonome Temporaire »). La « TAZ » ne se manifeste qu'à celui qui a reçu l'autorisation de la voir, selon H. Bey qui l'identifie ainsi : « *[…] apparaissant-disparaissant pour mieux échapper aux arpenteurs de l'État, elle occupe provisoirement un territoire, dans l'espace, le temps ou l'imaginaire, et se dissout dès lors qu'elle est répertoriée. La TAZ fuit les TAZs affichées, les espaces « concédés » à la liberté : elle prend d'assaut, et retourne à l'invisible. […] La TAZ ne peut exister qu'en préservant un certain anonymat* ».

[228] Hakim Bey, 1991, « *T.A.Z. The Temporary Autonomous Zone. Ontological Anarchy, Poetic Terrorism* », *Autonomedia*.

Nous sommes, par conséquent désarmés face aux « utopies pirates » que ce soit celles du XVIIIème siècle, ou bien les acteurs actuels de la cybercriminalité. Aujourd'hui, ces derniers reposent totalement sur les principes de la « TAZ ». Le monde social de la cybercriminalité est anonyme, rempli d'acronymes et de pseudonymes. Les véritables cybercriminels vivent en marge de la société, selon les principes des hors-la-loi, ce qui fait partie de leur folklore identitaire, et ne s'affichent donc pas en tant que tels.

Pour comprendre les valeurs propres au monde social des « pirates informatiques », « *underground* » par essence, donc quasiment intouchables, il s'avère donc impossible d'adopter une véritable démarche compréhensive. S'inspirer des méthodes pionnières de l'École de Chicago[229], en intégrant le milieu « *underground* », en y passant énormément de temps, tout en franchissant la frontière de la légalité, s'est rapidement avéré hors de portée de cette étude. Nous ne pouvons le faire, à la fois parce qu'il faut beaucoup de temps pour être admis dans le cercle, qu'il faut manifestement apporter des preuves de ses compétences en réalisant quelques « coups », autant d'étapes infranchissables pour des raisons compréhensibles d'obligations professionnelles et morales. Autant s'intégrer dans les salles de boxe des noirs américains, comme l'a fait le sociologue Loïc Wacquant,[230] reste possible, même si ce n'est pas sans difficulté, autant recueillir les témoignages de « blousons noirs » comme a su le faire le sociologue Émile Copfermann reste du domaine du faisable,[231] autant le coût d'accès au monde des cybercriminels est exorbitant et échappe du coup à l'enquête sociologique traditionnelle.

Bien sûr les *hackers* savent s'organiser et se retrouver dans des manifestations à caractère public (ce qui ne veut pas dire tout public). Pour autant cela ne suffit pas à pouvoir pénétrer le milieu. Il faut d'autres moyens. C'est ce que semblent d'ailleurs avoir tenté les services de renseignement français, prouvant que seules des méthodes dignes de l'espionnage permettaient vraiment d'approcher les responsables actifs. Un *Chaos Computer Club* français est apparu à la fin des années 1980. À sa tête, J-B Condat, jeune informaticien français. Il s'avéra par la suite que ce club avait été monté de toutes pièces

[229] *L'Ecole de Chicago* (Coulon, 2002).
[230] *Corps et âme : carnets ethnographiques d'un apprenti boxeur* (Wacquant, 2002).
[231] *La génération des blousons noirs. Problèmes de la jeunesse française* (Copfermann, 2003).

par la DST (selon Jean-Bernard Condat lui-même - SIC) aux fins de constituer un fichier des pirates informatiques français. Cette tentative montre que pénétrer ce milieu n'est pas chose facile, et que les techniques d'infiltration individuelles habituelles ne peuvent suffire, même aux yeux des services de renseignement français.

Obtenir des informations sans être reconnu dans ce milieu en tant que « membre », est une mission quasi impossible, même pour des scientifiques, ce que note fort bien Max Kilger[232], psychologue au sein de *HoneyNet Project* (*Projet HoneyNet*, États-Unis) : « *Même un sociologue bien entraîné rencontrera de grandes difficultés pour enquêter sur la communauté des « hackers* ». Vous ne pouvez pas simplement allez à la rencontre de membres d'un groupe de *black-hat* et annoncer : « *Salut, je suis sociologue. Puis-je venir traîner avec vous les gars ?* » En fait, vous pourriez, mais vous obtiendriez probablement le même traitement reçu par un journaliste malchanceux, vu par un des auteurs de ce livre, lors d'une convention de « *hackers* » quand il s'est assis à une table complète de véritables et sérieux « *hackers* » et a posé la question : « « *Salut, avez-vous « hacké » de bonnes machines, récemment?* ». *Chacun à la table, l'a regardé avec mépris, et l'a soigneusement ignoré pour le reste du déjeuner* ».

De fait, n'étant pas reconnu par le système « méritocratique » *underground*, en tant que membre faisant partie des leurs (à savoir ayant fait ses preuves), ne pouvant le devenir (par contraintes professionnelles), sachant que pénétrer ce monde pour en gagner la confiance demande des années, nous avons opté pour une stratégie d'approche indirecte, *via* des interlocuteurs relais vers le monde « *underground »*, qui sont reconnus en tant que tel lorsqu'ils participent à des conventions de type « *hackers* ».

Notre passé, comme cyberpolicier (désormais connu par une partie de la communauté « *hacker* » *via* la circulation d'informations, notamment sur le portail d'actualité « *underground* » francophone : http://www.zataz.com), ne permet pas non plus, de faciliter cet accès. Même un travail actuel d'enquête sous couvert d'un statut de chercheur en sécurité de l'information ou aidé, sous couvert d'étude sociale, ne permet pas d'ouvrir des portes, finalement lourdement closes.

[232] *Know Your Enemy (Chap 16* « *Profiling* »*)* - 2nd Edition (HoneyNet Project, http://www.honeynet.org).

Ainsi, la clé de compréhension de cet univers clos repose sur l'identification de quelques portes d'accès (les conventions ou conférences de « *hackers* »), *via* des interlocuteurs relais qui font partie d'un second cercle concentrique gravitant autour du noyau dur des cybercriminels, en approchant donc certaines des pratiques et attitudes, sans toutefois pouvoir en dire trop. Parce que de leur loyauté au groupe dépend leur future admission au cercle, et parce que n'étant pas pleinement intégrés, beaucoup leur reste à apprendre et à découvrir. Nous avons donc cherché à cerner les autoreprésentations de la mouvance « *underground* » vis-à-vis du cybercrime, avec ces interlocuteurs relais présents à ces meetings identifiés. Ceux-ci ne nous ont donné que des pistes d'investigation, sachant que ces meetings, ne sont pour eux aussi qu'une des premières portes d'entrée vers l'*underground*, et que pour l'atteindre, il faut attester du franchissement d'une étape vers la délinquance, et passer beaucoup de temps sur le domaine, ce que la majorité ne peut faire, en raison de leur profession, de leur moralité, ou encore par peur du gendarme.

Ce monde des pirates informatiques est empreint véritablement d'une multitude d'individualités, et de délinquance affirmée, difficilement accessible, qui se réunit en comité clos, car se protégeant vis-à-vis d'études du type de celle que nous menons. Plusieurs « interlocuteurs » n'ont d'ailleurs pas donné suite à nos premiers entretiens. Pour ces personnages, le cybercrime est une réalité qui nécessite l'anonymat, lorsqu'on y est entré. Il s'agit de la formalisation, clairement identifiée, de la frontière entre le « *hacking* » et le cybercrime. Ainsi, nous avons investigué les endroits où trouver l'information, qui ne peut se faire, finalement, autrement qu'en passant par un filtre de connaissance (les interlocuteurs « connaisseurs » relais) du domaine, sans pour autant devenir délinquant.

Dans un premier temps nous proposerons de revenir sur le débat interne à la communauté du cybercrime qui distingue les comportements, de façon pas toujours probante, en traçant une frontière difficilement interprétable entre les « *hackers* » et les « *crackers* ». Puis nous proposons une rapide présentation des lieux de rencontres publics de cette communauté « *underground* », identifiés par nos interlocuteurs « connaisseurs » dans ce domaine, comme des portes d'entrée décisive du milieu. Enfin, nous mesurerons

les autoreprésentations de ce milieu « *underground* » de la cybercriminalité, *via* nos interlocuteurs, présents dans les rassemblements identifiés.

- La dichotomie fondatrice entre *hacker* et *cracker* : lutte symbolique autour d'une autodéfinition positive

Face à la montée en puissance dans les médias des années 1980-90 des articles concernant cet univers nouveau qui assez souvent a été abordé comme une menace, la communauté *underground* a voulu combattre de mauvaises représentations médiatiques en imposant une distinction, fondatrice aux yeux des « pirates informatiques », entre deux publics de pirates. Toute une série de discours sur ce thème puis la reprise de cette distinction terminologique dans des ouvrages plus grand public seront ici examinés, afin de mieux appréhender leur propre définition de la cybercriminalité et les raisons pour lesquelles une partie des individus concernés récusent cette labellisation, se considérant au contraire comme des êtres « purs ».

- Émergence des *hackers* et valorisation de leur « philosophie »

Pour comprendre l'émergence de cette terminologie, il faut refaire un bref historique. Dans les années 1960, l'informatique était, l'affaire de quelques professionnels, à IBM par exemple. Les utilisateurs n'étaient pas autorisés à approcher de la machine. Les programmes étaient sur cartes perforées, qu'il fallait corriger régulièrement, jusqu'à la bonne capacité de traitement de l'ordinateur. Certains, qui n'allaient pas tarder à s'appeler des « *hackers* » (que d'autres appelaient alors « *hobbyists* ») voulaient contourner la procédure. Ils revendiquaient le droit de comprendre comment la machine fonctionnait, d'y accéder, de travailler en temps réel, et de modifier la façon dont on l'utilisait. L'équipe la plus intéressée fut celle du MIT. Puis, les pionniers de l'informatique ont cherché à la rendre disponible pour tout utilisateur. D'abord par la dissémination de terminaux, puis par la mise au point du micro-ordinateur (*Personal Computer* - PC). S. Levy décrit la naissance de l'*Altair*, machine dont la seule interface avec l'utilisateur était constituée d'une rangée d'interrupteurs et d'une rangée de

lampes, et dans laquelle il fallait entrer le programme lors de chaque utilisation, « *les hackers avaient rapidement le bout des doigts calleux* ». Par la suite, naîtront les Apple I et II… C'est donc dans les années 1960 qu'un groupe « « *[…] de programmeurs passionnés du Massachusetts Institute of Technology » décide de se nommer hackers. Le terme va assez rapidement servir à désigner une élite informatique et constituer ce que l'on a appelé le « clergé » de l'informatique. Ce n'est que récemment que le terme hacker – devenu en français pirate – a commencé à désigner une personne capable de pousser un programme informatique au-delà de ses capacités supposées ou encore d'optimiser le code source d'un programme au maximum* ».[233]

S. Levy, en 1984,[234] retrace l'émergence et la multiplication des *hackers* aux États-Unis, de l'apparition du premier ordinateur mis à disposition des étudiants du MIT en 1959, un IBM 704, à l'apparition des premiers ordinateurs personnels, notamment le premier Apple Computer en 1976. Il en profite pour décrire pour la première fois dans un ouvrage grand public, la notion d'éthique *hacker* qu'il codifie selon les principes suivants :

- Toute information est par nature libre.

- Être anti-autoritariste.

- Les *hackers* peuvent se juger par leurs prouesses, non par d'autres hiérarchies sociales (ce qui permettra à un jeune prodige d'une dizaine d'années de rejoindre le groupe).

- Art et beauté peuvent être créés avec un ordinateur.

- Les ordinateurs peuvent changer et améliorer la vie.

- Les *hackers* dont parle S. Levy ne sont donc pas les briseurs de codes, les fabricants de virus, les fraudeurs que ce mot évoque aujourd'hui, mais les pionniers de l'informatique personnelle. L'idéologie reconnue aux *hackers*, permet également de les qualifier correctement : « *L'idéologie hacker, pour sa version la plus exigeante, repose sur le principe que toute information doit être libre et l'accès aux ordinateurs illimité et total […] L'esprit du hack : tous se doivent d'y adhérer – c'est d'ailleurs ce qui les*

[233] *Hackers ! : Le 5ème pouvoir – Qui sont les pirates de l'Internet* (Chatelain, Roche, 2003).
[234] *Hackers : Heroes of the Computer Revolution* (Levy, 1984).

distingue définitivement de la criminalité informatique et du terrorisme, comme d'ailleurs de toute industrie liée à la sécurité informatique »[235].

« *Parmi les valeurs de cet esprit du hack qui, en quelque sorte fonde le code des hackers, on trouve : la gratuité de l'information sur Internet ; la propriété intellectuelle doit appartenir à tous ceux qui en ont la compréhension ; les grandes entreprises ne sont pas dignes de confiance, les grands gouvernements le sont encore moins ; toute tentative de légiférer et donc de restreindre le cyber-espace doit être combattue ; le savoir-faire technique est la vertu qui doit être la plus valorisée* »[236].

P. Himanen traduit à travers son essai[237], nous l'avons vu, le principe de la « *hacker* attitude ». S. Levy met en évidence l'aspect des sensations possibles dans la recherche de la compréhension du fonctionnement des ordinateurs, comparés dans ce cadre à une véritable lampe d'Aladin[238].

- Une identité positive contestée

Les *hackers* revendiquent toujours aujourd'hui, le partage de l'information, le caractère ouvert et le statut public d'Internet, la définition de standards communs et accessibles au plus grand nombre : ce sont devenus de « véritables dogmes » selon P. Mounier[239]. Toutefois, si cette différenciation était chose aisée dans les années 1960 et 1970, elle ne l'est plus de nos jours, notamment à travers la confusion médiatique entretenue sur ces appellations. Le mot *hacker*, en vieillissant et en se répandant hors de la communauté *underground*, a pris une connotation négative au niveau de l'opinion publique, mélangeant abondamment *hackers* et *crackers*. Le *hacking* dans une acception malveillante, « *apparaît dans les années 1980 dans la presse informatique pour désigner, désormais, toutes les atteintes aux systèmes de traitement automatisé de données : manipulations de programmes, falsifications de données, intrusions*

[235] *Hackers : Heroes of the Computer Revolution* (Levy, 1984).
[236] *Hackers ! : Le 5ème pouvoir – Qui sont les pirates de l'Internet* (Chatelain, Roche, 2003).
[237] *L'Ethique Hacker et l'Esprit de l'ère de l'information*, (Himanem, 2001).
[238] « *When you grow up with an insatiable curiosity as to how things work, the delight you find upon discovering something as elegant as circuit logic, where all connections have to complete their loops, is profoundly thrilling. A computer was surely like Alladin's lamp* ».
[239] *Les Maîtres du Réseau, les enjeux politiques d'Internet* (Mounier, 2002).

malveillantes dans les systèmes informatiques… »[240]. Au cœur de la définition officielle américaine de ces menaces informatiques de type intentionnel, le *National Institute of Standardization Technology* (N.I.S.T) constitue une référence. Cet organisme s'est, très tôt, intéressé aux risques de piratage, ayant défini les rôles « clef » en matière de sécurité informatique. Qualifiés de concert « d'agents menaçants », les « *hackers* » et les « *crackers* » sont assimilés dans un document interne, tant par leurs motivations (goût du défi, ego et vanité…), que par leurs effets (destruction, altération de données, divulgation d'information, gain monétaire). R. Trégouët donne en 1997 une définition du terme *hacker* : « *une personne qui aime comprendre et utiliser les finesses techniques des programmes* »[241]. Mais par son usage, il qualifie aussi ainsi tous les délinquants pénétrant par effraction des sites informatiques. On retrouve le même type d'hésitations dans des organes officiels français de répression, même si l'effort de la communauté pour imposer une dichotomie a partiellement porté ses fruits. En 1994, le Service Central de la Sécurité des Systèmes d'Information (S.C.S.S.I) (devenu depuis D.C.S.S.I[242]) édite un guide intitulé *« La menace et les vulnérabilités des systèmes d'information* »[243]. Ce guide présente les pirates informatiques :

« nous proposons les deux profils de pirates les plus souvent identifiés :

- hacker : individu curieux, qui cherche à se faire plaisir. Pirate par jeu ou par défi, il ne nuit pas intentionnellement et possède souvent un code d'honneur et de conduite. Plutôt jeune, avec des compétences non négligeables, il est patient et tenace.

- cracker : plus dangereux que le hacker, cherche à nuire et montrer qu'il est le plus fort. Souvent mal dans sa peau et dans son environnement, il peut causer de nombreux dégâts en cherchant à se venger d'une société – ou d'individus – qui l'a rejeté ou qu'il déteste. Il veut prouver sa supériorité et fait partie de clubs où il peut échanger des informations avec ses semblables ».

[240] *Hackers le 5ème Pouvoir* (Chatelain, Roche, 2003).
[241] *Des pyramides du pouvoir aux réseaux de savoirs* (Tregouet, 1997).
[242] *Direction Centrale de la Sécurité des Systèmes d'Information, dépendant des services de M. le Premier Ministre.*
[243] *La menace et les attaques informatiques* (S.C.S.S.I., Service Central – N°650 du 28 mars 1994).

La frontière entre le « *hacking* » et le « *cracking* » est donc loin d'être intangible dans le repérage du phénomène de cybercriminalité par les personnes extérieures au milieu.

- Réaction des *hackers* : une distinction protectrice

Face à cela, la communauté du *hacking* a propagé sur ses réseaux et dans ses écrits Internet, l'idée qu'il fallait savoir distinguer entre les intentions des pirates informatiques, afin de trier le bon grain de l'ivraie. Dans le Jargon file[244], dictionnaire collaboratif, on trouve la définition suivante des *hackers*, particulièrement hagiographique : *« individus qui programment avec enthousiasme, « croyant » que le partage de l'information est un bien influent et positif et qu'il est de leur devoir de partager leur expertise en écrivant des logiciels libres et en facilitant l'accès à l'information ainsi qu'aux ressources informatiques autant que possible* ». Bien sûr, le « *cracker* » est celui qui est positionné à l'opposé de cette définition, qui agit pour son enrichissement personnel ou par pure malveillance. La communauté a tout fait pour distinguer, stigmatisant une partie des fraudeurs informatiques afin d'éviter d'être soi-même stigmatisée, en vain donc. Le dictionnaire *The Jargon File* distingue ainsi clairement le *hacker* malveillant – qu'il nomme *cracker* – des autres *hackers*, en soulignant que c'est en réaction aux impropriétés terminologiques des journalistes.

D. Bellin a souligné dès 1985, que les motivations des « *hackers* » en faisaient davantage des héros que des criminels. En effet, ils sont guidés par trois facteurs : « *L'excitation intellectuelle, le désir d'apprendre toujours plus des ordinateurs, et le goût du défi pour pénétrer un ordinateur situé à distance. Il indique que, de son point de vue, dans la majeure partie des cas, il n'existe pas d'intention criminelle. Les groupes ciblés par les hackers sont au premier chef : les politiciens, et gouvernements, les manufacturiers informatiques, et enfin les experts informatiques, ce qui contribue à en faire plutôt des robins des bois des temps modernes que des criminels. En fait,*

[244]Dictionnaire des hackers rédigé collectivement sur Internet : http://www.tuxedo.org/~esr/jargon/html/entry/hacker.html.

criminaliser les activités des hackers n'aiderait en rien à comprendre la situation et à lui trouver des solutions »[245].

- Un dichotomie qui s'est imposée

Ce travail de séparation, afin de sauver la réputation d'une partie des acteurs du piratage, a porté ses fruits. De nombreux ouvrages ou documents professionnels parus ces dernières années tendent à donner quitus aux *hackers* et font leur la dichotomie fondatrice. Il y a eu beaucoup de controverses et de confusion dans l'usage des termes *hackers*, et *crackers* […] Les *hackers* déterminent uniquement des personnes intéressées par les réseaux et les ordinateurs. Les *crackers* tentent de pénétrer à l'intérieur des systèmes ou de les détruire. Dans son entreprise de compréhension des ressorts psychologiques des *hackers*, dans la lignée de Rogers, J. V. Beveren[246] souligne que ceux-ci ne forment pas un groupe homogène, comme plusieurs auteurs ont voulu le démontrer (Taylor, 1999 ; Denning, 1998 ; Post, 1996 ; Sperling, 1992). Il indique que le terme *hacker* est trop large, qu'il décrit une activité, sans tenir compte des différences en interne de ceux qui sont concernés par l'activité du *hacking*.

Nous avons aussi noté que, dès l'introduction de l'enquête du Boston Consulting Group, est présenté le découpage sémantique qui est au fondement de la communauté : « *hackers not crackers* ».

En octobre 2002, Pirat'z édite un dossier intitulé « *Comment devenir un hacker (La philosophie du hack)* ». La première partie vise, également à faire le tri dans les définitions et différentes terminologies utilisées jusqu'alors. En effet, la presse spécialisée notamment, ayant désormais, l'habitude de ce phénomène, tend à éviter l'amalgame. En effet, la distinction est bien faite : « *Qu'est-ce qu'un hacker ? Le sens de ce mot est très controversé. Pour les puristes, un hacker est un passionné spécialiste des ordinateurs, des réseaux, de la programmation…C'est effectivement le sens initial du mot. De son côté, le sens populaire imposé par les médias affirme qu'un hacker est un pirate informatique* ». Le magazine fait état du *hacker* au sens d'une personne très

[245] *High school hackers : Heroes or criminals?* (Bellin, 1985).
[246] *A conceptual model of hacker development and motivations* (Beveren, 2001).

compétente en informatique et en programmation, qui est également passionnée de sécurité informatique et « *aime à chercher comment on peut la contourner* ». Le magazine établit la différence entre un *hacker* et un pirate ; elle réside essentiellement dans la perception d'une certaine philosophie du « *hack* » : « *Tout le monde a entendu parler de la philosophie des premiers hackers, des puristes, initiée par Richard Stallman. Parmi leurs idées on trouve la libre diffusion de l'information, le logiciel libre et le droit inaliénable du hacker à passer ses nuits devant un écran comme l'asocial qu'il est* ». Il est également fait mention, ce qui est relativement rare dans la presse magazine, d'une « philosophie plus radicale », notamment *via* un texte reconnu par cette communauté « underground » (mouvement parallèle ou encore « sous terrain ») à savoir le « *Manifeste du Mentor* » (publié il y a quinze ans). À cette époque, le réseau était « vierge », à son tout début ; de fait les *hackers* souhaitaient alors produire un idéal dans une sorte de « nouveau monde virtuel ». « *Depuis les choses ont changé, Internet est devenu, pour sa majeure partie, la vitrine du monde réel* ». Par éthique du *hacker*, le magazine entend *« l'idée d'un droit fondamental de l'information à libre diffusion. Les réseaux sont des espaces de pures informations, donc de libertés totales. Il est interdit de réglementer le réseau, de le soumettre à des lois, et bien sûr de protéger l'accès aux systèmes* ». En bas de page de cet article, un encart rappelle la Loi N°88-19 du 05 janvier 1988 relative à la fraude informatique. Dans ce dossier, plusieurs définitions permettent de faire un point sur les différentes terminologies employées. Le dossier présente les différents types d' «attaquants » catégorisés selon leur expérience et leurs motivations :

« Les White Hat Hackers : hacker au sens noble du terme, dont le but est d'aider à l'amélioration des systèmes et technologies informatiques que nous utilisons aujourd'hui. Le courrier électronique en est un exemple ».

« Les Black Hat Hackers, plus couramment appelés pirates (ou appelés également crackers par extension du terme), sont des personnes s'introduisant dans les systèmes informatiques dans un but nuisible ».

« Les Script Kiddies (« gamins du script » ou encore craschers, lamers…) sont de jeunes utilisateurs du réseau utilisant des programmes trouvés sur Internet, généralement de façon maladroite pour vandaliser des systèmes informatiques afin de s'amuser ».

« Les phreakers sont des pirates s'intéressant au réseau téléphonique commuté (RTC) afin de les utiliser gratuitement grâce à des circuits électroniques connectés à la ligne téléphonique dans le but d'en falsifier le fonctionnement ».

« Les Hacktivistes (contraction de hackers et activistes que l'on peut traduire en cyber-militants ou cyber-résistants), sont des hackers dont la motivation est principalement idéologique ». Ce terme a été fortement relayé par la presse, en parallèle avec la notion de « *underground* » qui caractérise les *hackers*. »

B. Arief et B. Denis, en 2004[247], consacrent un chapitre à la compréhension du monde des *hackers*, reprenant les principes édictés par Rogers. Enfin, toujours en 2004, « *The Hackers Profiling Project* »[248], projet de recherche international propose de fournir une connaissance de la sécurité globale et pratique, ainsi que des clés de connaissance pour résoudre les problèmes d'insécurité. La volonté est de comprendre les motivations et identifier les acteurs concernés. Les *hackers* sont présentés sous un jour noble (*ethical hacker*), tandis que les « *wanabbe lamer* » ou encore les « *script-kiddies* » sont dénigrés.

Une nouvelle fois (cf. deuxième partie – III – 2)), le principe historique dichotomique des acteurs de la cyberdélinquance est repris et respecté par des personnes extérieures au milieu. Dans la lutte symbolique pour l'appellation des pratiques et des acteurs, il semble que les *hackers* aient donc réussi à faire repencher un peu la balance en leur faveur.

2) Modes d'organisation de la mouvance « *underground* »

- Meetings & mouvance « underground » :

Nous avons effectué les rencontres prévues avec des acteurs ayant participé aux meetings ou aux travaux relevant du monde social des pirates informatiques. Ces

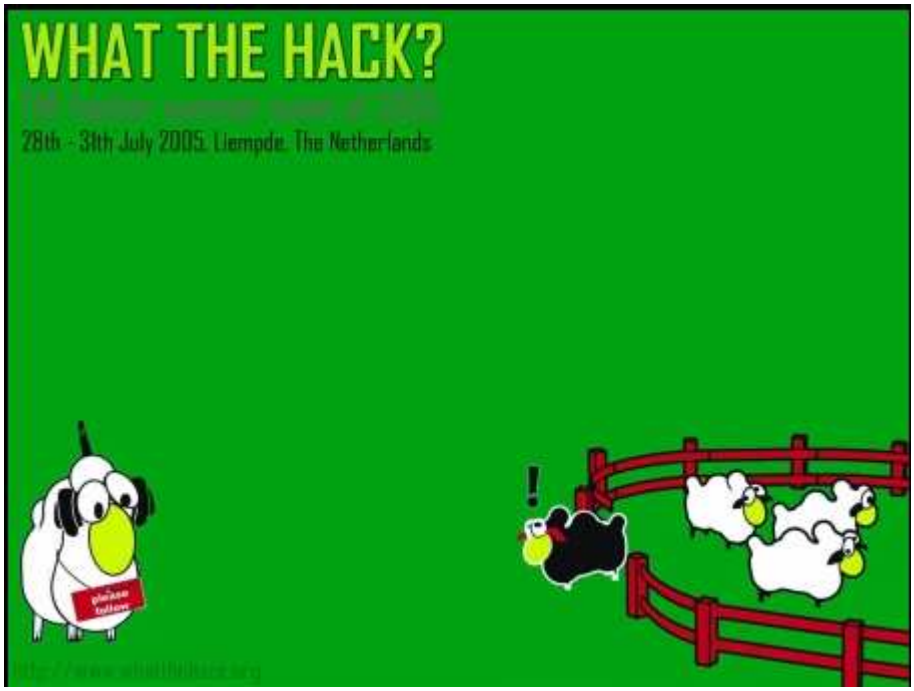
[247] « *A hacker is someone that experiments with systems… [hacking] is playing with systems and making free calls is just a small part of that. Hacking is also about freedom of speech and free access to information – being able to find out anything. There is also the David and Goliath side of it, the underdog vs. the system, and the ethic of being a folk hero, albeit a minor one* ».
Budi A., Besnard D., 2004, Technical and Human Issues in Computer-Based Systems Security, University of Newcastle..

[248] *The Hackers Profiling Project*, 2004.

entretiens permettent d'apporter une vue large et des retours d'expérience notamment de l' « auto-représentation » mise en valeur par les personnages principaux de la cybercriminalité. Ces acteurs nous ont fourni des informations sur les conférences les plus caractéristiques, auxquelles ils se déplacent. En voici la description.

- What the Hack

« *What The Hack* » est une conférence de « *hackers* » qui s'est tenue du 28 au 31 juilllet 2005 au sud de la Hollande (LIEMPDE, Netherlands – « *Come to What The Hack, July 28-31 2005, Lat 51°33.270858 / Lon 5°20.620584 (Liempde, near Den Bosch, The Netherlands) »*).



- Figure 5. *What the Hack*, 28 au 31 juilllet 2005

Cette conférence[249] se tient tous les quatre ans. Au départ, elle réunissait quelques passionnés centrés autour du petit magazine de « *hacking* » dénommé « *Hack-Tic* ». La

[249] Inscription sur pancarte : « *please, follow* ».

dernière parution date de 1993, malgré tout l'événement se poursuit. En 1989 a eu lieu la « *Galactic Hacker Party* », en 1993 : « *Hacking at the End of the Universe* », en 1997 : « *Hacking in progress* », et en 2001 : « *Hackers At Large* ».



- Figure 6. *What the Hack*, 28 au 31 juilllet 2005

Ces réunions rassemblent toute personne ayant un intérêt particulier pour l'univers du « *hacking* », le développement de logiciel open-source, les activistes de libertés civiles et de vies privées, des experts dans les champs des réseaux et de la sécurité de l'information.

Cependant, ce type de réunions n'est pas réservé uniquement pour ceux qui se déclarent « *hackers* », mais c'est un de leurs endroits de rencontre identifié. Ainsi, ce type de conférence permet de croiser de nombreuses cultures.

En marge du sujet principal, des thèmes satellites sont déclinés, à savoir : la liberté d'expression, la transparence gouvernementale, l'insécurité des ordinateurs, la vie privée, les logiciels ouverts, et les réseaux communautaires.

La conférence « *What the hack* » traite surtout des points suivants : passeports digitaux, de biométrie, et de cryptographie. Elle a réunit près de 3000 experts et passionnés du sujet.

Le point critique du contrôle d'accès physique à la conférence « *what the hack* » fut d'ailleurs traité avec des moyens d'experts :



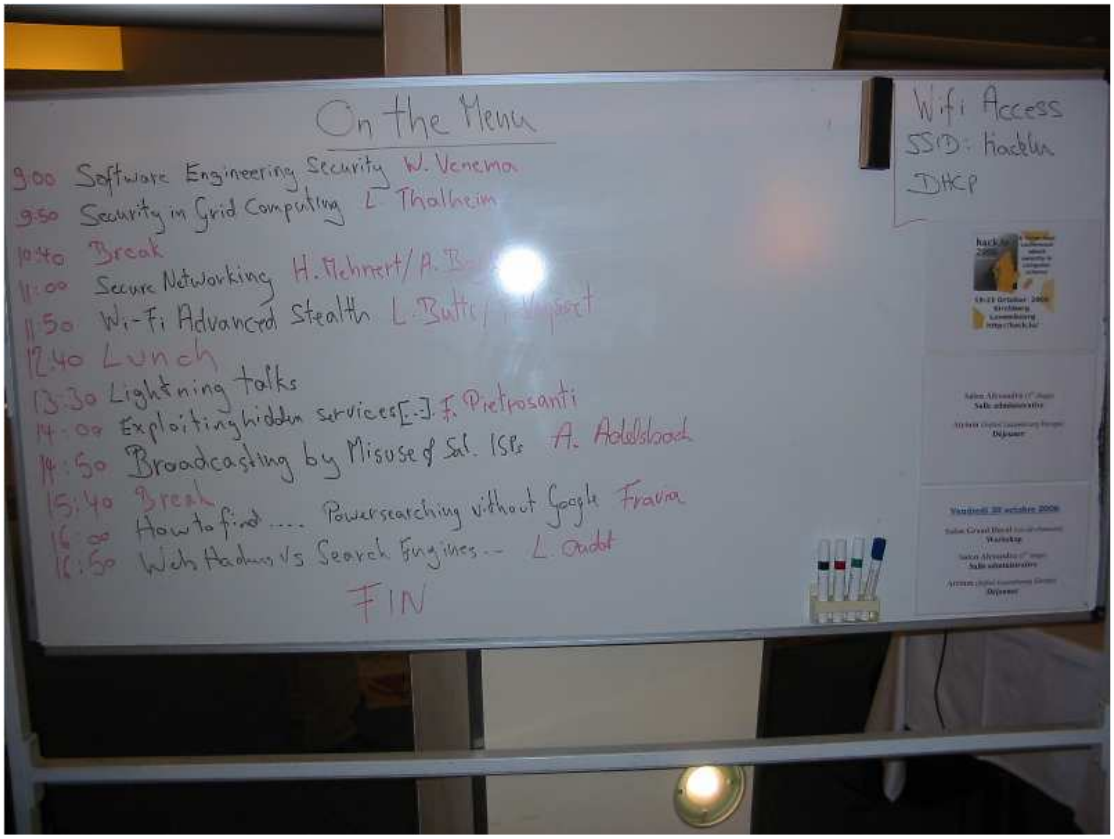
- Figure 7. *What the Hack*, 28 au 31 juilllet 2005

Rop Gonggrijp (professionnel d'Internet et un des organisateurs de « *Galactic Hacker Party* » – 1989), indique qu'il est important que ce type de réunion soit en plein air, et se passe dans une ambiance « relaxe » (sic), totalement ouverte. Ce dernier indiquant que l'idée est de casser le stéréotype des « *hackers* », qui est réellement à l'inverse d'un « vandale » : « *Ils n'ont jamais fait partie de cette communauté. Et*

maintenant, il y a heureusement un espace dans les médias permettant de distinguer plus qu'une image (le stéréotype) du hacker »[250].

- Hack.lu

Le dernier salon hack.lu (http://www.hack.lu) a eu lieu du 19 au 21 octobre 2006.



- Figure 8. *Hack.lu*, 19 au 21 octobre 2006

Depuis deux ans, ce salon est incontournable pour tous ceux qui souhaitent faire le point sur les connaissances de « *hacking* » et de sécurité SSI. Les présentations de cette conférence à caractère international, sont soumises à comité de relecture (nous avons participé à celui de 2006), et sont toujours de qualité sur le sujet traité. Notons, par

[250] « *The idea was to break the stereotype of hackers as sun-averse malcontents bent on vandalism. They've never been part of this community. And now there's fortunately space in the media for more than one kind of hacker* ».

exemple, l'intervention « *Using Computer Forensic at the police by FCCU (Federal Computer Crime Unit of Belgium)* ». De nombreux outils à disposition de la FCCU, leur permettant de déterminer rapidement si un ordinateur est suspect, ont été présentés (photo : valise interopérable, permettant d'analyser tout type d'ordinateur).



- Figure 9. *Hack.lu*, 19 au 21 octobre 2006

Deux policiers belges ont exposé les outils informatiques et leurs matériels utilisés lors de perquisitions pour des affaires judiciaires de type cybercriminelles. Ils ont par ailleurs fait une démonstration d'une distribution linux, qu'ils ont « compilée » eux-mêmes, avec des programmes permettant de retrouver une multitude de traces dans Windows par exemple (des images, des vidéos, le mot de passe des *user account* (Compte utilisateur) dans la base SAM, …).



- Figure 10. *Hack.lu*, 19 au 21 octobre 2006

Interrogés sur les affaires en cours, un des policiers nous a indiqué que les affaires actuelles sont surtout en rapport avec des actes illicites utilisant l'ordinateur comme moyen et non comme cible. Les attaques de pénétration réseau, ayant des suites judiciaires sont rares ; désormais, les policiers doivent surtout faire face à une criminalisation croissante de ces actes sur Internet, reprise par de nombreuses mafias, et de fait doivent souvent prêter main-forte aux autres unités de police, dans des affaires judiciaires classiques de ce type, mais demandant désormais des compétences en « *forensic* technique » (analyse légistes techniques – recherche de traces et de preuve qualifiant l'infraction). Les ordinateurs étant devenus des outils du quotidien de ces activités illégales et criminelles.

- Black-Hat

Black Hat est une société fondée en 1997 par Jeff Moss (plus connu sous le *nickname* de *Dark Tangent*), réputée pour organiser un réseau de conférences fournissant des points de vue nouveaux et exclusifs sur la sécurité de l'information. Les Conférences *Black Hat* (ou *Black Hat Briefings*) forment un évènement unique qui rassemble officiellement des experts des agences gouvernementales américaines et des industries, américaines ou non, avec les *hackers* les plus respectés de l'« *underground* ».

Ces forums sont régulièrement organisés à Las Vegas (*Black Hat USA*), Amsterdam (*Black Hat Europe – depuis 2000, partenariat :* Radware, CLUSIF, EICAR,

IEEE, *Security Task Force*, GVIB, EEMA, IPv6 Forum, SecurIST, WCAI), Tokyo (*Black Hat Japan*), et Singapour (*Black Hat Asia*).

Un évènement est spécialement organisé pour les agences fédérales américaines à Washington (*Black Hat Federal*), et un autre sur la sécurité des systèmes d'exploitation Microsoft Windows (*Black Hat Windows Security*). L'évènement à Las Vegas se déroule juste avant la conférence *DefCon* (voir détails en *infra*), un autre évènement majeur en sécurité de l'information.

En 2005, Jeff Moss a vendu *Black Hat* à *CMP Media*, une filiale de *United Business Media* basée en Grande Bretagne, pour 14 millions de dollars américains. Il continue toutefois à organiser la conférence *DefCon* qui n'était pas incluse dans la transaction. Les *Black Hats* (pirates au chapeau noir), représentent, à l'origine, une famille de *hackers*. À la différence des *White Hats*, les *Black Hats* sont plutôt orientés pleinement vers les actions illégales. Cela va de la création de virus aux chevaux de Troie, en passant par les vers et les logiciels de type espion. Ces individus tirent parti de leurs compétences informatiques dans un but lucratif ou bien dans le but de nuire à des individus ou à des organisations (Cyber-terroristes). Plus généralement, les *Black-Hats* utilisent leur savoir pour découvrir des aspects des réseaux d'information et de communication qui leur sont cachés.

Il est confirmé une criminalisation croissante sur Internet, en effet le nombre de *Black-Hats* augmente constamment, notamment vis-à-vis de la mise à disposition *via* les réseaux d'informations de valeur, pouvant intéresser hautement toute organisation orientée dans la guerre économique. Il n'est cependant pas impossible que certains *Black Hats*, d'origine, finissent par changer de bord et se fassent employer par des sociétés spécialisées dans la sécurité informatique (exemple récent : Sven Jaschan, auteur du virus *Sasser*, recruté en 2005, par la PME allemande Securepoint).

La communauté des *Black Hats* est hétérogène : les différents membres ne se reconnaissent pas toujours entre eux, à cause de leurs différences d'opinion, de capacités ou de philosophie. (exemple : Sven Jaschan est considéré, nous l'avons vu, comme un *traître* par certains *Black Hats* qui considèrent qu'il ne devait pas se vanter de ses actions douteuses…).

- DefCon

Nous avons vu que la défense des flux de circulation de la communication et de l'information est effectivement la grande idée prônée par les *hackers*. Il s'agit du thème récurrent de la manifestation annuelle *Defense Condition* (*DefCon*), organisée par Jeff Moss (voir *supra*).

Note : DefCon : il s'agit du nom de code d'origine utilisé par la Défense américaine en cas d'attaque nucléaire.

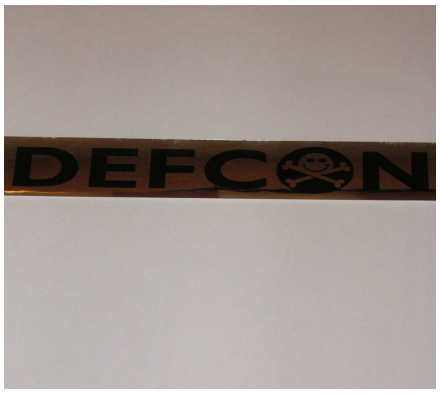
DefCon est la convention *hacker* la plus connue à travers le monde. La première convention *DefCon*[251] s'est déroulée en juin 1993. Depuis, cette manifestation a toujours été organisée à Las Vegas, aux États-Unis d'Amérique, généralement en juillet de chaque année.



- Figure 11. Badge d'accès à la conférence *DefCon*

Le public de cette convention est pour la plupart composé de professionnels de la sécurité des systèmes d'information, de *crackers*, et de *hackers* intéressés par la programmation et l'architecture des réseaux.

[251] http://www.defcon.org & http://www.2600.com.



- Figure 12. Bannière *DefCon (sticker)*

Limité à 5000 participants, le droit d'entrée actuel est de 100 dollars, pour l'ensemble des accès au congrès, ce qui est réellement peu coûteux en regard par exemple du salon *Black Hat*, vendant des accès à des interventions/formations pouvant dépasser 2000 dollars.

- Chaos Communication Congress

Le *Chaos Communication Congress* est un rendez-vous annuel de la scène *hacker* internationale, organisé par le *Chaos Computer Club* (*CCC* qui a été créé par des pirates allemands). Le congrès propose une série de conférences et d'ateliers sur des sujets techniques et politiques. L'évènement se déroule à la fin de chaque année, entre le 27 décembre et le 29 décembre, depuis 1984. Le congrès a commencé à être organisé à Hambourg, en Allemagne, puis a été déplacé à Berlin en 1998. Il attire généralement entre 2500 et 3000 participants.

Le congrès est un évènement organisé avec peu de budget, et tente de conserver des prix d'entrée relativement bas pour permettre aux jeunes personnes d'y participer. Une part importante du congrès est le *hack center*, permettant d'héberger environ 600 personnes. Le *hack cente*r et les autres zones du congrès sont connectés à Internet par une ligne haut débit. « *Pour anecdote, depuis 1997, le congrès héberge chaque année les*

championnats allemands de crochetage de serrure… »[252]. Il est à noter que le concept d'*underground* est apparu avec le *CCC* de Hambourg qui souhaitait pousser ses réflexions sur les *hackers* et le *phreaking* (néologisme construit à partir de « *freak* » (mordu), « *free* » (gratuit) et « *phone* » (téléphone)). Le *phreaking* vise à ne pas payer les communications téléphoniques et d'autre part, à pirater les lignes. « *Dans les années 80, quelques personnes proches du CCC, ont essayé de vendre des informations aux services secrets soviétiques d'alors, le KGB* »[253]. Ce qui entraîna de nombreuses enquêtes judiciaires au niveau international. Le *CCC* est depuis devenu une respectable association.

En 1998, un membre du *CCC*, connu sous le nom de Tron, a été victime d'un homicide (*CCC* – 24 octobre 1998). Les circonstances de sa mort demeurent mystérieuses pour l'ensemble de la communauté *underground*.



[252] *Hackers ! : Le 5ème pouvoir – Qui sont les pirates de l'Internet* (Chatelain, Roche, 2003).
[253] *Hackers ! : Le 5ème pouvoir – Qui sont les pirates de l'Internet* (Chatelain, Roche, 2003).



- Figures 13, 14 et 15. *What the Hack*, 28 au 31 juilllet 2005 – *CCC Camp*

Le *CCC* français est apparu à la fin des années 80. A sa tête, Jean-Bernard Condat, jeune informaticien français. Il s'avéra par la suite que ce club était monté de toutes pièces (par la DST (sic Jean-Bernard Condat)) aux fins de constituer un fichier des pirates informatiques français (voir *supra*).

- Meeting 2600

Les pirates informatiques racontent aussi leurs exploits dans des forums baptisés « 2600 » (fondés par *Emmanuel Goldstein, patron du magazine des « phreakers » (pirates téléphoniques) « 2600 » (fréquence du son que produit une pièce de vingt-cinq cents tombant dans un taxiphone américain. Captain Crunch pirate précurseur avait découvert cette particularité, qui, pendant des années, a permis aux pirates de téléphoner gratuitement* »).

Les meetings « 2600 » ont lieu au niveau international chaque premier vendredi du mois (France : Place d'Italie à Paris, au Grand-Duché de Luxembourg également).

Ce type de réunions forme un club de rencontre de spécialistes de la sécurité et de l'informatique ayant pour but de trouver des techniques, des protections, mais tout en restant dans les limites légales. Un magazine « 2600 » est publié tous les trimestres faisant état de nombreux articles « décalés » traitant de sécurité et d'insécurité informatique. L'abonnement est disponible aux Etats-Unis, mais de nombreux abonnés sont en Europe. En page de fin du magazine, se trouvent notamment tous les endroits du monde où se réunissent les groupes 2600 :

« *France : Avignon (Rue de la République), Grenoble (campus St. Martin), Paris (Place de la République), Rennes (devant le magasin « Blue Box ») ». Pour pouvoir être recensé en tant que tel, il faut respecter des principes 2600 : réunions tous les premiers vendredi du mois, espace public, ouvert à tous… (voir site web : http://www.2600.com).* »

L'ensemble des photos « *What the hack* » de cette partie ont été présentées lors de la rencontre SPIRAL[254] le 26 septembre 2006 : « *S'il te plaît… dessine-moi un pirate informatique !* » (G-D de Luxembourg) (voir *supra*).

- Acteurs & mouvance « *underground* » :

Nous avons procédé à l'identification des acteurs « *underground* » ou considérés en tant que tel (Note : l'anonymat est requis pour ce type de personnage). Notre recherche visait à identifier des personnages clés de ce milieu « *underground* », en mesure de nous fournir des informations pertinentes sur le phénomène du cybercrime, tout en tenant compte de nos contraintes professionnelles.

Nous avons rencontré cinq de ces personnages pouvant être considérés comme « parties prenantes des mondes de la cybercriminalité », sans pour autant nous confirmer leur participation à de réels actes de piratages informatiques actuels (certains ont

[254] Réseau des professionnels de l'IT au Grand-Duché de Luxembourg – http://www.spiral.lu.

cependant confirmé avoir été mis en cause pour piratage informatique au niveau judiciaire, dans le passé…)[255].

La synthèse suivante se substitue aux entretiens qui n'ont pas été rédigés en tant que tel, mais fait l'objet de notes rapides au fur et à mesure des échanges avec ces personnes proches ou « sachants » du milieu « *underground* », très méfiantes sur ce sujet (pour respecter ces aspects nous préserverons leur identité, et ils seront présentés par numéro). En fait, au fil de l'année 2006, et de cette étude, nous nous sommes rendus compte d'une véritable chasse-gardée sur le sujet de notre problématique, et de la difficulté de réunir des informations pertinentes ou simplement de rencontrer des actifs, en présentant directement notre travail pour sujet de discussion. De plus, dès que nous touchons à l'aspect social du « cybercrime », le sujet devient complexe à traiter. Ce sont donc les personnes qui ont permis d'identifier les réunions phares de réunions de type pirate (voir point précédent) et qui y participent, qui demeurent nos principaux interlocuteurs sur ce sujet.

Notre interlocuteur numéro un participe chaque année au *Chaos Communication Camp* (Allemagne), ainsi qu'aux congrès *Black Hat* et *DefCon* (Etats-Unis). Ces trois réunions sont pour lui incontournables pour parfaire ses connaissances (techniques et relationnelles) du monde « *underground* ». Ce dernier nous décrit le *Chaos Communication Camp* comme un rendez-vous international de *hackers*, plus en marge de ceux que nous avons décrit *supra*, se déroulant à Paulshof près de Altlandsberg, près de Berlin (notre interlocuteur nous indique d'ailleurs que d'autres manifestations sont organisées ensuite entre « intéressés » du piratage informatique, par petits groupes, mais non divulguées (sap)). Organisé par le *Chaos Computer Club* (CCC), quatre éditions ont eu lieu, en 1993, 2003, 2005 et 2006 (décembre). Le *Chaos Communication Camp* est un évènement principalement anglophone fournissant des informations sur des sujets comme la vie privée et la sécurité de l'information, d'un point de vue technique ou politique.

[255] Note : notre profession et le travail en cours de thèse mené sur le sujet « Mondes de la cyberdélinquance et images sociales du pirate informatique », ne nous a pas permis d'intégrer plus en avant la mouvance *underground* très méfiante quant à notre travail relatif aux aspects sociaux du pirate informatique. De plus, notre travail est désormais connu *via* les aspects de promotion et de marketing, notamment sur le portail de l'actualité « *underground* » francophone : http://www.zataz.com.

Notre interlocuteur nous indique que ce type de réunion est plus en marge que *Black-Hat* ou *DefCon*, et qu'il est possible de rencontrer de véritables pirates très actifs. Le rendez-vous est très apprécié de la scène « *underground* » très technique.

Quant à *Black Hat*, il s'agit d'un rendez-vous historique qui prend sa dimension surtout aux Etats-Unis où toutes les conditions sont réunies pour rencontrer les principaux acteurs de la problématique. Lors du dernier congrès, notre interlocuteur nous a rendu compte du problème avec *Cisco*, lors d'une présentation réalisée par un chercheur en sécurité, M. Lynn. Celui-ci avait démontré comment prendre le contrôle d'un routeur Cisco à l'aide d'une faille dans *Internetwork Operating System* (*IOS*), un système d'exploitation interne à plusieurs produits du fabricant. La réputation d'inviolabilité était alors terminée, provoquant une véritable « colère » (sic) de Cisco, qui a, tout de suite, souhaité déposer plainte.

L'employeur de Lynn, *ISS* (*Internet Security Systems*), a décidé d' « étouffer » la présentation. L'ensemble des présentations de cette faille, disponibles dans le cahier des présentations de la conférence, fut d'ailleurs arraché à la main et détruites par les organisateurs (notre interlocuteur est fier de disposer encore d'un exemplaire et de nous l'avoir montré (collector (sic))). Lynn a depuis démissionné et s'est retrouvé poursuivi par *Cisco* et…*ISS* elle-même. Il a ensuite, en effet, publié et communiqué rapidement sur cette faille, reprise alors par la communauté « *underground* ». Notre interlocuteur juge la conférence *Black Hat* finalement trop commerciale, et cette réaction des organisateurs en lien avec ce jugement en est une preuve. Il prône l'intérêt de participer à *DefCon* plutôt très proche de la communauté et plus libre. Il indique que les « fédéraux » sont présents, mais qu'ils sont avertis, un jeu permet même de tenter de les démasquer (sic).

Notre interlocuteur indique que les *White Hats* se rapprochent des préoccupations actuelles des institutionnels, vis-à-vis de la problématique de la protection nécessaire des TIC. Il nous indique également qu'il manque un pont, une couche sociale entre les « *Geeks* » (passionnés), qu'il juge trop proches de la technique et dans leur monde, et le citoyen qu'il faut sensibiliser à la nécessaire sécurité de l'information. Cette absence de lien, pour lui, donne libre cours à l'interprétation de l'opinion publique vis-à-vis du cybercrime et à la production d'images plus proches du stéréotype que de la réalité (sic).

Notre interlocuteur numéro deux participe principalement aux conférences *Black Hat* et *DefCon* (Etats-Unis). Pour ce dernier, la conférence *Black Hat* est depuis plusieurs années une référence en termes de sécurité, la conférence ayant changé d'image avec les années pour devenir ce point de repère attendu pour faire le point sur la sécurité en général. La fréquentation de la conférence a clairement évolué pour atteindre cette année environ 3000 personnes. Désormais, une conférence *Black Hat*, réunit des professionnels de la sécurité, des ingénieurs, des développeurs, des agents fédéraux, des vendeurs et, bien sûr, quand même les fameux *hackers*. Notre interlocuteur spécifie que le lieu rassemble à la fois la scène « *underground* », la CIA, les spécialistes sécurité, et que durant ce temps les clivages et les « querelles de chapelles » (sic) sont mis de côté. La réunion prend alors, pour sa part, un côté mystique.

Lors de la dernière conférence, il fut étonné du nombre d' « asiatiques » (sic) présents et semblant très compétents ; pour sa part, il s'agit d'une première. Il nous indique que les fédéraux sont bien présents et nous a décrit notamment la célèbre activité « off » : « *Find the Fed* » (« identifiez l'agent du FBI ») qui consiste à identifier parmi les *hackers* celui ou ceux qui sont passés sous contrôle du Gouvernement américain. Ceux qui trouvent, gagnent un tee-shirt « *I found the Fed* ». En « *off* », également, un écran géant déroule en permanence l'ensemble des trames de télécommunication ou de réseaux « *sniffées* » (interceptées) durant le meeting ; ou encore les fédéraux qui disposent d'un stand, distribuent des « *goodies* » (gadgets) en échange d'un CV (sic).

Notre interlocuteur classifie de fait, en fonction de son expérience, la scène « *underground* » ainsi :

« *- Black Hats : qui exploitent les failles techniques, soit pour déstabiliser ou par aspect ludique, soit à but lucratif.*

- Hacktivists : principalement aux fins de déstabiliser un pouvoir par motivation politique (origine principale actuellement : Brésil, Turquie et Iran, souvent actions de « defacement » (défiguration de sites web) (sic)).

- White Hats : personnages empreints d'éthique, ils ne dépassent pas la frontière de la loi, écrivent les « exploits » permettant d'exploiter une faille, mais l'utilisent rarement

(test en réseaux locaux), le but principal étant l'innovation de la sécurité des NTIC. De grands experts sécurité en font partie.

- Grey Hats : ces derniers écrivent et exploitent les « exploits », ils préviennent les sites testés, cependant, entre-temps, ils ont franchi la frontière légale.

Notre interlocuteur précise que la véritable cybercriminalité se situe au niveau des Black Hats, des Grey Hats et des Hacktivists. »

Notre interlocuteur numéro trois, présent à « *What the hack* », nous a indiqué que ce type de réunion donne vraiment l'impression d'un camp de vacances, sans préfigurer la présence de véritables dangereux pirates. Cependant, il confirme que durant ce congrès, les activités de « *hacking* » étaient nombreuses : certaines personnes infiltraient les tentes des autres pour tenter de récupérer des informations de configuration de leur réseau, dans le but de les pirater ensuite plus facilement. Beaucoup, se faisant démasquer rapidement sur place, les « victimes » n'étant pas étrangères en la matière. Ce dernier, présent depuis peu dans cette communauté, a indiqué qu'il est difficile d'échanger avec les personnes présentes, qu'il existe durant ce type de réunion des réseaux associés où se retrouvent des personnes se connaissant très bien. Il précise que de nombreux piratages semblaient discutés et/ou testés durant ces réunions, mais sans en avoir confirmation.

Le grand message ressortant et validé par notre interlocuteur est que, finalement, les activités de « *hacking* » ne relèvent pas du cybercrime, mais de la participation à l'innovation et la compréhension des réseaux d'information et de communication, participant de fait à la défense.



- Figure 16. *What the Hack*, 28 au 31 juilllet 2005

En justification, notre interlocuteur trouve cette photo très claire et parlante. De fait, « *what the hack* » ressemble à un espace public recréé pour redonner une place à l'image du *hacker*, dévié de son sens premier par les médias notamment (sic).

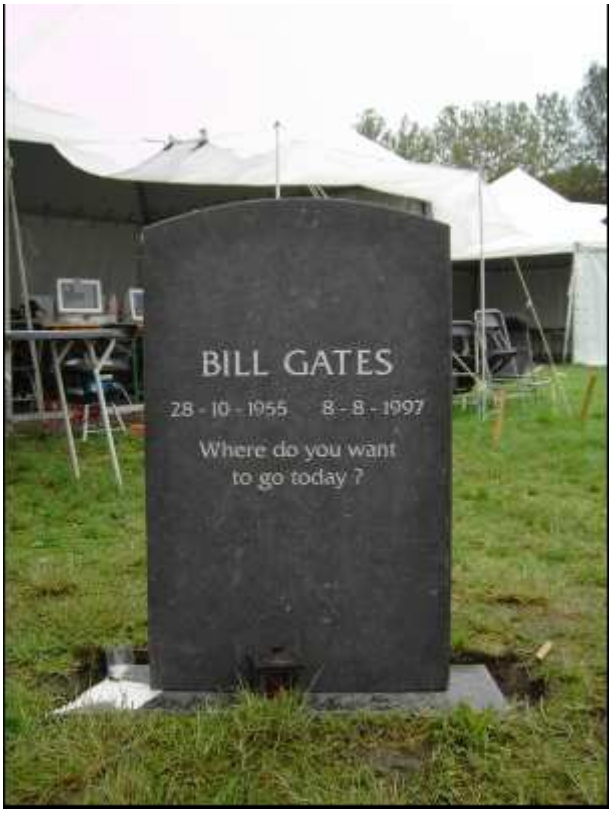
Notre interlocuteur numéro quatre est un fervent défenseur des valeurs et de la pure tradition de l'idéologie des « *hackers* ». Nous nous souvenons de ce dernier, présent à une de nos conférences et qui, avant que nous présentions la catégorisation des menaces IT, nous a clairement dit « *…merci de défendre l'image des « hackers »* ». Ce qui ne laissait aucun doute sur les convictions de ce dernier. Et en amont lors d'une réunion précédente, ce dernier nous indiquait : « *mais si ton ordinateur est connecté et en ligne avec le public, rien n'empêche d'y accéder, l'information en ligne est libre, et doit être libre, accessible pour tous…* ».

Ce dernier, très fervent défenseur du monde du logiciel « libre », cherche *via* son activité quotidienne à « construire quelque chose » dans son domaine d'activité, et surtout

transmettre ce « quelque chose », à destination de tous ceux qui veulent apprendre. De plus, clairement ce dernier confirme qu'il est impossible de se proclamer « *hacker* », que généralement se sont les « pairs » (ceux de la « scène » (milieu *underground*)) qui vous reconnaissent en tant que tel, et qui vous qualifient en fonction de vos développements et actions reconnues.

Dans le cadre de cette reconnaissance, il indique que l'expertise technique est indissociable, et doit être de très haut niveau ; il est inutile de maîtriser Windows (sauf pour le « *hacker* » ou le dénigrer), mais important de maîtriser Unix et Linux, logiciel de type libre, ouvrant à toute connaissance possible, pour le système d'exploitation mais aussi pour les interfaces et applications réseaux qu'ils proposent. Cette grande liberté de ce type de logiciel, associé au monde de l'*Open Source* (source ouverte), permet justement de développer, de créer, en fait de « construire quelque chose ».




BILL GATES
28 - 10 - 1955 8 - 8 - 1997
Where do you want
to go today ?



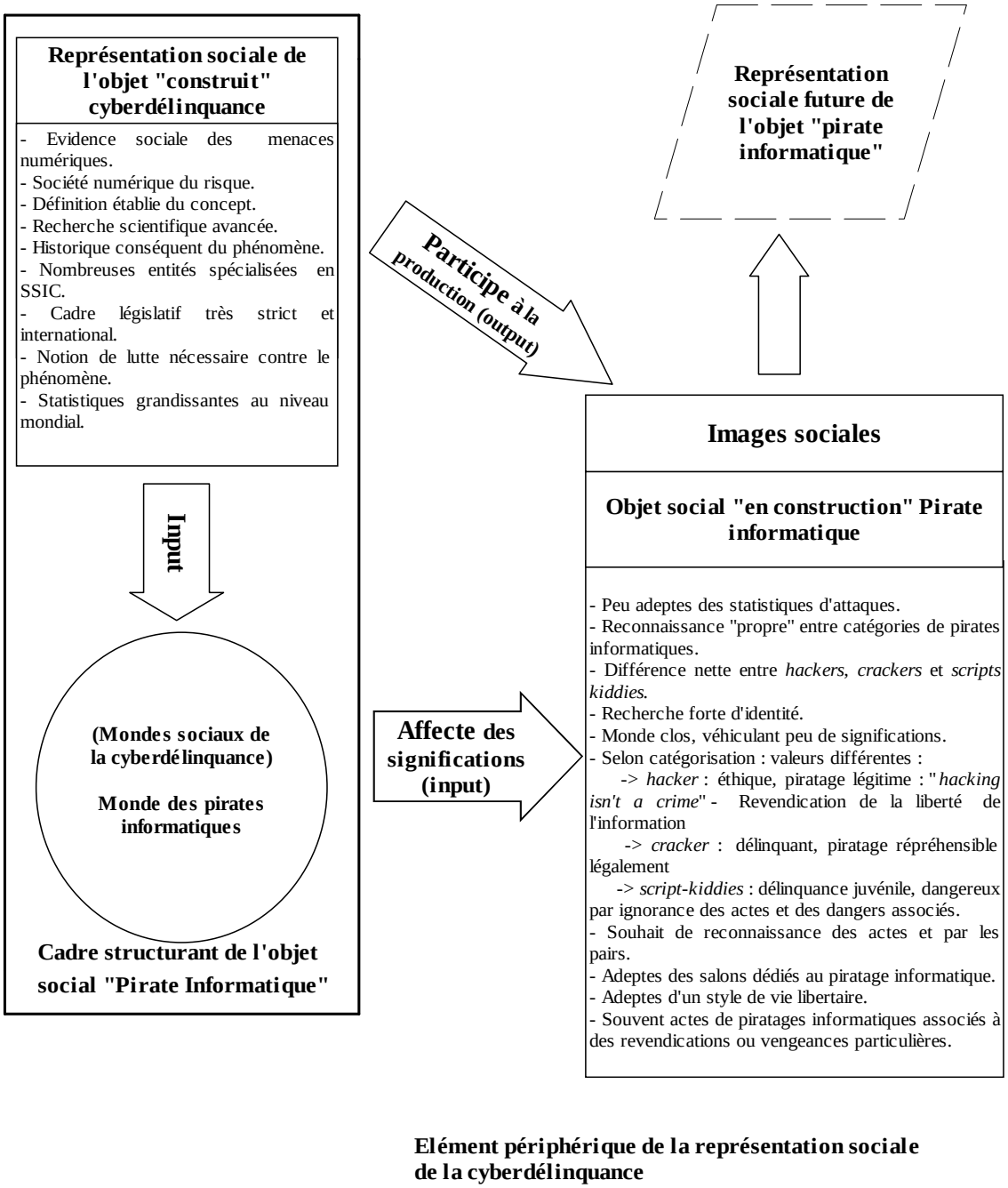


- Figures 17, 18, 19 et 20. *What the Hack*, 28 au 31 juilllet 2005

Le « *hack* » est finalement un esprit, véritablement opposé au cybercrime. Dans cet esprit il faut distinguer véritablement les « *hackers* » de véritables cybercriminels. Le cybercrime correspond à des attaques sur les réseaux et ordinateurs, mais finalement notre interlocuteur nous indique « *qu'est-ce qu'une attaque ?* », « *comment la qualifier en tant que telle ? Ne seraient-ce finalement pas simplement des paquets comme les autres qui passent sur le réseau ?* ». A l'extrême de la défense de la liberté de l'information, certains jugeraient facilement que le cybercrime n'existe pas. Enfin, notre cinquième interlocuteur nous a permis de prendre conscience de la criminalisation croissante de la cybercriminalité. Ce dernier est en relation avec le milieu *underground*, et au-delà du clivage entre les images sociales des acteurs de la cybercriminalité, ce dernier s'est rendu compte de la dérive récente des actes de cybercrime, notamment *via* les réseaux mafieux, en provenance des pays de l'Est. Pour ce dernier, il s'agit de la vraie cybercriminalité, qui n'hésite pas à « recruter » des pirates informatiques « en exercice » pour les utiliser à des fins malveillantes.

Ces aspects se traduisent également *via* les attaques croissantes sur les sites reliés à Internet. Actuellement, les *Intrusion Detection System* (IDS) sont « *plein à craquer* », et de nombreuses origines d'attaques proviennent de sites localisés en « .ru » (Russie) (sic).

- Figure 21. Modélisation graphique de la représentation du pirate informatique par le monde des pirates informatiques



III – Exemple de cas concret d'application de l'intégration des significations : le Grand-Duché de Luxembourg

Nous proposons de terminer notre étude par l'exemple de nos réflexions à la dimension d'un pays, le Grand-Duché de Luxembourg. L'« *étude de la mise en place d'un observatoire des menaces IT (Information Technology) au Grand-Duché de Luxembourg* » que nous avons menée, sera mise en lumière. Cette dernière fut présentée fin décembre 2006, pour le compte du Comité d'Accompagnement de la Plate-Forme d'Innovation « Sécurité de l'Information », en collaboration avec la structure CASES (Ministère de l'Ėconomie et du Commerce extérieur). Cet exemple détaillé, dans sa construction, nous permet de vérifier la construction culturelle d'un instrument de réponse à la cyberdélinquance, via un consensus de plusieurs parties, partageant les mêmes significations vis-à-vis de l'objet de recherche, validant au sein d'un monde l'interactionnisme symbolique productif, et la vision du monde social tel que le concept a été developpé par H.S Becker, participant alors à la construction d'un même objet.

1) Le besoin identifié d'une struture nationale d'observation des menaces IT

Un observatoire de la cyberdélinquance au G-D de Luxembourg demeure un outil de facilitation de connaissance, une aide à la compréhension *via* l'information et la communication, ainsi qu'une sensibilisation accrue (« *awareness raising* ») vis-à-vis du pirate informatique. Ce dernier objet étant en construction, il est important de considérer sa nécessaire observation, cela au niveau national et international.

L'objectif des travaux, qui ont conduit à la rédaction de ce rapport, était d'apporter des éléments d'analyse, et des scenarii sur la faisabilité de la mise en place au Grand-Duché de Luxembourg d'un observatoire des menaces de type IT. En effet, dans le cadre des réflexions stratégiques nationales actuelles, relatives aux perceptions et impacts de la cybercriminalité sur les réseaux d'information et de communication, l'enjeu de l'étude réside dans la mise en évidence des besoins nécessaires pour la mise en place d'un tel observatoire.

Il est désormais établi que les actes de cybercriminalité sont exponentiels, cela au niveau mondial (de nombreuses statistiques spécialisées, nous l'avons vu, déterminent cet état de fait (CSI/FBI, CLUSIF…)). Mais, si la démarche et les actes sont relativement connus, un véritable manque est, cependant, identifié au G-D de Luxembourg quant aux impacts véritables sur le territoire national de ces menaces. Cet état de fait justifie pleinement la réflexion de la mise en place d'un observatoire dédié à la mesure effective de ces menaces.

Depuis 2004, la sécurité de l'information fait l'objet d'une politique coordonnée par le gouvernement luxembourgeois. Le signe le plus concret et visible de cette politique est le site CASES (http://www.cases.public.lu), portail de la sécurité de l'information au Grand-Duché de Luxembourg. Il s'agit d'une des initiatives mises en œuvre dans le cadre du Plan Directeur National de la Sécurité des Réseaux. Le plan directeur a comme objectif d'inciter et d'aider toutes les parties concernées à mettre en place des politiques, procédures et outils de sécurisation efficaces pour contrer ces menaces.

Ce plan prévoit une collaboration étroite de toutes les parties concernées à un niveau national et international afin de créer une culture de sécurité et propose des actions dans les domaines suivants :

- **la prévention et la sensibilisation** : les pouvoirs publics doivent lancer des campagnes de sensibilisation et d'éducation. Le gouvernement doit mettre en place un système d'alerte ; [Ce premier pilier « sensibilisation » ayant d'ores et déjà été concrétisé par la mise en place de la structure CASES (*Cyberworld Awareness & Security Enhancement Structure*)] ;
- **l'intervention** : l'Etat doit mettre en place une structure capable de gérer rapidement et efficacement les incidents informatiques ;
- **l'investigation** : les moyens et les techniques d'investigation doivent être améliorés ;
- **la législation :** la législation luxembourgeoise ainsi que ses moyens d'action doivent être améliorés de façon à permettre une poursuite efficace de tout crime informatique.

Le plan fait appel aux citoyens, au secteur privé et public, financier, des télécommunications, de la santé ainsi qu'aux chambres professionnelles et patronales afin

de collaborer étroitement à la mise en place de structures nationales répondant aux actions de sécurité décrites. Cette perspective montre clairement, une interculturalité de fait, instrumentalisée, *via* la prise en compte des significations de chaque membre, par des structures de sécurité de l'information et de la communication se mettant en place progressivement au G-D de Luxembourg.

Ainsi, afin de poser la réflexion, il fut donc convenu, au niveau national, de procéder à une étude de réalisation de mise en place, après CASES, d'une structure de réponse sur incident IT, tout en tenant compte des significations de chaque partie (cette étude a été menée conjointement par CASES et le CITI (PFI Sécurité – Projet de Recherche R2SIC (voir supra))). Trois chapitres principaux composent cette étude résolument conduite dans le but de fournir des pistes concrètes de réalisation.

Une première partie consiste à recenser les informations disponibles sur ce domaine en effectuant une veille technologique recensant un échantillonnage de l'ensemble de la documentation disponible au niveau international (voir annexe 11), d'en proposer une synthèse à des fins didactique, tout en faisant le point sur les initiatives passées, et en cours dans les pays voisins du G-D de Luxembourg (cartographie).

Une deuxième partie s'attache à établir le contexte du cybercrime au G-D de Luxembourg. Pour ce faire nous prendrons en compte la mesure des significations des parties prenantes, en utilisant notre questionnaire réalisé pour le sondage (vu en deuxième partie – I – 2) ; voir annexes 6 et 7).

Enfin, la troisième partie vise à recenser, vis-à-vis de la problématique « *reporting* du cybercrime au G-D de Luxembourg », les besoins ressentis par l'ensemble de la communauté luxembourgeoise concernée, dans le domaine de la sécurité des systèmes d'information, plus particulièrement les membres du CAP de la PFI Sécurité du Centre de Recherche Public Henri Tudor (CITI)[256].

[256] Le CAP PFI Sécurité a mandaté le CRP Henri Tudor pour réaliser cette étude de faisabilité pour la mise en place de ce type d'observatoire « sécurité » au G-D de Luxembourg (Décision CAP PFI Sécurité du 07/03/2006 - CRR4_20060307 CAP SECURITE V1.0).

Ces trois chapitres permettront de définir les différents scenarii pour la mise en oeuvre d'une telle infrastructure, en regard des résultats fournis, de manière inter-significative entre les parties prenantes.

Cette étude vise la pérennisation de la collaboration des différents acteurs de la sécurité sur cette thématique, en fédérant les besoins. Convenue comme un avant-projet de recherche, elle fut menée comme telle, avec cet objectif de dessiner les contours d'un projet de recherche rejoignant l'ensemble des exigences des partenaires, du G-D de Luxembourg, et la mise en valeur des résultats de l'étude, mais ne se substituant pas à tout autre scénario possible. Un but doit être privilégié : permettre le suivi annuel au G-D de Luxembourg de la progression des incidents et des menaces IT (tendances, impacts, préjudices au niveau national), *via* une structure pérenne de type « observatoire des menaces ». Nous présentons ci-après, les principaux résultats utiles à notre propos.

2) Le domaine de la réponse sur incidents (recherche et veille)

Un observatoire national des menaces IT doit permettre de rendre compte de la situation relative aux différentes attaques menées sur le territoire numérique luxembourgeois. Le noyau central de cette observation est le relevé de l'incident de sécurité. L'incident de sécurité peut être vu de différente manière :

- un incident de sécurité non relevé ne peut être traité,
- un incident peut-être relevé et stoppé, voire contré,
- un incident peut être relevé et non archivé en tant que tel,
- enfin un incident peut faire l'objet d'une réponse sur incident.

Ces différents cas de traitement d'un incident de sécurité ont guidé notre réflexion pour la mise en place d'un observatoire des menaces IT au Luxembourg. En effet, la façon dont les incidents sont pris en compte peut engendrer des impacts sérieux et préjudiciables, pour l'entité concernée mais aussi pour l'ensemble de la communauté interconnectée (Exemple : en 1988, Robert Morris, le fils d'un des principaux scientifiques du *National Computer Security Center*, « lâche » dans la nature le premier ver Internet, qui va se répandre sur 6000 machines connectées). Depuis, de nombreux CSIRT ont été mis en place.

Note : « *What is a CSIRT?* » *:* CSIRT signifie « *Computer Security Incident Response Team* ». Ce terme est utilisé de manière prédominante en Europe en regard du terme CERT qui est protégé, et sous *copyright* aux Etats-Unis par le CERT-CC. Différents termes sont utilisés pour ce domaine de la réponse sur incidents : CERT (*Computer Emergency and Response Team*), CSIRT, IRT (*Incident Response Team*), CIRT (*Computer Incident Response Team*), SERT (*Security Emergency Response Team*), plus localement CSRRT (*Computer Security Research & Response Team*). Pour notre part, nous avons choisi le terme globalisant d'observatoire des menaces IT, sachant que différents services peuvent être proposés par l'ensemble des structures présentées.
Il existe environ une centaine de « CSIRT » actuellement recensés en Europe[257].

La définition d'un CSIRT est la suivante : « *Un CSIRT est une équipe d'experts sécurité dont le travail est de répondre aux incidents de sécurité informatique. Il fournit les services nécessaires afin de les traiter et soutenir leurs composants pour combler leurs brèches* »[258].

Deux axes ont pu alors guider notre réflexion quant aux missions de l'observatoire des menaces luxembourgeois :

- les services réactifs de réponse sur incidents,
- les services proactifs.

Comment un pays peut-il relever et répondre aux incidents de sécurité ? Plusieurs services peuvent être proposés par l'observatoire :

- Une surveillance constante est en place, dès qu'un incident est détecté, l'observatoire peut être averti immédiatement. Modèle passif de la détection d'intrusion, il est le plus simple à mettre en place. La plupart des systèmes d'information permettent de mettre en place des outils de surveillance dont les sorties peuvent être étudiées pour déceler des indications d'attaques. Ces informations peuvent alors être véhiculées vers l'observatoire. Cependant, dans ce cas, il faut un *reporting* actif de la part des victimes.

---

[257] ENISA Inventory, http://www.enisa.eu/ENISA%CERT/index.htm.

[258] « *A CSIRT is a team of IT security experts whose main business is to respond to computer security incident. It provides the necessary services to handle them and support their constituents to recover from breaches* ».
ENISA, 2006, *A step by step approach on how to set up a CSIRT* (Deliverable WP2006/5.1 (CERT – D1/D2).

- Remédier (réparation) à l'incident, le plus rapidement possible, afin de poursuivre les activités normales avec une perte de temps minimale. Pour cela, auparavant, le repérage de l'incident a été effectif, un remède apporté, et l'attaque bloquée. A ce niveau, il faut empêcher le développement actif de l'attaque et obtenir les informations de génération et de propagation afin d'éviter la multiplication d'attaques semblables.

- Poursuivre en justice. Après avoir rassemblé les preuves, et suivi en interne la procédure de poursuite (avec caution du service juridique), tout en tentant de poursuivre l'observation et d'enregistrer les faits, si cela est possible. Ensuite un dépôt de plainte demeure le stade ultime de la poursuite.

- Importance de la mise en place d'un plan de réponse interne (côté victime). Le rôle d'un organisme est de prévenir le vol d'information, de protéger la vie privée, l'intégrité des données sensibles, de prévenir l'interruption de services et de sensibiliser le personnel pour atteindre ces objectifs *via* notamment un moyen : un mécanisme de réponse sur incident (un outil de décision) qui évalue la situation problématique et détermine rapidement une solution de reprise, détermine les attaquants, et permet de prendre des mesures légales ou administratives contre les attaquants. Le but principal est de mettre en évidence la (les) atteinte(s) illégale(s) et déterminer l'identité des attaquants (responsables).

Quel que soit le service offert par l'observatoire, la victime doit avoir prévu un plan de réponse sur incidents, déterminant les procédures à exécuter et les responsabilités engagées. Il permet à l'entreprise de s'organiser, chacun sachant alors exactement ce qu'il doit faire. Cependant chaque organisme peut décider de l'importance de ce plan de réponse sur incident (selon : surveiller et avertir, réparer et signaler ou encore poursuivre en justice). La documentation associée à l'incident de la victime est, quoi qu'il en soit, un pré requis nécessaire pour l'observatoire (spécifiquement pour un service visant à remédier à incident). L'incident doit être le plus détaillé possible : nécessité de remplir un « ticket » d'incident par la victime et d'utiliser un outil de gestion des incidents pour l'observatoire.

L'incident de sécurité est le noyau central de l'activité d'un observatoire national des menaces IT. Sans cette matière première : impossible pour une telle structure de décliner son rôle d'observation, ni les axes suivants que sont la réponse et l'évolution de l'état de sécurité IT au niveau national. Ainsi, les incidents de sécurité IT enregistrés au Luxembourg doivent pouvoir converger vers l'observatoire de manière certaine, tout en assurant une confiance sans faille sur le traitement associé.

Sans nul doute, de nombreux incidents de sécurité sont relevés sur le territoire luxembourgeois, que ce soit par le secteur privé ou public, cependant aucun organisme ne les centralise aux fins d'effectuer un historique, un reporting, une analyse, des recoupements, une veille, des statistiques, etc…

Pour ce faire, l'ensemble des secteurs économiques doit pouvoir, en toute sérénité (en tenant compte de leurs exigences), transmettre ses incidents, aux fins de retour vers la totalité des autres entités connectées sur le territoire numérique luxembourgeois, et ainsi rendre possible un reporting des menaces spécifiques actives au G-D du Luxembourg. Afin de gagner la confiance et devenir incontournable un observatoire des menaces doit présenter des services clairement identifiés. Ainsi, il s'agit, dès le départ, de faire des choix, lors de la mise en place d'une telle structure, qui déterminent ensuite les ressources, les compétences, les partenariats dont l'équipe mise en place aura besoin pour fonctionner correctement. Les services offerts doivent être réalistes et honnêtes (« *mieux vaut offrir peu de services que beaucoup pauvrement…* »[259]). Ainsi, chaque observatoire est différent selon ses missions, buts, et la consistance de l'équipe en place. Les principaux relevés actuellement sont principalement des services proactifs, réactifs sur incidents de sécurité, et de gestion de la qualité de la sécurité[260]. Le service de traitement d'incident de sécurité est le pré requis à considérer pour un observatoire. Il apparaît, de l'expérience de la mise en place des différents CERT au niveau international[261] que, quels que soient les services choisis par l'observatoire, il demeure primordial, et c'est un

[259] Carnegie Mellon University (2002, CSIRT Services) - Stelvio bv, The Netherlands; PRESECURE Consulting GmbH, Germany.

[260] A step by step approach on how to set up a CSIRT (ENISA, 2006) - Deliverable WP2006/5.1 (CERT – D1/D2).

[261] Carnegie Mellon University (2002, CSIRT Services) - Stelvio bv, The Netherlands; PRESECURE Consulting GmbH, Germany.

facteur de succès, de mettre en place une équipe suffisamment consistante pour fournir une véritable valeur ajoutée aux membres de la communauté. Sinon l'observatoire ne sera pas un succès et ses membres ne lui communiqueront pas d'incidents de sécurité [(SIC) in : *CSIRT Services*; Stelvio bv, The Netherlands; PRESECURE Consulting GmbH, Germany Carnegie Mellon University, 2002].

Dans ce cadre, notre étude a notamment permis de rencontrer le CERT-A (Administration en France) pour un retour d'expérience, en « *input* » pour nos besoins. Les organismes de contrôle français en matière de sécurité (SGDN, DST et DCSSI) ont créé deux CERT en France, un dédié aux administrations (le CERT-A), le deuxième pour le monde de la Recherche et de l'Education (le CERT RENATER). Un troisième CERT a été créé pour le monde de l'Industrie (le CERT-IST : Industrie, Services, Tertiaires) par quatre partenaires le CNES, Alcatel, France Telecom et Sanofi-Synthèlabo.

- Exemple de retour d'expérience avec le CERT-A. Le Centre Opérationnel de la Sécurité des Systèmes d'information (COSSI) en France est composé de la Cellule de veille SSI (CEVECS - création en 2003) et du CERT-A (création en 1999) qui en est la cellule technique. Le COSSI dépend du Premier Ministre/SGDN/DCSSI/SDO (Sous Direction Opérations). En France il existe une chaîne fonctionnelle relative aux incidents : un Fonctionnaire de la SSI (FSSI) qui dépend du HFD au sein de chaque Ministère. Le FSSI est le centralisateur des incidents.

Le CERT-A a pour partenaires : FIRST, TF-CSIRT, CERT Gouvernementaux, CERT français, etc... Cet organisme réalise des notes d'information, travaille sur les alertes des pare-feux des différents Ministères (veille de jour, et veille de nuit active. A tout moment quatre personnes au minimum sont rapidement mobilisables au COSSI).

3) Perception du cybercrime au G-D de Luxembourg

Dans le but de décrire ce que l'on appelle les attaques sur les réseaux de l'information et de la communication, des termes aussi divers que : « cyberdélinquance », « crime numérique », « crime binaire », ou encore « cybercrime » peuvent indifféremment être utilisés. Afin de conserver une homogénéité dans la reconnaissance

sociétale et fédératrice du terme, nous conserverons le terme de « cybercrime » pour la description de ce phénomène. Quel est-il au Grand-Duché de Luxembourg ?

Quelle est l'importance du cybercrime ainsi que son impact au Luxembourg ?

Il est toujours difficile de donner une réponse officielle à cette question, d'autant plus qu'il n'existe pas de structure nationale de type CERT (*Computer Emergency & Response Team*) « officiel », en charge de relever les incidents de sécurité de ce type, de les traiter, de les synthétiser et de communiquer à leur propos, dans le but d'améliorer la sécurité des infrastructures numériques en place. Ainsi, il est presque impossible de quantifier, voire de qualifier objectivement (de manière globale) les cybermenaces actives au Luxembourg. A ce jour, seule une structure de type A.S.B.L (C.S.R.R.T - *Computer Security Research & Reponse Team* – http://www.csrrt.org.lu) joue ce rôle au Grand-Duché et est reconnue en tant que telle par l'agence européenne de la sécurité de l'information, plus connue sous le dénominatif d'ENISA (*European Network & Information Security Agency* – http://www.enisa.eu.int).

La majorité des pays, au niveau international, s'est organisée « pour faire face à une menace globale, par une réponse globale », généralement en mettant en place au moins une structure de type CERT, souvent nationale, voire parfois plusieurs par secteur d'activité économique. Pour l'heure, ce type de structure n'a pas encore été créé au Luxembourg, néanmoins, une telle réalisation est prévue et mentionnée dans le pilier numéro deux du Plan Directeur National de la Sécurité des Réseaux Luxembourg, qui en compte quatre au total.

Autant de questions auxquelles nous avons tenté de répondre *via* le seul terrain d'observation innovant, disponible au Grand-Duché du Luxembourg, à savoir le projet « *HoneyLux* » qui s'inscrit dans le cadre international du *HoneyNet Project* (www.honeynet.org). *HoneyNet* est un projet de Recherche reposant sur le volontariat et qui fédère l'ensemble des *HoneyPots* disponibles sur Internet. Les *HoneyPots* (littéralement pots de miel) visent à piéger des *crackers* afin d'étudier leurs techniques d'attaques. *HoneyNet* est littéralement un réseau d'*HoneyPots*. *HoneyLux* est un *HoneyPot* luxembourgeois (sachant que la plus forte présence *HoneyPots* se situe aux

Etats-Unis) constituant un véritable projet de recherche et reposant sur le volontariat des organisateurs, chercheurs et autres participants. Il est constitué de machines interconnectées sur Internet à partir du territoire luxembourgeois, apparaissant de manière anonyme (implantation confidentielle), telles des machines de production classiques. Ainsi, *HoneyLux* est actif depuis quatre ans au Grand-Duché du Luxembourg et vise à capturer les traces de piratages informatiques, pour ensuite les étudier et en tirer des enseignements sur les techniques utilisées par les *crackers* ; traduisant de facto la menace du moment sur le réseau Internet. A l'inverse d'une approche théorique, *HoneyLux* vise une approche purement pratique dans le but principal de mieux appréhender les difficultés rencontrées sur le terrain ? Ceci, dans l'optique de déceler les nouvelles attaques, de manière à mieux s'en protéger. L'intérêt réside également dans le fait que *HoneyLux* capte les attaques mais les stocke également, ce qui permet de les analyser plus en profondeur. Nous avons vu que cela permet d'effectuer une analyse de type « légiste » (*Forensic Analysis*) de l'entrave à l'information et à la communication.

De manière générale, il faut savoir qu'une machine *HoneyLux* est attaquée dans la minute suivant sa mise en ligne sur Internet… Cependant, avant toute analyse, déterminons notre problématique en définissant la cybercriminalité, ainsi que ses principaux acteurs ; le cadrage du cybercrime peut être perçu *via* la rédaction de la première partie du « *Panorama Cybercrime Luxembourg 2006* » dont voici un extrait (l'intégralité peut être lu en annexe 12) : « *Le cybercrime est désormais un véritable état de fait. L'ensemble des nations a tôt fait de réagir en mettant en place des contre-mesures (le plus souvent d'envergure) vis-à-vis de cette menace. De nombreux pays se sont sérieusement organisés dès le développement exponentiel d'Internet, notamment lorsque les offres de connexion sont devenues possibles vers le citoyen. Ainsi, la France a, par exemple, dès 1994, mis en place des services de police spécialisés pour non seulement lutter contre la cybercriminalité, mais aussi pour sensibiliser les entreprises à la nécessité de se protéger contre ces nouvelles menaces à l'encontre de l'information et de la communication publiquement mises en réseau. Très tôt, le basculement de l'économie vers le numérique, associé à sa mise en ligne vers des réseaux publics, rencontra les inquiétudes étatiques, les gouvernements craignant concrètement une menace pour ce modèle de développement économique via les réseaux, devant plutôt*

globalement être soutenu (Initiative e-Europe de l'Union Européenne), et non soumis aux diverses tentatives possibles de dégradations/détériorations/destructions. La multiplication des affaires de piratages informatiques (vol d'informations, espionnage d'informations, « défiguration » de sites web, mise hors service de sites,…) a donc considérablement renforcé les initiatives de protection des pouvoirs publics.

La première loi concernant directement la criminalité informatique et la répression de la cyberdélinquance a été adoptée en 1984 aux Etats-Unis (Comprehensive Crime Control Act), et rapidement amendée par le Computer Fraud and Abuse Act de 1986 qui criminalise six types d'accès frauduleux aux systèmes informatiques, en fonction de la finalité de l'opération d'intrusion réalisée.

En France, les enjeux de la sécurité informatique ont été pris en compte dans la loi Godfrain du 05 janvier 1988, reprise dans le Nouveau Code pénal sous les articles 323-1 et suivants. En cette matière l'arsenal juridique est formé de trois délits distincts, visant les atteintes aux systèmes et les atteintes aux données.

Au Luxembourg, la loi du 15 juillet 1993 détermine les infractions pénales informatiques, s'inspirant fortement de la loi Godfrain (France) :

- article 509.1 : Accès frauduleux ou maintien non autorisé dans un système de traitement ou de transmission de données.

- article 509.2 : Entrave intentionnelle au fonctionnement d'un système de traitement de données.

- article 509.3 : Introduction intentionnelle, directe ou indirecte, de données dans un système de traitement de données, suppression ou modification de données, suppression ou modification des modes de traitement ou de transmission de données.

Pour ces trois infractions les peines encourues varient entre 2 mois et 3 ans d'emprisonnement et entre 500 et 25 000 Euros d'amende.

- Qu'est-ce que la cybercriminalité ? (http://www.cases.public.lu)

La cybercriminalité se définit communément, comme toute action illicite, visant l'intégrité d'un site informatique déterminé, ou bien menée à l'aide d'un outil informatique. Cette définition se décline selon l'utilisation faite du médium informatique. En effet, soit ce dernier est utilisé par le délinquant comme outil d'un délit ou d'un crime

conventionnel (escroquerie, menaces…), soit l'ordinateur est la cible même visée par le délinquant (vol, utilisation frauduleuse ou encore destructions de données,…) ».

Perception locale du cybercrime et de ses acteurs principaux

La nécessité d'un tel observatoire requiert une vérification des besoins ressentis au niveau national, permettant de déterminer la représentation associée à notre objet de recherche, mais aussi par extension à la mise en place d'une telle infrastructure. Pour ce faire, une partie des acteurs clés de la sécurité au Grand-Duché de Luxembourg ont été rencontrés, plus particulièrement les membres du Comité d'Accompagnement de la Plate-Forme d'Innovation Sécurité du CRP Henri Tudor (voir Titre III – I – 2)), partenaires privilégiés et à l'origine de cette étude.

Un questionnaire a été mis en place ; il vise à percevoir les besoins d'une structure de type observatoire des menaces IT au Grand-Duché de Luxembourg (il s'agit essentiellement d'un guide de conversation, ayant laissée libre notre discussion avec l'interlocuteur). Dans le cadre de leur suivi, les partenaires du Comité d'accompagnement ont répondu à ce questionnaire, ce qui a permis d'enrichir l'étude :

- 17/05/2006 : M. Steve Breier (Chambre de Commerce Luxembourg)
- 19/05/2006 : M. François Thill (Ministère de l'Economie et du Commerce extérieur)
- 24/05/2006 : M. Jean Trimbour (Luxinnovation)
- 24/05/2006 : M. Pierre Weimerskirch (Commission Nationale pour la Protection des données)
- 26/05/2006 : M. Nico Binsfeld (Association des Professionnels de la Société de l'Information (APSI))
- 30/05/2006 : MM. Jérôme Carrère et Brenna (Telindus)
- 07/06/2006 : M. Thomas Tamisier (CRP Gabriel Lippmann)
- 17/07/2006 : M. David Crochemore (CERT-A France)
- 02/08/2006 : M. Jean-Yves Kayser (Chambre des Métiers)
- 02/08/2006 : MM. Alexandre Dulaunoy et Fred Arbogast (CSRRT)
- 07/08/2006 : M. David Hagen (CSSF – Commission de Surveillance du Secteur Financier)

- 08/08/2006 : M. Houtsch Patrick (CIE – Centre Informatique de l'Ėtat)
- 11/08/2006 : MM. Ourdane Mohammed et Julien Pereira (P&T Luxembourg)

Des divers entretiens (les opinions sont respectées, aucun lien direct ne peut être fait entre un interlocuteur et une réponse particulière), il ressort les points suivants pouvant être utilement retenus dans le cadre de notre étude.

- Le « *reporting* » des besoins :

1 - La perception du cybercrime de manière générale : le contexte international (synthèse des entretiens menés)

Les définitions :

Des différents entretiens, il ressort le plus souvent la définition suivante du terme « cybercrime », tenant compte de la dichotomie des termes « cyber » et « crime » :
- Cyber : ce qui fait appel au virtuel, généralement lié aux aspects des NTIC.
- Crime : ce qui fait appel à la loi, tout ce qui va fortement à son encontre. Ce qui est légalement qualifié.

La distinction entre cybercrime et cyberdélinquance a également été précisée, beaucoup de faits répertoriés en cybercrime, ne correspondent pas forcément au fait, ce sont aussi parfois des erreurs, des problèmes techniques. Le cybercrime serait surtout en lien avec une caractéristique fortement pénale : à savoir l'intention coupable, l'intention de nuire fortement. Ainsi, certains chiffres de préjudices qualifiés de « cybercrime » peuvent apparaître exagérés (le lien vers le rapport CSI/FBI est souvent pris en exemple comme une vue quantitative difficile à intégrer, à expliquer). Parfois aussi, le crime binaire ne correspond qu'à la recherche du plaisir ludique.

Cependant, il ne faut pas occulter la réalité, chaque jour des *I.D.S.* (*Intrusion Detection System),* au G-D de Luxembourg, bloquent actuellement des attaques de haut niveau en provenance de « .ru » (Russie), par exemple, ce qui ne signifie cependant pas que les attaques proviennent forcément de ce pays (des pratiques de rebond étant fortement possibles). La tendance aux attaques massives sur des « *exploits* » (vulnérabilités identifiées) *Microsoft* est également forte actuellement et mise en

évidence. Au cours des entretiens menés, nous avons déterminé des problèmes de définition claire du terme « cybercrime ». En effet, la perception des significations varie fortement selon les différentes personnes rencontrées. Seule une référence fut fournie de manière très précise à savoir la définition du *Computer Crime Research* (Unité de Recherche en criminalité informatique) qui distingue trois catégories, selon la cible victime :

- Crime informatique contre des personnes (pédophilie, dommages divers, *happy slapping*…).
- Crime informatique contre la propriété (destruction de site, virus, vol de propriété intellectuelle (à distinguer si but avantage concurrentiel) etc…),
- Crime contre un gouvernement (notion de terrorisme informatique).

Cette classification démontre un esprit différent selon ces différents aspects : les motivations sont pour chaque cible différentes : le cyberterrorisme vise notamment à la déstabilisation d'un pouvoir, par exemple. Il apparaît aussi important de faire la distinction entre les attaques à l'aveugle sans cible déterminée, et celle prenant pour cible une organisation précise.

Nous pouvons finalement retenir une définition qui recueille un certain consensus par l'ensemble des partenaires : le cybercrime correspondant à toute activité illégale (le terme crime fait référence à un cadre précis de sanctions prévues par la loi) qui utilise l'ordinateur soit comme outil (copie de CD, « faire de l'argent », pédophilie, terrorisme, vente et communication) soit comme cible par différents types de personnages dans différents buts (jusqu'au niveau espionnage *via* les réseaux, mais également les attaques des réseaux publics d'information ; toute attaque possible : déni de service, espionnage…).

Souvent les articles de loi luxembourgeois « 509 » sont connus des personnes avec lesquelles nous nous sommes entretenues. Ces articles définissent *de facto* au mieux le cybercrime. Des différents entretiens, il ressort également que l'avis quant au sens commun sociétal du cybercrime est souvent compris comme les activités liées aux activités de virologie informatique (le pirate informatique étant celui qui programme ce type de virus). Par contre, les aspects de copies pirates de CD ou autres œuvres faisant

l'objet de droits d'auteur sont souvent exclus de ce champ en terme de représentations sociales.

Les aspects d'attaques externes sont un fait, cependant, ce n'est que la partie visible (fait souvent appel au « spectaculaire » *via* la presse), ce qui est jugé d'importance sont principalement les attaques internes.

Importance du phénomène ?

Ce type de menace semble augmenter à tout niveau en terme d'exposition ; il semble nécessaire de comprendre et savoir ce qui se passe sur le terrain numérique. En effet, l'absence d'information peut entraîner aussi des abus autres que l'absence de sécurité. Ainsi, certains pourront exploiter la peur des risques et de l'insécurité totale pour vendre plus et pas forcément de manière adaptée. Cependant, la plupart des interlocuteurs ne savent qualifier clairement ce qui se passe réellement. La connaissance ne doit, de plus, pas venir uniquement de l'étranger et les menaces enregistrées localement doivent être connues. Finalement, en termes de cybercrime, le danger est estimé globalement réel et sous-estimé : *« Heureusement il n'y a encore pas eu de gros problème de phishing ; néanmoins des nuisances très grandes sont possibles ! Il semble donc nécessaire de former et éduquer en conséquence et ne pas attendre de subir les événements* » (sic).

Le phénomène semble véritablement en croissance exponentielle, pour preuve, par exemple, le développement des attaques de type *malware* (*malicious software*, logiciel malveillant), la tendance à l'espionnage, au *pharming*, au *phishing*, ou encore *chevaux de Troie*, avec une criminalisation croissante des faits. Une sensibilisation adaptée s'impose donc, notamment face aux actions des utilisateurs, mêmes protégés techniquement. *« Le phénomène semble important mais demeure difficilement mesurable, et les médias paraissent montrer ce qu'ils veulent laisser voir. Le cybercrime demeure un outil de l'espionnage économique* » (sic).

Le danger repose aussi dans la perte de communication, par exemple la saturation réseau. Mais, en terme de conséquence aussi, la réputation de l'entreprise, la perte d'information (manque à gagner), l'impact financier direct reste difficile à déterminer.

La prise en compte du phénomène demeure primordiale ; les préjudices sont multiples pour le particulier, pour le citoyen : risque pour les cartes bancaires volées, … Le cybercrime nuit au développement des sociétés, les coûts des réparations sont très importants et il faut une approche systématique, pour développer son système en toute sécurité. Une réflexion globale semble nécessaire. Il faut alors anticiper les menaces, apporter des réponses claires et donner des directives pour les preneurs de décisions : « *Les décideurs sont non spécialistes ! Il faut une information claire ! : il faut éclaircir et communiquer simplement* » (sic). Les entreprises s'informatisent, et le cybercrime augmente en fonction. Il appert important, au moins, de les sensibiliser. Au-delà de la réalité technique, il ne semble pas qu'on puisse stopper le cybercrime avec des techniques, même s'il faut maintenir le niveau, il faut surtout rendre conscient l'utilisateur du fait et tenir compte de l' « humain ». Il semble important d'expliquer la sécurité, son champ. « *C'est une notion de civisme numérique : au G-D de Luxembourg, lors de l'achat de machines, le vendeur ne conseille pas le client sur les aspects sécurité, une fois connectées, et sous ADSL, elles sont le plus souvent rapidement « blacklistées* » *(littéralement en « liste noire »), et surtout piratées* » (sic).

Les régulateurs et ISP (Internet Service Provider – Fournisseur d'accès Internet) peuvent aussi agir en réaction à des machines pouvant poser problème et débrancher le « responsable ». « *Le problème est certain lorsque des utilisateurs ne « patchent » pas (« patcher » : action de corriger une vulnérabilité) alors que d'autres testent ces failles non patchées »* (sic). Il semble important de communiquer l'information pour les autres ; le G-D de Luxembourg est une cible non négligeable pour tout ce qui est *phishing* notamment. Sur le réseau *honeylux*, par exemple, un serveur de ce type a été mis en place : 100 personnes sur 30000/400000 mails envoyés ont transmis leurs coordonnées personnelles. Les activités de *Botnets* (réseau de « robots ») sont aussi légion avec une forte activité de chantage (Exemple : demande de 5000 euros pour libérer le « bourrage » de ligne). « *Les ISP peuvent parfois devenir trop radicaux dans leurs actions de sécurisation, par exemple supprimer le « port 25 » trop vulnérable, et le citoyen ne peut alors plus installer un serveur mail* » (sic).

Finalement, l'observatoire peut apporter le moyen aussi de faire le tri dans ce qui se passe en terme de problèmes sur les activités « *undergrounds* » : « *Dire ce qu'il en est*

vraiment des attaques, la réalité des faits, afin d'écarter les incertitudes. Les dangers concernent autant les vers Internet que de véritables attaques prenant directement la machine pour cible » (sic).

Vue du phénomène ?

« *Avoir une vue statistique serait une bonne idée pour le G-D de Luxembourg, un encouragement moral et financier, très visible. Les préjudices rapportés ne sont qu'une « partie de l'iceberg ». L'idéal est de pouvoir prévenir ce phénomène ; il est possible d'être une proie soit facile, soit difficile, et il est primordial que le G-D de Luxembourg soit une proie difficile à atteindre. En terme de prévention, idéalement l'ISP peut bloquer les sources d'attaques interne et/ou externe. Une surveillance demeure, en effet, la bonne approche. Un observatoire peut, par exemple, relever les informations transmises par les ISP, par dénonciation ou par détection d'attaques virulentes : des sanctions peuvent alors être possibles* » (sic).

Il est difficile de connaître le coût des impacts au G-D de Luxembourg, une seule personne a été condamnée pour de tels faits (une fiche réalisée par CASES détaille à ce titre comment déposer plainte en cas de piratage informatique). Quant au ROI (*Return of Investment – Retour sur investissement*) des dépenses de sécurité : comment le calculer ? Le fait de connaître les menaces réelles pour les consultants est important afin d'orienter correctement leurs différentes offres de services et pouvoir les adapter au contexte. Cependant, le calcul du ROI reste difficile à déterminer.

Les interlocuteurs relèvent qu'il est primordial de se protéger, et donc de montrer les risques et les contre-mesures : « *Il faut clarifier les dangers : ne pas montrer le catastrophisme ; et surtout faciliter la compréhension de l'utilisateur ! On adapte ainsi la couverture du risque…ce sera moins coûteux si des contre-mesures sont en place. Il faut inventorier les mesures à prendre (les contre-mesures) et adapter la couverture du cybercrime aussi. Si les bases sont solides, à mesure de prévention : les choses peuvent se faire de manière favorable au développement de l'activité* » (sic).

Des chiffres officiels du G-D de Luxembourg seraient alors intéressants car adaptés véritablement à son contexte. Les chiffres des autres ne peuvent, en effet, suffire

pour éclaircir le phénomène national. Quelles menaces « impactent » réellement le pays ? « *Le cybercrime passe aussi par l'espionnage industriel* » (sic).

L'importance de sites comme *SANS, Security Focus,* et *CERT CC* est, de même, mise en évidence, par nos interlocuteurs.

2 - La perception du cybercrime au Luxembourg (synthèse des entretiens menés)

L'absence de mesure fédérée nationale est reconnue comme un problème. « *En effet, il n'y a pas de raison de ne pas être « touché » au G-D de Luxembourg ; le fait est que de gros dégâts n'ont pas été reportés pour l'instant. Cependant, les IDS (Intrusion Detection Systems) sont « pleins à craquer », et de plus les attaques de type « social engineering » ne sont pas relevées* » (sic). Souvent, l'information sur un problème particulier est ponctuelle. « *Une grande banque aurait même connu des soucis de crime informatique récemment, au niveau national* » (sic). La tendance actuelle pourrait être critique pour le G-D de Luxembourg, notamment avec le « *phishing* », en effet la majorité des banques luxembourgeoises (40 % du PIB) sont en ligne ; de telles attaques pourraient « décrédibiliser" le G-D de Luxembourg. Ainsi, la baisse de la qualité/sécurité pourrait poser un risque certain en terme de clientèle bancaire notamment. Il importe donc de traiter correctement le cybercrime pour assurer une image de qualité pérenne du G-D de Luxembourg, le pays doit être précurseur dans la recherche des solutions relatives à la préservation de l'intégrité de son image, et aux moyens de répression pour ceux qui voudrait l'atteindre : une garantie doit être possible. L'état luxembourgeois doit donc permettre la répression. La perception du phénomène est cependant difficile ; « *Les luxembourgeois sont très attentifs à ce phénomène, les entreprises et les particuliers aussi ; vu la comparaison avec les autres pays, les enjeux de sécurité sont bien compris par les utilisateurs, ils sont bien encadrés. Les ISP au G-D de Luxembourg sont au courant des rebonds, il existe de nombreux outils qui tournent et collectent de l'information. Souvent, il manque un interlocuteur. Surtout le phénomène ne s'arrête pas aux frontières* » (sic). Même si le G-D de Luxembourg n'est pas forcément une cible, il peut le devenir, car il s'agit d'un pays évolué et « riche » (économiquement) pouvant attirer les convoitises, il n'y a aucune raison que ce pays ne soit pas concerné.

Notamment dans le domaine bancaire : 99 % des cas de vers et virus concernent ces institutions, 1 % des cas de SQL injection (NESSUS, actions de script-kiddies : « .ru » et « .lu »). De plus, les PC (*Personal Computer*, ordinateur personnel) Windows directement reliés à Internet sont généralement piratés en quinze minutes. Cependant, parfois, trop de sécurité peut aussi bloquer et limiter les utilisateurs.

Les entreprises luxembourgeoises sont concernées par le phénomène de cyberdélinquance, mais elles ne sont certainement pas véritablement conscientes du fait. « Surtout les PMEs et TPEs, quid de la protection de leurs bases de données ? Les grandes entreprises (grande banque, centres de recherche) semblent mieux protégées que les petites, les menaces ne sont pas les mêmes en fonction de leur taille.

« *La plupart d'entre elles n'ont cependant pas conscience de la valeur de leurs biens !* » (sic). Des sociétés sont très sensibles et nécessitent des protections particulières. « *Les PME semblent mal protégées, sachant que 120 banques au G-D de Luxembourg sont des PMEs. En tout, nous comptons 15000 PME/PMI à protéger* » (sic).

Cependant, les incidents de sécurité des uns concernent forcément les autres. En effet, désormais l'absence de frontière numérique est effective, et les incidents semblent certainement sous-estimés. « *Nous ne sommes pas sur une île et ce qui arrive aux uns peut arriver aux autres…* » (sic).

Relever ou fédérer les incidents, pour les distribuer vers tous ensuite, semble être une idée fédératrice ; mais cela devra demeurer anonyme, sur le même principe de l'enquête du CSI/FBI, par exemple. Des entités comme les Chambres de Commerce et des Métiers peuvent procéder à l'anonymisation (pour respect d'une règle d'indépendance). Des relais pourraient aussi être mis en place ainsi, par secteur, avec le schéma suivant : l'entreprise contacte son organisme de représentation qui peut contacter ensuite l'observatoire.

« *L'Observatoire doit demeurer neutre* » (sic). Le rapport est quasiment direct, moins il y aura d'intermédiaire, plus la confidentialité est ainsi assurée. Un grand niveau de confiance devra entourer l'observatoire et sa composition. C'est la seule façon de comprendre les phénomènes relevés rapidement. La collaboration avec les autres CERTs est ainsi requise. Selon les connexions primaires avec les ISP, les vecteurs d'attaques

varient et peuvent provenir en majorité du pays vers lequel les connexions sont principales. A noter, qu'en Belgique, une loi permet de fermer une adresse qui distribue des virus, par exemple ; « *Le G-D de Luxembourg disposant d'une connexion privilégiée ISP vers l'Allemagne, et ce dernier ne disposant pas de ce type de loi, notre pays ne peut alors que subir ce type de menace*» (sic). Un projet pourrait viser à sélectionner les points d'entrée au G-D de Luxembourg (au nombre de trois), et mettre en place des outils intelligents pour capter les attaques en entrée sur le territoire. Si le pays souhaite se positionner, en tant que centre de compétences bancaires, il semble judicieux d'asseoir une sérénité en terme de menaces connues et maîtrisées au niveau des TIC.

La manière de fédérer cette activité se pose : il s'agit d'une question de fond. Mais il semble important de redistribuer cette information des menaces, et ainsi de faire monter la maturité de certains face aux autres. L'enrichissement devient alors commun. Les incidents des uns pourront être facilement bloqués par les autres. « *Une bonne pratique pourrait être de mettre en œuvre une procédure pour permettre de déclarer facilement l'incident et de générer un rapport, puis conserver les traces* » (sic).

A l'unanimité, un observatoire des menaces semble une solution naturelle pour observer les menaces TIC. « *Il faut que cet observatoire soit connu et fasse du marketing, de la publicité* » (sic). Un site web d'information et d'accompagnement serait aussi une bonne pratique. Cependant, il ne faut pas focaliser sur les incidents uniquement techniques, car il y existe aussi des problèmes de sécurité de l'information plus généraux. Il faut « asseoir » les TIC et les conforter, ne pas les condamner, en assurer une image de qualité, afin d'en faire un « plus ». A ce titre, l'observatoire doit aussi atteindre le chef d'entreprise. Il doit pouvoir offrir des services de *reporting* et de diffusion vers ses cibles. Certaines listes spécialisées existent déjà mais le G-D de Luxembourg doit filtrer l'ensemble en fonction de ses besoins, de son contexte et de ses particularités. Une structure centrale de ce type permet ensuite de répartir l'information aux différentes cibles.

Tous les secteurs économiques semblent concernés au G-D de Luxembourg (banques, industries, hôtels…80 % du PIB) par le phénomène de cyberdélinquance. « *L'observatoire devrait travailler avec la Chambre de Commerce : 40 000 membres, 22000 PME. Il faudra tenir compte aussi des fédérations* » (sic).

Au Grand-Duché de Luxembourg, finalement beaucoup de sites sont attaqués, mais ne le savent pas. « *Depuis l'étranger notamment* » (sic). Les PME ou les petites banques sont plus sensibles, le domaine de la santé aussi. Le gros des problèmes ne semble pas communiqué, beaucoup d'attaques par rebonds sont recensées, ce qui est repris dans le *Symantec Threat Report*, montrant le G-D de Luxembourg comme principalement concerné, en tant qu'attaquant.

Souvent le but est d'attaquer quelqu'un de vulnérable, ainsi que d'autres *via* rebond ou encore *via* « *Botnet* ». Le grand public en est victime *via* « *phishing »*, mais cela ne concerne pas uniquement le G-D de Luxembourg. Le secteur bancaire demeure une cible de choix. De plus en plus de *botnet* essayent d'attaquer le Grand-Duché de Luxembourg. « *Sont investiguées actuellement de vraies attaques intentionnelles. Mais, dans la majorité des cas, les cibles s'effectuent au hasard* » (sic). « *Le Grand-Duché de Luxembourg est en tant qu'attaquant le 9*^{ème} *pays au monde, en fonction des rebonds. Ce chiffre peut apparaître discutable, mais le pays reste vulnérable ! Une structure pourrait veiller à rendre compte et à informer : « Vous êtes attaquant : vous êtes piraté ? », et gérer ainsi une « blacklist » à jour* » (sic).

Cependant, les menaces de cyberterrorisme pourraient être un peu exagérées pour le G-D de Luxembourg. « *Au-delà du jeu, le programmeur de virus, n'est pas un spécialiste, il n'a pas forcément d'intention de faire du dégât. Mais attention le hacking n'est pas un jeu, et demeure répréhensible par la loi. Généralement les attaquants ne sont pas des acteurs* » (sic). L'origine varie, des taxinomies existent mais un travail de fond est nécessaire. Les traces « *honeynet »* et « *phishing »* montrent que les attaquants travaillent en groupe. Il existe deux mondes entre les attaquants Windows et Unix (ces derniers sont plus « poussés » en terme de compétences). Beaucoup de traces sont en provenance des pays de l'Est, mais sans aucune certitude (possibilités de rebonds). De plus en plus de *botnets* tentent d'attaquer. Dans la majorité des cas, il s'agit de cibles prises au hasard, par exemple sur les résultats de moteurs de recherche de type « *google* ». Il existe aussi beaucoup de réseaux anonymisants : réseau « *thor* » (client à installer et autant de serveur : et crypté) *via* un nœud : on entre et on ressort avec l'adresse de ce nœud : impossible de savoir « qui est qui » sur le réseau mondial : client ou serveur « *thor* » ?

Statistiquement, 46 % des interviewés trouvent le personnage du pirate informatique dangereux, même s'il ne se rend pas compte de ce qu'il fait : « *peu importe les motivations, il représente un véritable danger pour l'économie nationale* » (sic). Certains le trouvent sympathique, pour d'autres, l'acteur peut prendre tous les aspects. Enfin, 38 % trouvent le personnage génial : « *Il y a du travail derrière – « c'est tordu » ! Ils sont passionnés. Persévérant. Ingénieux. Les hackers sont géniaux, s'ils veulent que cela fonctionne : il faut être novateur…pour réussir ! » (sic).*

La plupart des interviewés indique tout de même que les médias dirigent fortement l'image du pirate informatique et que ce dernier, une fois « catalogué », a du mal à se défaire de cette étiquette. Les médias ne remettent jamais en cause l'aspect génial et intelligent de ces acteurs.

77 % indiquent un degré de dangerosité important - voire très important quand les acteurs sont nombreux. Souvent, ils précisent que cela dépend du cas concerné et de ce qu'ils recherchent, mais aussi du personnage même, de son niveau. Certains parlent du « génie inconscient », en opposition au *« délinquant qui ne travaille pas seul, mais en lien avec la mafia* » (sic). Un seul trouve le degré de dangerosité moyen, tandis qu'un autre pose la question « *Un pirate : c'est quoi ?* ». Des réflexions, il ressort, que la bonne définition pour le terme « menace » est : « susceptible de porter préjudice », et que les médias recherchent le sensationnel ; mais l'essentiel reste inconnu.

61 % estiment que les médias guident cette représentation, certains ajoutent que cela est « *du cinéma, mais c'est ce que les gens retiennent* ». 30 % pensent que le pirate informatique lui-même fournit sa représentation, bien qu'il ne soit pas évident d'accéder à celle-ci, le monde étant considéré comme fermé, avec ses codes et ses clés de compréhension. 25 % de ces derniers pensent que les experts sécurité jouent aussi ce rôle de représentation du pirate informatique.

Pour 70 % : les pirates informatiques sont innovants : « *Car ces derniers font avancer les choses, notamment la sécurité des systèmes d'information* » (sic). Ils demeurent cependant délinquants. 30 % les estiment déviants, par définition, mais aussi souvent par inconscience.

25 % trouvent l'image du pirate informatique plutôt positive. « *S'il y a vol, destruction, cela permet d'améliorer le niveau de sécurité* » (sic). 65 % la trouve négative, surtout lorsque l'on a connu une expérience de piratage. 5 % la trouve neutre : « *ni blanc, ni noir* » (sic). De plus, 15 % pensent que l'image négative est celle qui est la plus dominante : « *C'est celui qui part en prison* ». Par contre, pour 70 % l'image est celle d'un acteur fort, de niveau supérieur.

A la question : « Un *hacker :* c'est un pirate qui vise à détruire ou voler des données disponibles sur un site victime ? », pour 60 % cela est faux (car il ne s'agit pas d'un criminel). Un seul ne sait pas, tandis que 30 % estiment que cette définition est la bonne.

A la question : « Un *cracker* : c'est un pirate qui recherche des failles de sécurité afin de progresser au niveau technologique ? », pour 60 % cela est faux, « *mais cette différence n'est pas connue par la moitié des informaticiens* » (sic).

Pour la moitié des interviewés, une communauté de pirates informatique existe certainement, des professionnels qui s'organisent vers une cible bien déterminée : le gouvernement ou autre… « *Il y a du monde derrière* » (sic). Pour l'autre moitié, cela est faux, ce sont plutôt des solitaires.

A la question : « Connaissez-vous cette classification des acteurs de la cyberdélinquance : « *Script kiddies* » : jeunes pirates informatiques de bas niveau ; « *Crackers* » : pirates qui attaquent un site pour destruction ou vol de données ; « *Hackers* » : pirates qui visent à découvrir des failles de sécurité pour en comprendre le fonctionnement (Cette classification vous semble t-elle : Juste ? Fausse ? Restrictive ? Pourquoi ?) ». « *Cette classification pose des problèmes, et apparaît quelque peu restricitve, car plus ils sont nombreux, moins la compréhension est possible, et de fait sous couvert de cette représentation, il est fort possible de ne pas prendre réellement conscience du danger* » (sic). Seul le *Hacker* pourrait jouir d'une véritable reconnaissance sociale. Pour 70 % cependant, cette classification est juste.

Enfin, la majorité des interrogés répond juste au questionnaire du CERT-CC des pertes estimées, relative à la cyberdélinquance : 666 millions $, ce chiffre ayant été largement relayé par les différents canaux de sensibilisation de la sécurité de l'information et de la communication au G-D de Luxembourg.

Cet état des significations montre que ces dernières peuvent être croisées et que de l'interaction peut naître le consensus. Aujourd'hui, le projet d'observatoire est en phase « pilote », et évolue tout en tenant compte des avis retenus et partagés lors de cette étude de faisabilité.

Note : le questionnaire et la démarche participative commune utilisée ont finalement servi d'instrument fédérateur pour les différents interlocuteurs impliqués.

Conclusion

Via notre étude nous pouvons conclure qu'il existe véritablement un ensemble d'images en provenance de différents mondes sociaux, vis-à-vis de l'objet de recherche que constitue le pirate informatique. Ces images, mêmes si elles ne se confrontent pas véritablement en tant que tel, et non perçues de la sorte la plupart du temps, montrent une incompatibilité « culturelle » de fait. La construction des significations étant intrinsèquement différente, car en provenance de contextes sociaux « culturellement » fortement différents. Ces mondes constituant le contexte social d'émergence de ces images (associé à la représentation sociale de la cyberdélinquance), nous pouvons conclure également qu'elles constituent les amorces de la représentation sociale du pirate informatique en terme de cadre structurant. Il n'existe pas actuellement de consensus général entre ces mondes ou encore de domination d'un monde sur les autres ; bien que les médias « tirent », pour l'instant, l'image sociale dominante du pirate informatique, par défaut, et profitent de canaux de diffusion extrêmement larges. Ce travail de thèse permet d'établir et de valider, la construction en cours de la représentation sociale du pirate informatique, via trois mondes sociaux déterminés (les médias, les experts de la sécurité de l'information, et les pirates informatiques) en inter relation avec la force structurante du jeu de la représentation sociale et du noyau central de la cyberdélinquance.

Un état, plusieurs acteurs, de multiples significations

Même si le phénomène de la cyberdélinquance apparaît socialement construit, *via* notamment un état quantitatif certain (cf. Partie I), l'objet social « pirate informatique » semble donc, pour sa part, demeurer en construction. En effet, les différences d'interprétation et de significations, détaillées *via* les différents mondes identifiés de la cyberdélinquance, formalisent spécifiquement cette vision du phénomène. Chacun apporte des caractéristiques sociales aux agents menaçants (des spécifications), permettant de déterminer une palette de choix des images sociales du pirate informatique. Cela est un résultat exploitable, notamment par le citoyen profane. Par exemple, la catégorisation, prônée par le monde des experts sécurité, permet surtout de bien comprendre les différents actes malveillants possibles pouvant atteindre tout utilisateur TIC. L'explication des motivations permet aussi de qualifier l'importance et la dangerosité de ces actes potentiels, mais surtout les différents « claviers » de la

délinquance sur lesquels peuvent jouer les pirates informatiques. Les différentes catégorisations proposées par le monde « *underground* » ne sont pas, pour leur part, réellement précises, et rarement reliées à des qualifications de délinquance, de toute manière en confrontation généralement avec les autres.

Il appert finalement que les différents mondes qualifient chacun ainsi une catégorisation de l'objet social plus ou moins précise, à tout le moins des significations spécifiques. Il en retourne la génération possible de la construction discursive de différents personnages pour le même objet social. Ces mondes attribuent en fait un registre de spécifications diverses (que l'on peut nommer des fonctions) à l'objet en question. Chaque monde étudié participe ainsi à cette construction selon des codes, cultures, besoins, histoires qui lui sont propres. Les images du pirate informatique créées sont alors délimitées selon les significations associées et le contexte dans lequel elles sont générées. En effet, chaque monde est caractérisé par un champ que nous définirons comme lieu où sont considérés des enjeux sociaux, c'est-à-dire un espace structuré de positions sociales. Les champs se caractérisent par des formes distinctes de capital engagé, c'est-à-dire des propriétés distinctives, les individus du champ donné (en l'occurrence, pour notre étude, autant de champs que de mondes de la cyberdélinquance identifiés) partageant un certain nombre de présuppositions constitutives du champ et ses règles du jeu, une fois à l'intérieur. « *Il s'ensuit qu'à chaque champ correspond un regard propre sur l'univers, créant les objets dignes d'attention (et donc aussi ceux qui ne le sont point) et les principes de compréhension et d'explication qui leur conviennent. Une même réalité fait par conséquent l'objet de représentations sociales diverses.* »[262]. Souvent, les significations émanant des différents champs sont antagonistes, irréductibles les unes aux autres. Ainsi, l'enjeu social de chaque monde de la cyberdélinquance est de maintenir ou d'augmenter la position de ses significations par rapports aux autres. La dynamique de chaque monde est ainsi marquée : « *[…] où des forces ne se manifestent que dans la relation avec certaines dispositions : c'est ainsi que les mêmes pratiques peuvent recevoir des sens et des valeurs opposées dans des champs différents, dans des*

[262] *La construction sociale du risque* (Nuffelen, 2004).

états différents ou des secteurs opposés du même champ »[263]. La théorie des champs semble spécifiquement s'appliquer à notre contexte social identifié par les mondes de la cyberdélinquance. Chaque image produite est également interdépendante à la fois des mondes dans laquelle elle s'inscrit (le contexte), mais aussi un produit de la représentation sociale de la cyberdélinquance (identifiée en première partie). Ainsi, les images sociales peuvent être reconnues comme des produits de la représentation sociale de la cyberdélinquance, qui eux-mêmes prennent naissance à travers les différents mondes qui développent, pour chacun, des significations consensuelles du pirate informatique. Cela engendre la construction de la représentation sociale du pirate informatique (en cours), et fait aussi évoluer « lentement », les valeurs affectées au noyau central de la représentation sociale de la cyberdélinquance. Le pirate informatique est donc véritablement un objet social en construction.

Au niveau sociétal, pour l'utilisateur TIC, il sera ainsi difficile d'objectiver une image du pirate informatique, y compris pour tout individu, car la construction sociale de l'objet sera dans un premier temps en fonction de l'habitus qui le prédispose, et qui, dans un second temps est orienté par le champ dans lequel il est pris (le choix souvent « obligatoire » d'un monde de la cyberdélinquance pour repère et généralement le plus pragmatique d'accès : les médias). La représentation sociale de la cyberdélinquance sera alors le point de repère fédérateur. A ce titre, le monde des médias peut-être considéré comme l'effecteur principal en amont des significations à disposition du citoyen, s'agissant du monde social le plus proche d'accès, et le plus diffusé. Cependant, idéalement, afin de qualifier plus finement les acteurs malveillants, il semblerait nécessaire de prendre en compte les différents mondes à l'origine de significations les concernant, tout en tentant de caractériser les frontières marquées, et les passerelles possibles entre ces mondes. L'usage de bonnes pratiques de partage de ces significations (tenant compte des rôles de chacun au sein des mondes de la cyberdélinquance dans la construction sociale), existe sous la forme de ponts de significations « ouverts » entre les mondes. Pour exemples de bonnes pratiques « inter significations » et « interculturelles »

[263] *La distinction. Critique sociale du jugement (Boudieu, 1979).*

: le salon Hack.lu[264]. Ce salon de *hack* réunit à la fois des experts sécurité, des *hackers*, des pirates informatiques, des institutionnels et des journalistes, traduisant une réelle lecture possible des significations entre les champs. Le comité de relecture, auquel nous avons participé (édition 2006), a permis d'atteindre des partages de significations, vis-à-vis du même objet, entre les différents mondes, par un partage de culture adaptée. Le rapport du CLUSIF[265], est un autre exemple présentant une communication médiatique qui est aussi « expertisée » par des spécialistes de la sécurité de l'information, *via* la production annuelle du « panorama cybercrime ».

A ce niveau de partage, la représentation du pirate informatique se construit alors *via* la corrélation des significations des mondes associés. La représentation sociale de la cyberdélinquance demeurant, l'unique point stable « producteur » des images sociales (et médiatiques tel que nous l'avons décrit précédemment), *via* son noyau central (cf. figure un *supra*).

La corrélation des significations pour principe de représentation

Dans la plupart des cas, l'image du pirate informatique que se fait l'utilisateur repose sur les significations sociales « les plus faciles d'accès », orientée par champs spécifiques, alors que nous venons de montrer qu'une démarche plus rigoureuse semblerait nécessaire dans le but de construire une représentation « juste » de l'objet, sa réalité sociale ou, à tout le moins, penser la construction en cours de l'objet. « *Une des propriétés des représentations sociales serait de privilégier la congruence psychologique par rapport à la cohérence logique et de faire passer l'efficience affectivo-cognitive avant l'efficace théorico-scientifique* »[266]. En effet, les images sociales de l'objet de recherche durant cette phase de construction non figée, ne répugnent pas à emprunter à l'irrationnel et à la « sagesse populaire », au risque de reposer sur la formalisation, en aval, de « préjugés », de « clichés », alors que nous avons montré que l'objet social est plutôt en perpétuelle construction et qu'il ne fait pas forcément l'objet d'émergence de

[264] http://www.hack.lu : « *The aim of the convention is to make a bridge of the various actors in the computer security world* » (Le but du meeting est de jeter un pont entre les différents acteurs dans le monde de la sécurité informatique).
[265] http://www.clusif.asso.fr.
[266] *Les représentations sociales* (Mannoni, 2001).

significations en provenance d'un seul monde social, mais de plusieurs. Cela peut être déjà le cas vis-à-vis des images médiatiques fortement présentes quant à la signification de l'objet de recherche. Une seule catégorisation retenue, ou la domination significative d'un seul champ ne peut sembler suffire. Une des solutions à ce problème reposerait sur la sensibilisation objective de l'utilisateur TIC en lui permettant de pouvoir tenir compte de la réalité et des mondes différents, des valeurs diverses mises en relation selon des contextes sociaux spécifiques, qui participent à la construction sociale de cet objet, de manière à pouvoir « balayer » les problèmes récurrents de définitions et de significations trop statiques, voire déterministes.

Suite à notre travail de recherche, nous proposons donc, en termes de prospective de connaissance quant à cet objet social, une démarche intégrée de réflexion. Cette démarche s'appuie, en amont de la représentation de l'objet social, sur la prise en compte de la dimension interculturelle de l'ensemble des mondes sociaux dans lesquels les images (significations) de l'objet prennent forme. Ainsi, s'approcher d'une représentation « objective » de l'objet social devient possible, en entrant notamment dans chaque monde de la cyberdélinquance et en se plaçant du point de vue de l'acteur de chacun, et en tenant compte du fait qu'ils proposent une construction singulière pour l'instant.

L'existence de plusieurs mondes contribue à faire coexister plusieurs images sociales et médiatiques qui font apparaître l'objet comme multiforme et d'appropriation complexe. Dans ce contexte, tant que l'objet est en construction (socialement), que des champs s'opposent sur les significations, que les ponts ne sont pas plus nombreux, alors le lissage de ces dernières semble impossible, du fait de la multiplicité des images disponibles. L'objet « pirate informatique » n'est en effet pas totalement partagé par les acteurs de ces mondes, contrairement, par exemple, à ceux des mondes de l'art : « *Les acteurs des mondes de l'art se divisent le travail. Chacun de ces derniers ayant une activité dans laquelle il est expert* »[267]. Dans notre cas, les mondes ne sont pas consensuels et concomitants, mais plutôt concurrentiels. De plus, généralement la communication médiatique emprunte des raccourcis pour faciliter la compréhension, faisant des choix dans ses propos, ce qui ne facilite pas la cognition véritable de la réalité

[267] *Les Mondes de l'art* (Becker, 1992).

sociale véritable de l'objet. De surcroît, la prégnance des médias dans la construction de la représentation sociale du pirate informatique est d'autant plus forte, que le récepteur de l'information n'appartient pas ou n'est pas en contact direct avec le monde social de l'objet. L'absence de communication entre ces mondes provoque indéniablement aussi une incapacité de rapprochement des significations. Ainsi, le poids des médias devient prédominant dans la construction de l'image sociale de l'objet, particulièrement pour ceux ne connaissant pas les différents mondes et étant donc incapables de s'en constituer une représentation réaliste. Cette constatation montre toute l'importance de tenir compte des significations provenant des différents mondes dans l'optique de la formalisation finale de l'image du pirate informatique, le risque demeurant sur la primauté accordée par défaut aux représentations médiatiques.

Reposant sur des modes culturels différents, les mondes sociaux de la cyberdélinquance construisent donc majoritairement des significations différentes, tout en étant en interdépendance de la représentation sociale de la cyberdélinquance. Les modèles des travaux de l'Ecole de Chicago, et notamment de ceux menés par H.S Becker, sociologue américain, au cœur des *Mondes de l'art*, se sont efforcés de montrer l'interactionnisme symbolique. Ainsi H.S. Becker présenta l'interdépendance et les relations entre les différents acteurs d'une chaîne de production avec une division du travail similaire à celle d'une entreprise automobile industrielle de Chicago, mais en démontrant que les liens entre les personnes sont implicites, qu'elles ne travaillent pas toutes dans un lieu clos, mais que leur but commun est d'arriver à diffuser une oeuvre d'art. L'interactionnisme symbolique au cœur de chaque monde de la cyberdélinquance est également identifié.

Cependant, entre et à travers les mondes de la cyberdélinquance, il semble, pour l'instant, difficile, d'application, chaque monde identifiant des valeurs, attributs et reconnaissance, en « cercle fermé », majoritairement à l'intérieur de son champ. Ainsi la chaîne de production de la réalité sociale du pirate informatique n'apparaît pas homogène, mais plutôt compartimentée. Nous parlerons donc, pour l'instant, des images sociales du pirate informatique et non d'une représentation sociale établie de cet objet. Nous parlerons d'un objet social en construction, composé de spécifications dynamiques

émanant de différents champs sociaux. Nous avons montré que le risque IT a pour élément déclencheur principal un type de menace bien caractéristique dénommé « cyberdélinquance ». Cette dernière présente un état statistiquement établi. Cependant, la représentation sociale de ses acteurs principaux (les pirates informatiques) demeurent fortement complexes à établir, elle est pour l'instant en définition. L'absence d'interaction entre ces mondes sociaux, forme aussi la base d'explication du fait. Même si chacun des mondes est conscient qu'il concoure à la construction de la représentation sociale du pirate informatique, ils ne partagent pas entre eux la construction finale d'un même objet, en effet, les fonctions et significations associées sont différentes. L'interactionnisme symbolique partagé dans les mondes sociaux de la cyberdélinquance est quasi inexistant entre les mondes expliquant un objet de recherche toujours en construction sociale.

Pour sa part, et en corrélation, l'utilisateur TIC ne perçoit généralement qu'une vue partielle de l'objet, car il n'a pas les moyens d'atteindre l'ensemble des significations des différents mondes de la cyberdélinquance identifiés. Le plus proche des mondes de l'utilisateur étant celui des médias, il en devient le plus influent et véhicule ainsi ses significations pour construction de la représentation sociale finale. Cette information singulière peut conduire à une mauvaise perception des menaces et des vulnérabilités associées. Une telle image partielle du risque numérique, souvent construite de facto sur des clichés et/ou préjugés, peut ainsi conduire soit à des mesures « hyper sécuritaires » de la part du citoyen (paranoïa, société du risque), soit au laxisme le plus total (pourquoi faire quelque chose alors que les pirates sont toujours « les plus forts » ?). Les messages incomplets des significations associées au pirate informatique doivent être adaptés par le marché de la sécurité de l'information.

L'utilisateur manque véritablement de perception de la réalité de l'objet de recherche. Il dispose le plus souvent d'une image singulière qui apparaît alors peu fiable, non partagée, non homogène, et non représentative de la réalité. Par le fait, il ne se raccroche pas à une représentation sociale établie de notre objet mais plutôt à des images alors fortement attachées à la représentation sociale de la cyberdélinquance. L'utilisateur devrait pouvoir atteindre l'ensemble des significations disponibles de différents mondes et fixer sa propre représentation à partir de la connaissance de l'ensemble. Il est à noter

que la définition officielle du pirate informatique en normalisation technique, par exemple, n'existe pas actuellement, un partage de significations consensuelles n'étant pas encore atteint (le principe même de la normalisation en termes de construction des normes), à ce titre. Seule une définition du terme « *hacker* » est normalisée au niveau international : *« (1) Passionné des ordinateur techniquement sophistiqués. (2) Passionné des ordinateurs techniquement sophistiqués utilisant ses connaissances et moyens pour accéder à des ressources protégées. »*[268]. En regard, les significations d'un seul monde ne peuvent permettre de formaliser l'image sociale du pirate informatique, car réductrices. Ainsi, il semble essentiel pour atteindre une caractérisation de l'objet « pirate informatique », d'user, par exemple, des bonnes pratiques représentatives suivantes ; d'une approche interculturelle :

- tenir compte de la construction sociale en cours de l'objet : il n'est pas construit (différent d'un état),
- tenir compte de la dimension cognitive interculturelle des différents mondes à l'origine de sa construction et de son image sociale,
- intégrer les différences, s'approprier les distinctions, (si possible),
- atteindre « la réalité » en croisant ces différentes significations.

Ainsi, en proposant ce modèle de réflexion, la représentation sociale de l'objet de recherche pour l'utilisateur des TIC pourrait paraître moins complexe, voire plus juste. Par le fait, l'individu pourrait alors participer, au cœur de la société de l'information, de la construction sociale du risque, en même temps qu'il participe à cette construction. « *Toute notre connaissance du monde, qu'elle s'exprime dans la pensée scientifique, comprend des constructions […] Cela ne signifie pas que, dans la vie quotidienne ou dans la science, nous soyons incapables de saisir la réalité du monde. Cela signifie simplement que nous n'en saisissons que certains aspects, notamment ceux qui sont*

[268] Seule la définition ISO de *Hacker* est disponible (correspondant à une partie seulement des significations possibles du pirate informatique) : « (1) *A technically sophisticated computer enthusiast (ISO/IEC 2382-1 :1993 Information technology — Vocabulary — Part 1 : Fundamental terms, 01.07.03). (2) a technically sophisticated computer enthusiast who uses his or her knowledge and means to gain unauthorized access to protected resources (ISO/IEC 2382-1 :1993 Information technology—Vocabulary—Part 1 : Fundamental terms, 01.07.03) »*. A ce titre, un nouveau projet va définir sous peu, *via* un Groupe de Travail ISO (ISO/IEC JTC1/SC7 WG22), la création d'une norme internationale sur le vocabulaire IT (*ISO 24765* « *Systems and software engineering — Vocabulary »*), avec certainement de nouvelles définitions en lien avec la représentation du champ de la cyberdélinquance.

pertinents pour nous, soit pour gérer notre propre vie, soit du point de vue du corpus de règles de procédures de pensée admises telles quelles appelé méthode scientifique »[269].

La cyberdélinquance qui pose finalement un enjeu de sécurité internationale, sur l'ensemble des réseaux informatiques, impose de mieux la comprendre, comme en témoigne l'appel à projet lancé par l'INHES en 2005[270], que nous avons eu la chance de réaliser en 2007. L'objectif de cette étude était d'aider à la prise de décision politico stratégique en confrontant les diverses significations de la cyberdélinquance qui circulent dans l'espace public, par une approche plutôt qualitative. Nous avons identifié les mêmes mondes que ceux de notre recherche participant, en effet, à la construction de l'image sociale du pirate informatique selon des codes, culture, besoins, histoire qui lui est propre. Ces acteurs sociaux sont généralement appelés à coopérer selon un certain nombre de procédures conventionnelles au sein de leurs réseaux. Cette étude traduit la même conclusion que notre travail de recherche. Ces trois mondes mobilisent de nombreux acteurs sociaux, coopérant ou non, utilisant ou non des procédures conventionnelles au sein de réseaux que l'on peut dénommer : mondes de la cyberdélinquance. Ces mondes engendrent des significations spécifiques formalisant, *sui generis*, une image singulière du pirate informatique. Chaque monde forge alors une catégorisation particulière de ces acteurs sociaux, dont rien n'indique a priori qu'ils soient obligés de se rencontrer.

Ainsi, la presse grand public a abandonné la vision idéalisée qu'elle pouvait avoir concernant les *hackers*, au profit d'une dénonciation sans ambiguïté des adeptes de la cyberdélinquance, assimilés explicitement à des escrocs, des voleurs, des mafieux. Que ce soit dans Libération : « *Moscou, la guerre aux cybermafieux* », (11 février 2006) ; « *Faites la nique aux arnaques en ligne. Cybercriminalité : bréviaire des modes opératoires des nouveaux escrocs* » (26 avril 2007), ou encore dans Le Figaro, « *Les nouvelles armes de la cybercriminalité* » (14 février 2007) où l'on parle *« des groupes très organisés qui sont à l'origine d'une véritable industrie de la cybercriminalité* ». Toutefois la vision héroïque n'a pas disparu, comme en témoigne l'article paru le 7 mars

[269] *Le Chercheur et le quotidien. Phénomènologie des sciences sociales* (Schutz, 1987).
[270] «*Vers la connaissance de la cybercriminalité – Etat de l'art* », (Vassileva, Mercier, Humbert, 2007) Rapport de Recherche INHES « *Espaces publics et sécurité – Thème : la cybercriminalité* » (131 pages)

2007 (« *Les pirates du Net à l'assaut des sites d'entreprises* ») qui évoquent les défenseurs de « la liberté de circuler sur la Toile », « *ces idéalistes qui se lancent des défis et multiplient ce qu'ils appellent des exploits* ». Même constat de balancement pour le journal Le Monde. Le 20 janvier 2007, suite à la présentation du « Panorama de la cyberdélinquance 2006 » par le Clusif, ce journal évoque le « *phishing* », en constatant qu'il « *n'épargne personne : Voyages-sncf.com (VSC), premier site de voyages en ligne français et premier site Internet marchand, filiale de la SNCF, vient d'en faire les frais, sans que beaucoup de clients en aient cependant à subir les conséquences* »... La question est donc traitée parce qu'elle devient concrète pour l'utilisateur qui observe un risque financier en l'espèce. La cyberdélinquance est donc devenue « une menace ». En revanche, pas de jugement de valeur de la sorte lors d'articles dans les journaux lorsque sur un site des *hackers* rendent publiques les failles de sécurité de sites de partis politiques : « *Zataz.com révèle des failles de sécurité dans deux sites Internet de l'UMP* » (Le Monde, 10 janvier 2007). Comme il l'indique sur son site, ce « *webzine* » offre une publicité à des pratiques de *hacking*, du moins celles qui visent apparemment à tester la sécurité des sites. Ainsi *« depuis 1996, ZATAZ Magazine propose le musée des sites francophones piratés. Un baromètre des actes des défaceurs. Si vous souhaitez nous indiquer un cas de piratage de site Internet, il vous suffit de rentrer le nom du pirate, son groupe et l'url du site modifié. Après contrôle de notre part, votre information apparaîtra dans le musée des défacements de ZATAZ Magazine* »[271].

Dans le tout récent article *« La cybercriminalité progresse en Suisse* », Nouvel Obs.com, (source : Associated Press) le 30 avril 2007, le début montre que le sujet est traité pour ce qu'il recèle désormais de possibilité d'identification des lecteurs avec les pratiques dénoncées. « *Espionnage économique, usurpation d'identité et vol de données sont en recrudescence en Suisse sur Internet. Les méthodes sont de plus en plus raffinées et les cybercriminels n'hésitent pas à recruter des personnes naïves pour en faire leurs complices* ». Autre exemple, issu du même hebdomadaire, « *Les États-Unis, berceau de la cybercriminalité* » (source : Associated Press) du 20 mars 2007, où le terme *hackers* devient en fait un terme qui désigne les cyberdélinquant en réseaux clandestins, rompant

[271] http://www.zataz.com

ainsi avec la distinctions *hackers*/*crackers*. « *L'organisation des hackers en réseaux internationaux permet par ailleurs de développer la concurrence entre ces organisations clandestines*... » La bataille sur la représentation du *hacking* comme une cybercriminalité tout aussi condamnable que les autres, au sens de la Loi sur la confiance dans l'économie numérique (LCEN) adoptée en avril 2004, semble donc être en voie d'être gagnée, du point de vue des acteurs de la répression. La LCEN rend punissable toute intrusion.

De cette recherche, il ressort aussi clairement que la démarche d'analyse concernant le point de vue des acteurs sociaux concernés, les pirates informatiques, en tenant compte des significations qu'ils attachent à leurs actions, s'est révélée bien plus compliquée que nous l'envisagions. S'il est possible de fournir, comme nous l'avons fait, quelques clés d'interprétation internes à cette communauté, force est de constater que cet univers reste volontairement opaque et qu'il semble durablement réfractaire à une enquête de type « sociologique » classique. Ces acteurs de la communauté *underground* ont réussi à imposer leurs significations d'un monde d'individus agissant, certes aux marges de la légalité mais à des fins qui ne sont pas si contestables que cela, et qui ne mériteraient en tout cas pas une assimilation avec la criminalité. Mais, la vision romantique du « bidouilleur » de génie, innocent et inconscient des torts causés, ne semble plus de mise dans les médias. La reconnaissance des dégâts considérables que ce type d'activité peut produire est acquise. Sans doute la généralisation de l'informatique personnelle à domicile, avec la montée en puissance des abonnements à Internet aide-t-elle à diffuser dans le grand public, et donc chez les journalistes, une prise de conscience, au moins partielle, de l'ampleur des gênes occasionnées, ne serait-ce que *via* les *spams* et les virus. Cela n'implique pas néanmoins, la diffusion d'une vision globalisante et stigmatisante de tous les *hackers* comme des criminels en puissance. Là aussi, l'esprit de tolérance que l'on retrouve dans les médias s'explique-t-il en partie par une identification possible du public à ces individus : qui n'a jamais piraté un logiciel, fait une copie illégale d'un fichier ? Qui ne peut s'identifier à une figure classique de la lutte des petits contre les gros, des défenseurs « acharnés » du logiciel libre par exemple. Nul doute également que le *hacking*, dans sa vision de test des procédures de sécurisation, soit perçue assez positivement et donc comprise, parce qu'elle bénéficie d'un environnement favorable, lié à la montée en puissance des idées et de quelques pratiques de cybercitoyenneté, de

démocratie participative liée à l'existence de forums, d'espaces de débat et de contrôle citoyen sur internet. La mouvance *hacker* peut donc parfaitement se rattacher à cet air du temps pour revendiquer une différentiation de la politique répressive contre les activités illicites sur internet. La distinction revendiquée entre *hackers* et *crackers* semble s'imposer dans le discours de presse et a donc de « bonne chance » de se voir reconnue dans l'opinion publique. Alors que la pédophilie facilitée par Internet ou que le cyberterrorisme ne peut que profiter d'un climat d'opinion hyper réactif à ces questions, le chemin à parcourir pour faire accepter une criminalisation de la violation des systèmes informatiques à des fins de test ou de performance peut sembler encore long.

De nouvelles pistes pour la répression de la criminalité informatique ?

Cela implique de réfléchir encore à la manière dont les autorités répressives devraient de nouveau aborder le problème. Finalement en tenant compte d'un objet social pirate informatique en prévision de construction, doivent-elles faire une pareille distinction, et prévoir, du même coup, une révision du système de pénalisation de ces activités, en envisageant par exemple l'introduction d'amendes et une gradation plus nette de l'échelle des activités illicites ? Les hésitations récentes du législateur concernant la protection des oeuvres musicales, mises en cause par le *peer-to-peer*, et la nature des sanctions à appliquer, donnent à voir toute la difficulté pour arriver aujourd'hui à faire passer un message très répressif sur ses pratiques.

Doivent-elles améliorer leurs stratégies de répression globale, en refusant toute distinction, jugée oiseuse, générée par certains acteurs eux-mêmes afin d'échapper aux poursuites ? Le prix à payer d'une telle approche n'est-il pas d'encourager plus encore ces activistes à se réfugier dans l' « *underground* » et user d'un fonctionnement collectif secret ? Les autorités, aussi paradoxal que cela puisse paraître au premier regard, ne peuvent-elles pas contribuer au contraire à structurer ce milieu, en France, sur le modèle de ce qui se pratique ailleurs, en tolérant des zones d'expression et de reconnaissance organisées ? Cet aspect développé au Grand-Duché de Luxembourg porte ses fruits par ce partage des connaissances, lors de l'organisation annuelle par exemple du salon

« *hack.lu* »[272], jetant des ponts de communication, et devenant désormais un rendez-vous attendu par les trois mondes de la cyberdélinquance analysés dans notre étude. Nous imaginons difficilement des criminels se vivant comme tels, organiser des assemblées annuelles, à vocation semi-publique, pour échanger sur leurs méthodes et leurs forfaits. Cela se passe pourtant mais dans plusieurs lieux identifiables. C'est une preuve de plus qu'une partie des membres de cet univers sont incapables de comprendre la pénalisation de leur activité. Face à une telle réalité deux attitudes sont possibles, l'une plus répressive, l'autre plus compréhensive. La démarche répressive consiste à amalgamer l'ensemble des activités illicites ayant l'informatique pour outil ou pour cible, sous un vocable commun : cybercriminalité, en espérant que la peur du gendarme, le rappel constant du caractère illégal des pratiques de piratage informatique, suffiront à dissuader de nombreux adeptes. Peu importe si un tel englobement suscite incompréhension profonde d'une partie des personnes concernées, force doit rester à la loi. Nous avons souvent entendu ce commentaire en rapport au cybercrime. En la matière justement, dans le domaine pénal nos interlocuteurs policiers estiment qu'on ne considère pas encore assez le cybercrime totalement comme du crime organisé. C'est donc une piste de réflexion à poursuivre. Mais cette difficulté de perception peut s'expliquer par le fait que justement le *hacker* est encore assimilé à un être individualiste et isolé. L'histoire des représentations sociales nous enseigne qu'il a toujours existé un décalage entre les pratiques sociales qui conduisent progressivement à construire et voir se diffuser une représentation dominante d'une pratique ou d'un groupe. Ce laps de temps peut alors contribuer à voir se mettre en place une représentation dominante qui soit en décalage avec des réalités les plus actuelles, puisqu'elles ont continué à évoluer alors même que les fondements de ces représentations sont enracinées dans un passé plus lointain. Cela semble le cas et ce que nous pensons comme la recherche actuelle entre l'état de cyberdélinquance en termes de représentation sociale bien établie avec pour noyau central l'illégalité (évoluant très lentement), tandis que les mondes de la cyberdélinquance eux continuent d'évoluer rapidement et confrontent leurs significations de l'objet « pirate informatique » avec à terme l'émergence d'une image dominante mais consensuelle. La confrontation est

[272] http://www.hack.lu

actuellement marquée par le rapport à la légitimité qui est tout de même différent du strict cadre de la légalité. Cependant, les deux axes entre représentation sociale et images sociales sont interdépendants et s'enrichissent l'un par rapport à l'autre. Quant à la variation de la représentation de la cyberdélinquance, C.Flament considère que sa transformation s'effectue à partir de la modification des schèmes périphériques, avec conservation du noyau central. Le caractère illégal de la cyberdélinquance semble bien établi pour longtemps. Cependant, il n'empêche pas dans ce cadre strict, la prise en compte d'échelle de graduation des peines en fonction des actes et de leur légitimité (possible) ou du comportement des acteurs responsables.

Vers une démarche plus compréhensive du cybercrime

Cela consisterait à prendre au sérieux la distinction revendiquée par les *hackers* eux-mêmes (avec toutes les ambiguïtés que recèle la délimitation d'une frontière entre activités illégales car illégitimes et illicites alors que servant le bien commun). C'est la démarche pragmatique adoptée par les autorités américaines, lors des *Black Hats* notamment, où la prise de parole publique pour décrire des activités informatiques illégales est tolérée, si cela permet d'améliorer du coup, la sécurité des systèmes. Plutôt que de mener une politique répressive, reposant sur une opposition frontale avec des activités très occultes par essence, il s'agit de laisser une marge d'expression « grisant » ces activités noires, en vue, pourquoi pas de les blanchir totalement, lorsque certains *hackers* sont recrutés par des services officiels pour devenir des professionnels attitrés de la sécurisation des systèmes informatiques. Il semble également que certains *hacktivistes* puissent être recrutés, dans une logique patriotique, pour mettre leurs talents au service de la fragilisation des réseaux électroniques de cibles hostiles ou pour se préparer à toute attaques potentielles. Lorsqu'on voit à quel point les réseaux criminels et terroristes savent d'ores et déjà exploiter les ressources Internet pour favoriser leurs activités et la coordination de leurs réseaux, il semble donc que le réservoir *hackers* peut se voir proposer un débouché utile pour réorienter ce qui peut être interprété comme un « pouvoir de nuisance » vers des fins plus constructives du point de vue de la sécurité publique ? Puisque la cybercriminalité apparaît de plus en plus éloignée de ses racines

historiques, récupérée et dépassée par les investissements criminels classiques et monétarisés, autour de l'extorsion de fonds aux entreprises et aux particuliers, on peut se demander s'il n'y a pas là matière à convaincre des « *hackers* » de mettre leurs « compétences » au profit de la défense d'un monde informatique pacifié et respectueux des droits de chacun, comme ils prétendent le faire lorsqu'ils affirment agir en « chevaliers blancs » d'un univers informatique plus sûr et respectueux des libertés individuelles. Entre des acteurs criminels qui agissent secrètement et ne revendiquent rien pour poursuivre leurs délits, et des « *hackers* » qui revendiquent un rôle social dans l'univers du web, des stratégies de réponses légales différenciées semblent accessibles, et peut-être souhaitables pour la sécurité publique. Bien sûr, nul ne peut ignorer le risque qu'une telle approche du problème contient, puisqu'elle peut contribuer à encourager le « vice », c'est-à-dire les pratiques illégales pour se faire repérer et reconnaître, mais c'est un risque que les agences fédérales américaines ont, semble t-il, assumé pleinement. De la même manière, il ne nous appartient pas de juger de l'attitude à adopter par les autorités officielles face aux cybercriminels en général. Nous nous sommes contentés aussi d'adopter une logique compréhensive face à notre objet de recherche, pour permettre de mieux apprécier les postures à adopter pour les comprendre. Notre travail de recherche établit que nous ne pouvons pas encore parler de représentation sociale du pirate informatique mais d'images sociales. Pour une gestion utilitaire du cybercrime, il semble pertinent de favoriser le champ du *hacking* réseau, *via* une aide contrôlée, et combattre alors farouchement le véritable cybercrime : alchimie nécessaire permettant de favoriser l'innovation dans ce domaine. Cela en faisant évoluer sainement le cadre régulatoire et punir les véritables « hors la loi ». Et, corrélativement, pour « remettre de l'ordre », ne faudrait-il pas redorer le blason des *hackers* ?

Le 14 octobre 2005, lors de la conférence « *hack.lu* » au Grand-Duché de Luxembourg, M. le ministre de l'Economie et du Commerce extérieur, Jeannot Krecké, déclarait, en ouverture, que les *hackers* doivent être considérés « *non comme des ennemis, mais comme des experts* ». C'est ainsi que le ministre a demandé aux participants : « *Si un jour vous arrivez à pirater le système de mon ministère et que vous trouvez les failles, dites-le moi s'il vous plaît !* ». Enfin, M. le Ministre a aussi mis en relation l'activité des *hackers* avec la stratégie de Lisbonne (Union Européenne) :

« *Qu'est-ce qu'une économie de la connaissance sinon l'excellence technologique, l'apprentissage tout au long de la vie (sans quoi, vous seriez rapidement dépassés) et l'esprit d'innovation dont vous faites preuve ?* ». Enfin, dans ce même ordre d'esprit, nous pouvons citer G. Conti qui spécifie : « *Si les membres d'un groupe sont traités comme des ennemis, il se comporteront ainsi, mais s'ils sont traités comme des pairs et des experts qui ont quelque chose à apporter, ils relèveront le challenge »*[273].

Pour aller plus en avant dans ces réflexions, nous proposons de retenir une prospective de connaissance « kaléidoscopique » du pirate informatique.

Vers la prospective de la connaissance du pirate informatique

Nous proposons des pistes en termes d'instruments facilitant la démarche de la construction globale du pirate informatique en terme d'objet social, et la compréhension de la pensée sociale en regard. La notion de ponts entre les différents mondes nous semble un critère important en terme d'évolution permettant d'atteindre pour un objet en construction la représentation sociale « homogène ». Des ponts nous ont semblé identifiables entre ces mondes de la cyberdélinquance (à l'origine des images sociales et médiatiques du pirate informatique) pour parachever la construction de l'objet sociale et aboutir vers une image sociale singulière : il nous semble important de tenir compte des ponts entre les mondes pour construire la prospective. L'intégration de l'ensemble des significations disponibles vis-à-vis du piratage informatique paraît nécessaire, ainsi que le travail de veille au cœur de chaque monde. Identifier ces passerelles culturelles devient nécessaire au développement des connaissances et de l'innovation *via* les ponts entre les mondes aux fins de construction d'une image unifiée permettant une meilleure connaissance. Cela permettra une aide certaine pour la sécurisation du monde numérique, en offrant des pistes d'améliorations de sensibilisation, et afin aussi qu'il ne reste des efforts de sécurisation adaptée qu'aux véritables criminels. Il en va aussi de la future

[273] « *If a group is treated as the enemy, they will behave like one, but if they are treated as peers and experts who have something to contribute they will rise to the challenge* ».
Why computer scientists should attend hacker conferences? (Conti, 2005).

représentation sociale du pirate informatique la plus « juste » possible, tenant compte de son interculturalité en amont, représentant « *l'ensemble des processus – psychiques, relationnels, groupaux, institutionnels, etc. – générés par les interactions de culture, dans un rapport d'échanges réciproques et dans une perspective de sauvegarde d'une relative identité culturelle entre les partenaires en relation* »[274].

Une gestion privée recommandée

Les résultats de notre étude portent un véritable besoin de sensibilisation vers l'entreprise qui doit être informée de ces menaces, mais surtout des différentes possibilités de menaces réelles réalisables à leur encontre. Cela devrait se faire en tenant compte de l'appréhension de l'ensemble des mondes de la cyberdélinquance, afin de ne pas tronquer la réalité. La gestion des menaces prend alors son importance, et nous proposons un outil pour ce faire : le questionnaire du sondage (seconde version) qui peut être alors utilement déployé en plan de sensibilisation dans l'entreprise, en lien avec la politique de sécurité de l'information de l'entreprise. Le but est de faire participer au fur et à mesure les employés, les utilisateurs, de manière interactive, en apportant la vue de chacun, de chaque monde, et surtout une aide non négligeable pour le RSSI qui va s'appuyer sur cette sensibilisation pour apporter une bonne vue des menaces, rapporter les lacunes de compréhension du phénomène, expliquer les différences culturelles et les rapprochements possibles, améliorer les comportements et surtout sensibiliser en adéquation avec la politique de sécurité en place, aux fins pour les sensibilisés de respecter les objectifs de SSIC dégagés et entérinés par la Direction de l'organisation concernée.

Une sensibilisation constructive : prise en compte de l'intégration des contextes

Il n'y a pas besoin d'études coûteuses pour prévoir que les attaques vont encore augmenter prochainement. L'évolution en matière de virus et de *spams* ouvre ici la voie

[274] *L'interculturel. Introduction aux approches interculturelles en Education et en Sciences Humaines* (Clanet, 1990)

de manière exemplaire. Certes, des solutions techniques en raison de leur développement continuel sont déjà aujourd'hui en mesure de filtrer d'avance plus de 90 % de tous les dangers. Si les salariés se comportent toutefois de manière négligente avec le courrier électronique, les anti-virus et les pare-feu n'aideront pas. C'est pourquoi il convient pour les entreprises de donner à leurs salariés des règles claires de comportement et ne pas laisser au hasard la prévention des menaces actuelles. Pour minimiser le préjudice d'un possible emploi abusif des propres sites Web, les entreprises qui travaillent dans le commerce électronique devraient garantir que tous les clients soient conscients du potentiel de danger des attaques de type « *phishing* » et prendre des directives correspondantes, à savoir quels sont les types d'informations demandés. Cela concerne tout citoyen. Pour chaque individu, la mesure de protection la plus importante réside finalement dans le fait qu'il faut être constamment vigilant lorsque des *e-mails* non sollicités sont transmises dans la boîte de réception. Des pièces jointes dans les messages non sollicités ne devraient généralement pas être ouvertes, car elles sont très souvent infectées par des virus et des programmes préjudiciables. On reconnaît souvent les *mails* « *phishing* » à des fautes de langue et des erreurs de format. Bien que les dernières évolutions (encore récemment au Grand-Duché de Luxembourg, en juillet 2007[275]) soient difficilement détectables, car techniquement et socialement perfectionnées, de qualité supérieure. La plupart contiennent en outre une adresse *web* et les objets se rapportent d'une certaine manière au compte personnel.

Outre ces mesures « éducatives » pleines de bon sens, il existe des technologies qui reconnaissent les activités douteuses et les contrecarrent sans cesse. La mesure la plus efficace demeure la surveillance proactive du trafic de tous les e-mails à filtrer afin de relever l'origine douteuse d'un mail, des failles de sécurité possibles et des codes de programme malveillants. De cette manière, les entreprises peuvent protéger efficacement les menaces en perpétuel changement devenues un fléau mondial. Le « *pharming* » ne peut aussi être contenu qu'avec des systèmes de sécurité proactifs, les modifications de l'adresse IP peuvent être reconnues et ainsi empêchées. Il est donc recommandé de se servir d'une solution de sécurité avec des systèmes réactifs et proactifs. Les systèmes

[275] http://www.cases.public.lu/alertes/2007/07/26_phishing/index.html

d’exploitation et les applications doivent de plus être régulièrement pourvus de mises à jours actuelles et de « *patches* » pour que les points faibles ne puissent pas être exploités.

Aspects pratiques de sensibilisation

La connaissance via l’observation demeure la seule chance de ne pas rater le train de mise en place de la confiance numérique. Pour exemple de bonnes pratiques fédérées de sensibilisation SSIC : du 1er au 6 février 2007, CASES (le Portail de la sécurité de l'information du ministère de l'Économie et du Commerce extérieur), http://www.petitweb.lu et Luxembourg *Safer Internet* ont organisé une exposition consacrée aux dangers d'Internet à la *Belle Étoile* (route d'Arlon à Bertrange). Dans le cadre du *Safer Internet Day* 2007 et des nombreuses actions menées à cette occasion, cet événement a pour but d'informer le public en faisant la lumière sur certains dangers liés à l'utilisation d'Internet, des TIC et sur les moyens de s'en protéger. Le développement croissant de ces technologies implique l'émergence de certains comportements à risques, faute de connaissances suffisantes en la matière. A ce titre, il est devenu essentiel de sensibiliser les usagers aux dangers inhérents à Internet et de leur prodiguer des conseils afin qu'ils puissent surfer en toute sécurité, tout en se protégeant des nombreux risques véhiculés par l'utilisation de cet outil. Divers documents didactiques rédigés en français et en allemand ont été proposés, et il a été possible d'assister à des démonstrations variées, telles que le « *cracking* » (forcer des dispositifs de sécurité) sur téléphone mobile et console de jeu, la configuration adéquate des routeurs *wireless* vendus au Grand-Duché de Luxembourg, etc…

Parallèlement à ces présentations, les jeunes internautes ont eu l'occasion de tester leurs connaissances en participant à un questionnaire grâce auquel ils ont eu la possibilité de prouver leur savoir en matière de sécurité informatique. Au terme de cet exercice sympathique et ludique, ils ont aussi pu (selon le nombre de points obtenus) décrocher leur permis « Web ». Une sensibilisation qui tient compte des images produites par les différents mondes…et qui les gère au quotidien. A ce titre, un concours a été mis en place avec ce libellé pour les enfants « *S’il-te-plaît … Dessine-moi un pirate informatique…* »

(En lien avec les principes de la conférence que nous avions tenu en septembre 2006 sur ce propos[276]).

La suite du travail de recherche entrepris

Afin de poursuivre les évolutions de la construction de la représentation sociale du pirate informatique, nous proposons la possibilité de mettre en place un travail de type « post-doctorat », ou de mise en œuvre d'un laboratoire social d'étude des cyberdélinquants, prenant en compte ces travaux, fortement utiles pour parfaire la recherche de la réalité de l'objet de recherche, de sa construction et de sa réalité sociales :

- Rencontre au cœur de l'Union européenne des individus effectivement condamnés pour faits de cyberdélinquance.
- Rencontre des mêmes individus pour les Etats-Unis.
- Rencontre des mêmes individus pour pays de l'Est.
- Inter-comparaisons des profils étudiés (lien avec la criminologie).
- Retour vers le champ de la sensibilisation.
- Retour vers le marché.
- Retour vers le monde de la sécurité de l'information.
- Retour vers les médias.
- Retour vers les services de police au niveau international.
- Adaptation corrélative des mesures anti-cybercrime.

La tentation de l'objectivité demeure, mais est-elle seulement possible puisque l'objet est en construction socialement ? L'objectivation d'un processus peut être dangereux et finalement un « trompe-l'œil », ne tenant pas compte des évolutions des significations des acteurs sociaux en amont.

[276] http://www.spiral.lu. Conférence, Luxembourg, Centre de Recherche Public Henri Tudor – Conférence dans le cadre du réseau des professionnels de l'IT (Information Technology) SPIRAL, du Grand-Duché de Luxembourg.

L'anthropologue Philippe Bourgeois, en étudiant de près le fonctionnement d'un gang de dealers de drogue, s'est placé dans une perspective « déterministe » pour affirmer que c'est le contexte socioculturel qui crée en partie les *gangs*. Mais il suppose également qu'à la base de cette économie parallèle se trouve un raisonnement rationnel : certains habitants inventent des « stratégies alternatives » de production de revenus. Le criminologue canadien Maurice Cusson est allé plus loin, en invoquant la notion de « rationalité » chez l'acteur – ce qui veut dire que pour comprendre l'action d'un individu, il faut prendre au sérieux les raisons que celui-ci invoque pour justifier de son acte. Ce dernier propose que la délinquance est un choix de vie, car le délinquant adopte un raisonnement selon lequel violer la loi lui apporte plus d'avantages que d'inconvénients.

Nouveau champ d'investigation des sciences de l'information et de la communication

Il s'agit d'une pierre angulaire à destination du travail de définition d'un nouveau champ important pour les sciences de l'information et de la communication, à savoir la sécurité des systèmes d'information et de communication, sans l'étude duquel, le développement des TIC n'est pas correctement envisageable, car potentiellement entravé. Damien Bruté de réaumur (Directeur du Département Sécurité de l'Information – Université de Montpellier I – Groupe Sup de Co. Montpellier) propose[277] la définition d'un champ de recherche original qui ouvre la voie à des travaux pluridisciplinaires. La sécurité de l'information émerge comme une problématique majeure dont le traitement ne peut relever des disciplines particulières nombreuses qui sont concernées mais d'une approche globale. Le concept de « champ sécant » permet de lever les ambiguïtés de la pluridisciplinarité en privilégiant une optique transversale. Ce dernier estime qu'un des domaines majeurs de la sécurité de l'information est la protection contre la cybercriminalité. Notre propos s'inscrit dans ce cadre en retenant, pour les sciences de l'information et de la communication, l'intérêt de la recherche pour la compréhension de

[277] *Un nouveau champ de recherche : La Sécurité de l'Information – Une illustration du concept de « champ sécant »* (Rémur, 2002).

l'objet « pirate informatique », *via* les interactions, médiations et significations associées pour cadre de construction.

Finalement, ce sont les images médiatiques qui jouent, en absence de contexte de l'objet à représenter ou par force du médium, le rôle d'image sociale forte et perçue majoritairement. Cette superposition peut masquer et/ou orienter finalement la perception de la construction de la représentation du pirate informatique. Dans son propos, Hélène Jeannin[278] semble conclure trop rapidement avec « *Car un élément semble définitivement acquis : le caractère irréversible de la nouvelle image du pirate* » (note : en déclin : négative et menace publique caractérisée). En effet, nous ne pouvons partager cet avis, car l'image du pirate informatique, même « déstructurée » de manière négative, continue à se construire à travers différents groupes et n'est donc pas figée, il s'agit d'un processus constant et non d'un état. Il semble plutôt que la représentation sociale de la cyberdélinquance quant à elle seule soit véritablement acquise. De fait, nous pouvons aussi considérer ces images en construction comme des « embryons » du noyau central futur de la représentation sociale du pirate informatique, il s'agit bien là de la même définition emprunté à Abric (1987, p68) et correspondant au passage du « modèle figuratif » à celle du noyau central correspondant à une volonté de « *passer du processus au produit* » (à l'état, à l'objet constitué), finalement à un « cadre cognitif stable ».

Vérifier l'état de la menace véritable est plus que jamais nécessaire, notamment pour ne pas se tromper. L'homme vit dans un monde de récits et la meilleure façon de comprendre la réalité (*via* les représentations) est de croire à la fiction. Les mythes (*hackers*, génies…) rentrent en scène et fascinent, il est bon d'y croire pour comprendre, mais impossible une fois fasciné de se raccrocher à un point de réalité comme au cinéma, car il n'y a pas de point de contact véritable, ni de véritable « cadre cognitif stable » établi, pour l'instant, en la matière, mis à part celui de la cyberdélinquance.

Pour notre objet, l'approche communicationnelle ne semble pas suffire, se résumant souvent à une approche strictement médiatique, seul le point d'accroche pourra

[278] *Du pirate informatique au cybercriminel : Grandeur et décadence d'une figure de héros contemporain* (Jeannin, 2004).

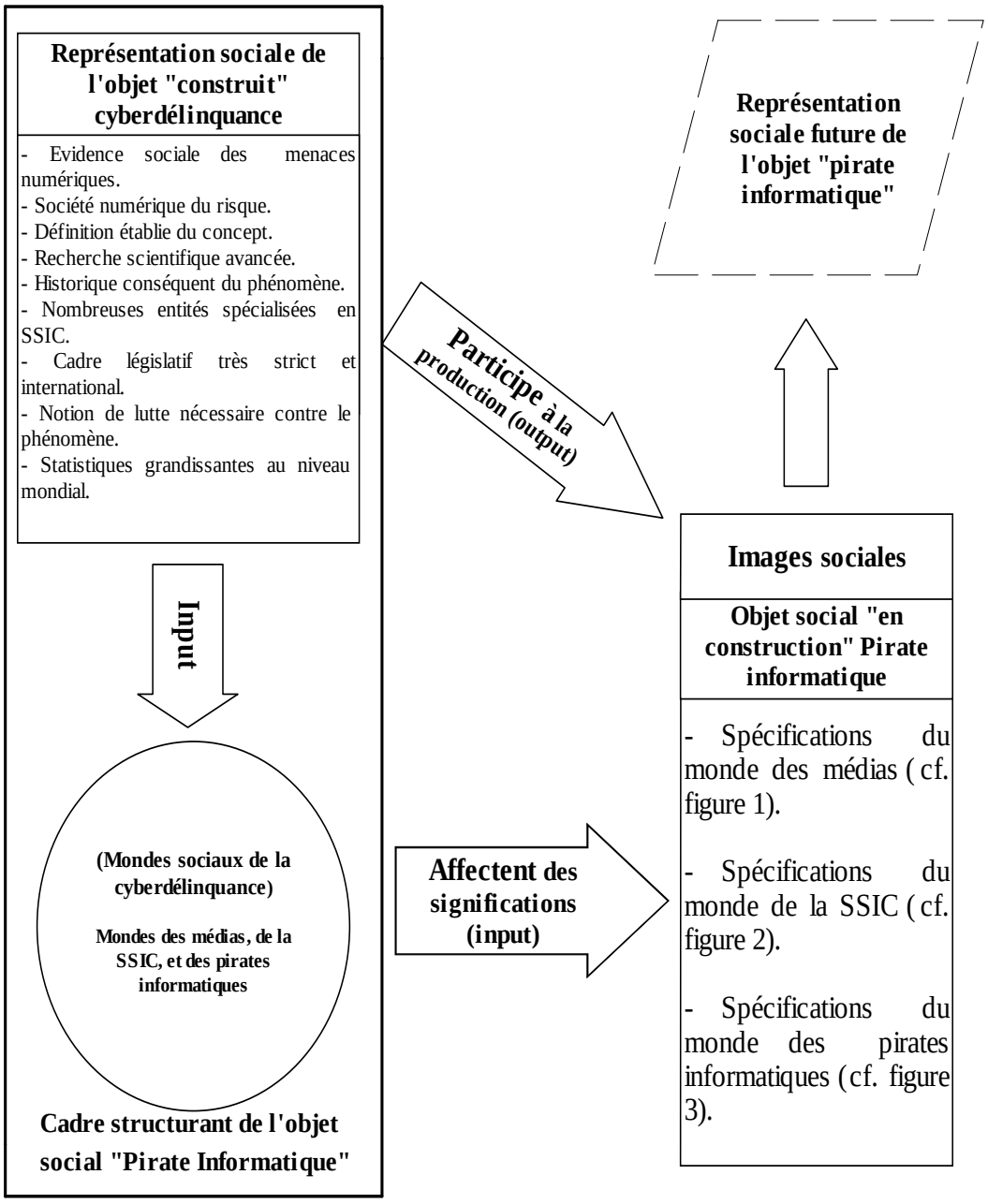
se faire avec la prise de conscience d'une approche multiculturelle via les mondes sociaux de la cyberdélinquance participant à la construction sociale de l'objet étudié. Nous espérons avec notre travail faciliter le passage d'un engagement personnel, vis-à-vis de l'objet de recherche, vers un engagement sociétal, en proposant des pistes concrètes méthodologiques pour y arriver, en tenant compte de la construction sociale à travers toutes les réalités des significations entourant l'objet de recherche traité. Cette construction, via les mondes de la cyberdélinquance, a un rapport au temps, qui peut se formaliser ainsi en termes de « temps qui transforme », tandis que la représentation sociale de la cyberdélinquance appartient « au temps qui dure », et enfin les images médiatiques « au temps qui passe ». Ainsi, certaines images actuellement fortement noircies, pourraient, à terme, blanchir, notamment en cas de besoin, par exemple de lutte contre le cyber-terrorisme… « […] *Il y a un fil conducteur – une passion pour la technologie et un intérêt intense pour comprendre le fonctionnement des choses. Vous feriez bien d'y aller ; ensemble les communautés ont plus à apprendre par rapport à une autre seule* »[279].

[279] « *But there is a common thread – a passion for technology and an intense interest in how things work. You would do well to attend; both communities have much to learn from one another* ».

Why computer scientists should attend hacker conferences? (Conti, 2005).

http://www.hack.lu : « *The aim of the convention is to make a bridge of the various actors in the computer security world* » (Le but du meeting est de jeter un pont entre les différents acteurs dans le monde de la sécurité informatique)…

- Figure 22. Modélisation graphique de l'objet de recherche « pirate informatique » en construction *via* les mondes de la cyberdélinquance



Bibliographie

A

- Abric J-C., 1987, *Coopération, Compétition et représentations sociales,* Cousset, DelVal.
- Abric J-C., 2003, *Méthodes d'études des représentations sociales*, Paris, Erès.
- Aeilts T., 2005, *Defending Against Cybercrime and Terrorism, a new role for Universities*, High Tech Crime Brief, Concept and Terms, Australian High Tech Crime Centre.
- Anonyme, 2001, *Sécurité Optimale*, Paris, Campus Press.
- Auge M., 1994, *Le chercheur et le quotidien. Phénomènologie des sciences sociales*, Paris.

B

- Beck U., 1986, *La société du risque*, Alto Aubier.
- Becker H. S., 2002, *Les ficelles du métier*, Paris, Guide Repères.
- Becker H. S., 1992, *Les Mondes de l'art*, Paris, Flammarion.
- Beveren J-V., 2001, A *conceptual model of hacker development and motivations*, Publication, University of Ballarat, Australia.
- Blanchard P., 1995, *Pirates de l'Informatique*, Paris, Addison Wesley.
- Bonardi, Roussiau, 1999, *Les représentations sociales*, Paris, Harmattan.
- Bosworth S., Kabay M.E., 2002, *Computer Security Handbook*, New York, Wiley.
- Bourdieu P., 1979, *La distinction. Critique sociale du jugement*, Paris, Les Editions de Minuit.
- Bouzon A., 2002, « *Ulrich Beck, La Société du Risque* », in Question de Communication (N°2).
- Bouyssou J., 1997, *Théorie Générale du risque*, Paris, Editions Economica.
- Breton P., Bertrand I., Heilmann E., 1991, *Entre l'ordre et le désordre des valeurs paradoxales du monde de l'informatique*, in Réseaux n°48/1991, pp. 19-21.
- Breton P., 2001, *Le Culte de l'Internet – Une menace pour le lien social*, Paris, La Découverte.

- Breton T., 2005, *Chantier sur la lutte contre la cybercriminalité*.
- Broadhurst R., Chantler N., 2006, *Cybercrime Update: Trends and Developments*, Queensland University of Technology, Brisbane, Australia.
- Budi A., Besnard D., 2004, *Technical and Human Issues in Computer-Based Systems Security*, University of Newcastle.
- Byers S., Rubin A., Kormann D., 2002, *Defending Against an Internet-based Attack on the Physical World*, WPES'2002, Washington, DC, USA.

C

- Capul J.Y., 2000, *L'Internet*, Paris, *Cahiers français, Documentation Française*.
- Carbonnier J., 1994, *Sociologie juridique*, Paris, Quadrige/PUF.
- Carnegie Mellon - Software Engineering Institute, 2001, OCTAVE v2.0.
- Carter D. L., 1992, *Computer Crime Categories : How Techno-Criminals Operate,* FBI Law Enforcement Bulletin.
- Castells M., 2002, *La Galaxie Internet*, Paris, Fayard.
- Chantler N. A., 1995, *The profile of computer hacker*, Thèse, Curtin University of Technology.
- Chatelain Y., Roche L., 2003, *Hackers ! : Le 5ème pouvoir – Qui sont les pirates de l'Internet,* Paris, Maxima.
- Chawki M., 2006, *Essai sur la notion de cybercriminalité*, IEHEI (Institut Européen des Hautes Etudes Internationales).
- Clanet C., 1990, *L'interculturel. Introduction aux approches interculturelles en Education et Sciences Humaines*, Toulouse, Presses universitaires du Mirail.
- Cohen F. B., 1995, *Protection and Security on the Information Superhighway*, Wiley.
- Coulon A., 2002, *L'Ecole de Chicago*, Presses Universitaires de France, Paris.
- Cybenko G., Giani A., Thompson P., 2003, *Cognitive Hacking : a Battle for the Mind*, Institute for Security Technology Studies and Thayer School of Engineering Darthmouth College, Hanover NH 03755.

D

- Denzin N., 1978, *The research act.*, Chicago, Aldine.
- Denzin N., Lincoln Y., 1998, *Emerging the field of qualitative research*. Em N. Denzin & Y. Lincoln (Orgs.), *Strategies of qualitative inquiry* (pp. 1-34), Londres, Sage.
- Délégation Interministérielle pour la Sécurité des Systèmes d'Information, 1994, *La menace et les attaques informatiques.*
- Direction Centrale de la Sécurité des Systèmes d'Information (France), 2004, *EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité.*
- Donald L. P., 2000, *Sécurité des Systèmes d'Information*, Campus Press.
- Duclos D., 2002, « *Le grand théâtre des experts du risque* », in Le Monde Diplomatique.
- Dufresne D., Latrive F., 2000, *Pirates et Flics du Net*, Paris, Seuil.
- Durkheim E., 1897, *Le suicide*, Paris, Quadrige Broché, 2002.
- Durkheim E., 1898, *Revue de métaphysique et de morale*, Paris.

E

- ENISA, 2006, *A step by step approach on how to set up a CSIRT* (Deliverable WP2006/5.1 (CERT – D1/D2).

F

- Flament C., 1984, *From the bias of structural balance to the representation of the group*. EM R. Farr, S. Moscovici (Orgs.), *Social representations* (269-285), Cambridge, Cambridge University Press.

G

- Guinier D., 2002, *Les systèmes d'information – Arts et pratiques*, Editions d'Organisation.
- Guisnel J., 1995, *Guerres dans le Cyberespace*, Paris, La Découverte.

H

- Himanem P., 2001, *L'Ethique Hacker et l'Esprit de l'ère de l'information*, Paris, Exils.
- Hoar S., 2005, *Trends in Cybercrime, the dark side of the Internet, Criminal Justice*, Volume 20, Number 3.
- Humbert J.Ph., 2003, *La cyberdélinquance, un risque pour Internet ? - Etude d'un corpus d'articles de la presse écrite française depuis l'émergence d'Internet (1995) à nos jours*, Mémoire de DEA en sciences de l'information et de la communication, Université Paul Verlaine – Metz.

J

- Jeannin H., 2004, *Du pirate informatique au cybercriminel : Grandeur et décadence d'une figure de héros contemporain*, Université de Paris III – Sorbonne Nouvelle.

K

- Kshetri N., 2006, *The simple economics of cybercrimes*, Etats-Unis.

L

- Lasbordes P., 2005, *La sécurité des systèmes d'information – Un enjeu majeur pour la France*.
- Le Breton D., 2004, *L'interactionnisme symbolique*, Presses Universitaires de France, Paris.
- Le Doran S., Rosé P., 1998, *Cyber MAFIAS*, Paris, Denoël.
- Levy S., 1984, *Hackers : Heroes of the Computer Revolution*, New York, Delta
- *Lignes directrices de l'OCDE régisant la sécurité des systèmes d'information* (O.C.D.E, 2002 : 7).
- Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique.
- Loi n°201-1062 du 15 novembre 2001 relative à la sécurité quotidienne.
- Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure.
- Loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.
- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
- Loi n°2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle.
- Longeon R., Archimbaud J-L., 1999, *Guide de la Sécurité des systèmes d'information*, Paris, CNRS.
- Lu C., Jen W., Chang W., Chou S., 2006, *Cybercrime & Cybercriminals : An overview of the Taiwan Experience*, Journal of Computers, Vol 1, Academy Publisher.

M

- Mannoni P., 2001, *Les représentations sociales*, Presses Universitaires de France, Paris.
- Martin D., 2001, *La menace de la cybercriminalité*, Rapport moral sur l'argent dans le monde, repris dans Problèmes économiques, n°2706, p19-22.
- Mitnick K., 2005, *L'art de l'Intrusion*, Paris, CampusPress.

- Monjardet D., Ocqueteau F., 2004, *La police : une réalité plurielle*, Paris, La Documentation française.
- Moscovici S., 1961, *La psychanalyse, son image et son public*, Paris, PUF.
- Mounier P., 2002, *Les maîtres du réseau*, Paris, La Découverte.
- Mucchielli L., 2001, *Violence et insécurité, fantasmes et réalités dans le débat français*, La découverte.

N

- National Institute For Standards And Technology (NIST), 2002, *Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30*.
- Newman R., 2006, *Cybercrime, Identity Theft, and fraud : Practicing Safe Internet – Network Security Threats and Vulnerabilities*, Georgia Southern University, Department of Information Systems.
- Nietzche F., 1950, *Le gai savoir*, Paris, Gallimard (aph. 112, p 159).
- Nisbet C., 2002, *Cybercrime and Cyber Terrorism*.
- Nuffelen D., 2004, *La construction sociale du risque*, Agence Fédérale de Contrôle nucléaire – Belgique, Scientific Bulletin.

O

- Organisation de Coopération et de Développement Economiques, 2002, *Lignes directrices de l'O.C.D.E. régissant la sécurité des systèmes et réseaux d'information*, Paris, O.C.D.E. Publications.

P

- Pansier F.J., Jez E., 1999, *La Criminalité sur l'Internet*, Paris, Presses Universitaires de France.

- Peretti Watel P., 2001, *La Société du risque*, Paris, La Découverte.
- Pipkin D., 2000, *Sécurité des systèmes d'information*, Paris, Campus Press.

R

- Raymond R., 2001, *The Cathedral and the Bazaar*, Broché.
- Rogers M. K., 2001, *A social learning theory and moral disengagement analysis of criminal computer behavior : an exploratory study,* Thèse en Philosophie, Département of Psychology University of Manitoba Winnipeg, Manitoba.
- Rouquette M-L., Rateau P., 1998, *Introduction à l'étude des représentations sociales*, Grenoble, Presses Universitaires de Grenoble.
- Russel R., 2001, *Stratégie Anti-Hackers*, Paris, Eyrolles.

S

- Schutz A., 1987, *Le Chercheur et le quotidien*. Phénomènologie des sciences sociales, Paris, Méridiens Klincksieck, pp. 9-10.
- Service Central de la Sécurité des Systèmes d'Information (S.C.S.S.I.), 1994, *La menace et les attaques informatiques*, Issy-les-Moulineaux.
- Simmel, 1981, *Sociologie et épistémologie*, Parie, PUF.
- Sukhai N., 2004, *Hacking and Cybercrime*, Proceedings of the first annual conference on Information security curriculum development InfoSecCD'04, ACM Press.
- Symantec, avril 2006, *Pirates, phishing virus...le cybercrime s'organise pour vider les caisses*, guide de la sécurité informatique, 92 Courbevoie.

T

- *The HoneyNet Project*, 2004, *Know Your Enemy: Learning about Security Threats (2nd Edition)*, Addison-Wesley Professional; 2ème édition, Canada.

- Tregouet R., 1998, *Des pyramides du pouvoir aux réseaux de savoirs*, t.1, Rapport d'information, 311-1997/1998, Commission des Finances, Sénat.

W

- Wacquant W., 2002, *Corps et âme. Carnets ethnographiques d'un apprenti boxeur*, Marseille, Agone.
- Wolkowicz M., 1996, « *Guerres dans le cyberespace, services secrets et Internet »*, note de lecture in Réseaux (N°75).

Annexes

Annexe 1 - Références (WEB)

http://www.cert.org

http ://www.first.org

http://www.ossir.org

http://www.urec.fr/securite

http://www.gocsi.com

http://www.sans.org

http://www.clusif.asso.fr

http://www.ssi.gouv.fr

http://www.zataz.com

http://www.clussil.lu

http://www.cases.public.lu

http://www.ansil.eu

http://www.honeynet.org

http://www.csrrt.org.lu

http://www.tuxedo.org

http://www.hack.lu

http://www.2600.com

http://www.defcon.org

http://www.ccc.de

http://www.spiral.lu

http://jph.cases-cc.org

http://www.oecd.org/doc/M00033000/M00033183.doc

http://www.cindynics.org

http://europa.eu.int/eur-lex/fr/com/cnc/2000/com2000_0890fr01.pdf

http://www.europa.eu.int/eur-lex/fr/com/cnc/2001/com2001_0298fr01.pdf

http://www.conventions.coe.int

http://europa.eu.int/scadplus/leg/en/lvb/l33193.htm

http://europa.eu.int/information_society/eeurope/news_library/eeurope2005/

http://www.cert.org

http://www.eicar.org/camdier/

http://pages.infinit.net/cybersoc/hackers/consequencestxt.htm

http://denislabrosse.net/articles/index.php

http://www.mediametrie.fr

http://www.usdoj.gov/criminal/cybercrime/FBI2005.pdf

http://www.cnrs.fr/Infosecu

Annexe 2 – Statistiques CSI/FBI 2005

L'étude de l'année 2005 succède à neuf autres. Le sondage a été fait sur la base des réponses de 700 professionnels en charge de la sécurité des systèmes d'information d'entreprises américaines, d'organismes gouvernementaux, d'institutions financières, d'établissements médicaux et d'universités.

Cette étude 2005 aborde les questions principales des enquêtes de CSI/FBI, à savoir :

- Utilisation non autorisée des parcs informatiques d'entreprise.
- Le nombre d'incidents tant internes qu'externes.
- Types des attaques ou d'abus détectés.
- Mesures prises en réponse aux intrusions.

Elle aborde également plusieurs questions naissantes de sécurité qui sont pour la première fois apparues lors de l'enquête CSI/FBI de 2004. La plupart d'entre elles s'apparentent aux décisions économiques prises par les entreprises en ce qui concerne la sécurité des systèmes d'information, notamment la prise en compte de la gestion de risques de sécurité.

Les champs suivants sont pris en compte :

- Comment les entreprises évaluent-elles la performance (efficience et efficacité) de leurs investissements en matière de sécurité de l'information ?
- Quelles sont les formations en sécurité pour répondre à leurs propres besoins ?

- Quelles sont les dépenses des entreprises en ce qui concernent les investissements de sécurité ?

- Quel est l'usage des audits et d'assurance sécurité ?

- Quelles sont les portions de budget IT allouées à la sécurité ?

Points clés de l'étude 2005 :

Note : comparativement à la précédente année, le nombre de répondants au sondage pour une taille d'échantillon inchangée, a connu une nette croissance, passant de 494 réponses en 2004, à 700 réponses en 2005.

- les attaques par virus constituent la source des plus grandes pertes financières,

- les accès illicites occupent la seconde position en termes de pertes occasionnées, remplaçant le *Denial of Service* (3ème position pour le rapport 2004),

- le montant total des pertes occasionnées par le cybercrime baisse de manière générale, le nombre des répondants ayant augmenté, la moyenne des pertes par répondant baisse significativement. Cependant, deux menaces offrent une moyenne par répondant en augmentation : l'accès illicite aux informations et le vol d'information propriétaire,

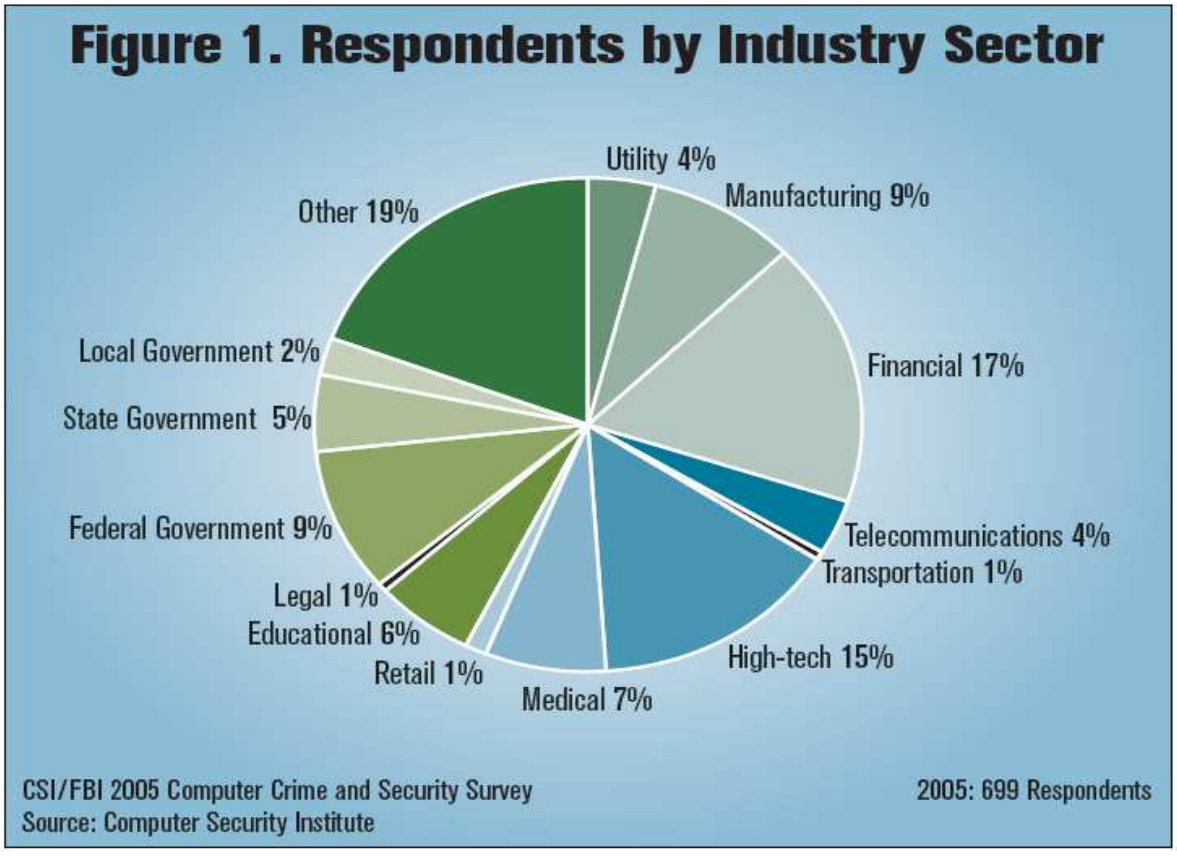
- les incidents sur sites web ont considérablement augmenté,

- le pourcentage des sociétés victimes d'incidents de sécurité et déposant plainte chute continuellement, avec pour principale raison : la peur de la publicité négative.

Caractéristiques des répondants :

Comme l'indique la figure suivante, les sondés proviennent de divers secteurs d'activité économiques, une manière d'illustrer le fait que la sécurité des systèmes d'informations n'est pas simplement restreinte aux entreprises spécialisées dans les NTIC (Nouvelles Technologies de l'information et de la Communication), mais concerne désormais toute activité économique « numérisée ».

Note : le succès de l'étude repose essentiellement sur la confiance des répondants en relation avec la conservation de l'anonymat des réponses.



- Figure 23. Rapport CSI/FBI 2005 – Réponses par secteur industriel

Le plus grand nombre de réponses provient du secteur financier (17 %), puis le secteur IT (15 %), et enfin industriel (9 %). La moitié des réponses provient d'entreprises de plus de 1500 employés. 23 % des réponses proviennent des entreprises comprenant de 1550 à

9999 employés, 11 % de celles de 50000 et plus, enfin 20 % en provenance des entreprises de moins de 100 employés.
57 % des entreprises répondant à cette enquête, génèrent plus de 100 millions $ de revenus annuels, et 37 % plus d'un milliard $.
Note : tout répondant est un membre actif de CSI, ou ayant assisté à une des conférences de l'organisme.

- Préoccupations sécuritaires demeurant faibles :

Les responsables sécurité des systèmes d'information sont de plus en plus conscients que les aspects financiers et les mesures de management liées à la sécurité sont tout aussi importants que les mesures techniques prises.

Malgré cette prise de conscience, les budgets liés à la sécurité restent cependant faibles, puisque plus de 73 % des entreprises répondent dédier seulement moins de 5 % de leur budget IT à la sécurité.

- Moins de 1 % : 11 %
- entre 1 et 5 % : 48 %
- plus de 5 % : 27 %

15 % des sondés ne connaissent même pas ce budget sécurité, ce qui tend à montrer que la sécurité informatique n'est pas encore acquise véritablement au niveau de la culture d'entreprise. Les responsables informatiques doivent donc prouver au niveau de la direction d'entreprise la nécessité d'investir dans la sécurité.

Pour ce faire, les responsables de la sécurité informatique sont amenés à utiliser des outils financiers pour rendre compte des menaces actives pouvant nuire à leur système d'information. Le rapport CSI/FBI indique que 38 % des responsables utilisent des formes d'évaluation économique de leurs dépenses sécurité :

- ROI (*Return On Investment*) : 38 %
- NVP (*Net Present Value*) : 18 %
- IRR (*Internal Rate of Return*) : 19 %

Plus de 87 % des répondants établissent des audits de sécurité (82 % en 2004). La majorité des répondants voit les formations de sensibilisation à la sécurité comme importantes.

Concernant les investissements au niveau de la sécurité, le rapport 2004 indiquait une croissance plus faible que la croissance générale. Les résultats 2005 permettent d'affiner ce phénomène, en effet, les sociétés représentées ayant un chiffre d'affaire annuel inférieur à 10 millions de dollars, dépensent en moyenne 700 dollars en sécurité informatique par employé, alors que pour les autres la moyenne se situe aux alentours de 250 dollars. Cette situation s'explique par le fait que les investissements en sécurité s'étalent alors sur un ensemble d'employés plus large.

Note : les pourcentages importants d'intérêt de mesure de type *ROI*, *NPV*, ou *IRR*[280] reposent sur des investissements importants en regard de la sécurité, suite aux nombreuses communications relatives aux failles de sécurité aux forts préjudices, ces investissements sécurité ont été vécus comme des projets « *must do* ». Bien que, en terme de type de mesure, les répondants ne sachent pas véritablement comment répondre à cette question, ne sachant pas ce qui est en place en interne.

Si on analyse l'investissement en fonction des secteurs d'activités des entreprises, on se rend compte que les entreprises étatiques sont au sommet de la hiérarchie, ce qui s'explique par le fait qu'un certain nombre de lois a été voté dans ce sens.

Un autre point abordé par le rapport CSI/FBI concerne l'*outsourcing* (service d'externalisation des ressources ou données), qui n'augmente pas, en effet moins de 1 %

[280] Kurtz, 2005, numerous state laws concerning information security recently enacted http://www.virtualmgmt.com/csia/news/may_execdir.html

Lawrence A.Gordon, Martin P.Loeb, *« Return of Information Security Investment : Myth vs. Reality »*, Strategic Finance, November 2002, pp 26-31.

Lawrence A.Gordon, Martin P.Loeb, Tashfeen Sohail, *« A framework for using Insurance for Cyber Risk Management »* Communications of the ACM, Mars 2003, pp 81-85.

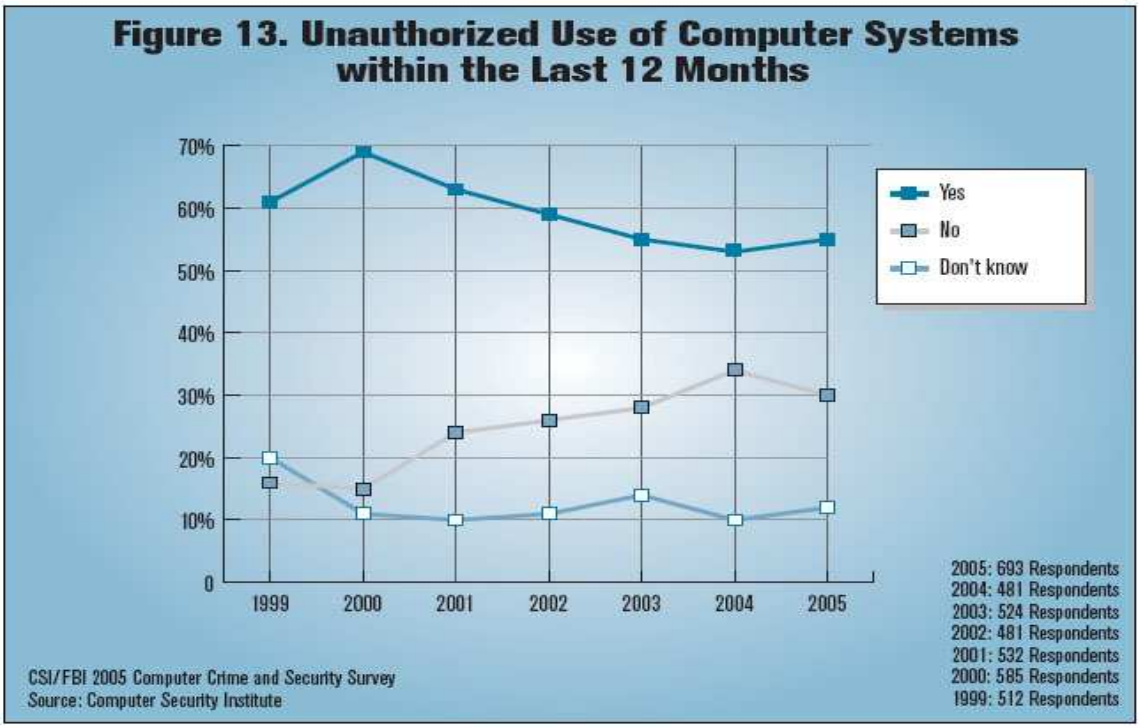
Katherine Campbell, Lawrence A.Gordon, Martin P.Loeb, Lei Zhou, *« The economic Cost of publicly Announced Information Security Breaches : Empirical Evidence from the Stock Market »*, Journal of Computer Security, vol. 11, N°3, 2003, pp. 431-448.

Lawrence A.Gordon, Martin P.Loeb and William Lucyshyn, *« Sharing Information on Computer System : An economic Analysis »*, Journal of Accounting and Public Policy, Vol. 22, N° 6, 2003, pp 461-485.

des entreprises affirment confier plus de 80 % de leurs fonctions de sécurité à l'extérieur, et plus de 63 % ne délèguent rien du tout. Alors que la tendance générale de l'*outsourcing* est à la hausse, on peut donc en conclure que l'aspect sécurité semble privilégié par les entreprises.

Le dernier point abordé par le rapport au niveau financier est l'assurance. Toutes les mesures techniques, tel que les « *IDS » (« Intrusion Detection System »)*, « *Firewall* », ou encore biométrie n'empêchent pas les infractions ainsi que les pertes financières à 100 %. Ainsi, on remarque que seulement 25 % des répondants affirment utiliser une assurance externe pour aider la gestion des risques de sécurité IT, pourtant il semblerait que cette voie devrait prendre un certain essor dans un futur proche.

- Evolution des utilisations abusives des systèmes d'information durant les 12 derniers mois :



- Figure 24. Rapport CSI/FBI 2005 – Usage illégal d'ordinateurs /12 derniers mois

Le nombre de sondés a véritablement augmenté depuis 2004. Les nombreuses campagnes de sensibilisation[281] trouvent un écho au cœur des sociétés de plus en plus conscientes des problématiques de sécurité. Cependant, le mombre de sociétés ne sachant pas si elles ont été victimes d'intrusions a sensiblement augmenté. A ce titre, soit l'évolution des techniques d'intrusion (de type « *rootkits backdoors* ») rend la détection de ces derniers difficiles, soit l'évolution des mentalités amène les sondés à être prudents et à remettre en doute l'efficacité de leur protection.

- Analyse des fréquences des incidents et de leur provenance :

Table 1: How Many Incidents? From the Outside? From the Inside?

How many incidents, by % of respondents	1–5	6–10	>10	Don't know
2005	43	19	9	28
2004	47	20	12	22
2003	38	20	16	26
2002	42	20	15	23
2001	33	24	11	31
2000	33	23	13	31
1999	34	22	14	29
How many incidents from the outside, by % of respondents	**1–5**	**6–10**	**>10**	**Don't know**
2005	47	10	8	35
2004	52	9	9	30
2003	46	10	13	31
2002	49	14	9	27
2001	41	14	7	39
2000	39	11	8	42
1999	43	8	9	39
How many incidents from the inside, by % of respondents	**1–5**	**6–10**	**>10**	**Don't know**
2005	46	7	3	44
2004	52	6	8	34
2003	45	11	12	33
2002	42	13	9	35
2001	40	12	7	41
2000	38	16	9	37
1999	37	16	12	35

CSI/FBI 2005 Computer Crime and Security Survey — 2005: 453 Respondents
Source: Computer Security Institute

- Tableau 18. Rapport CSI/FBI 2005 – Répartition des incidents internes/externes

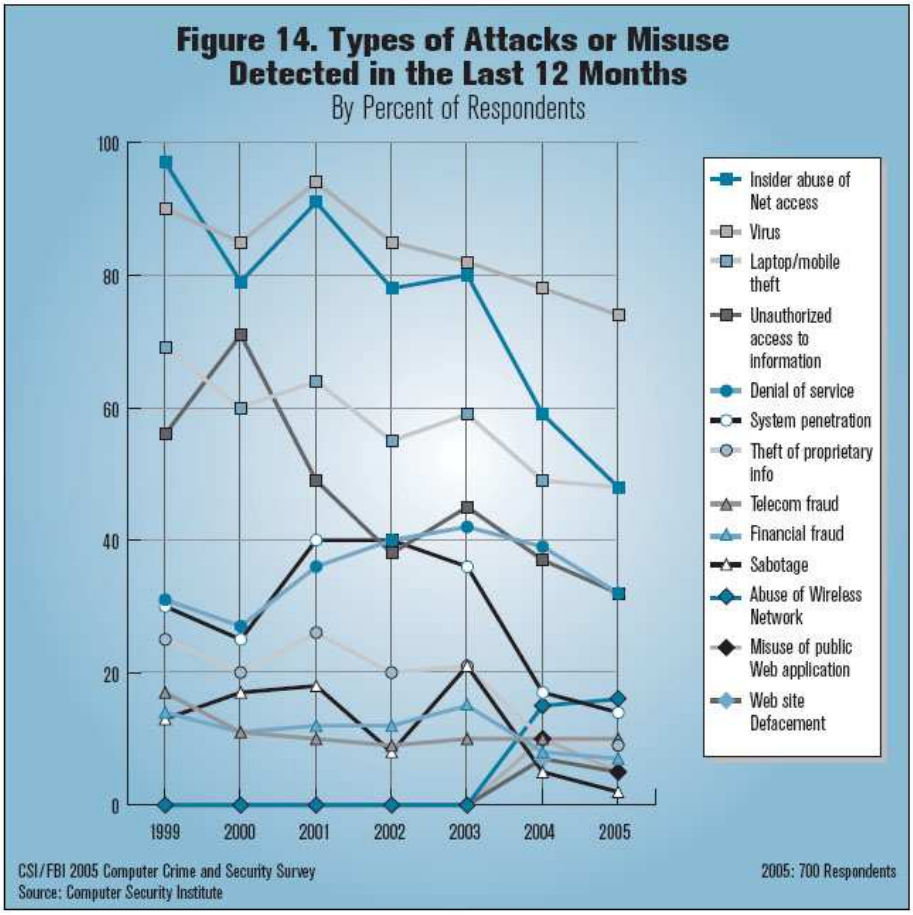
[281] http://www.cybercrime.gov

La chute amorcée du nombre de failles exploitées avec succès durant les quatre dernières années est stoppée, en effet 56 % des répondants déterminent un nombre en augmentation des accès illicites, en regard des 53 % relevés l'année dernière.
La fréquence des attaques décroît :

- 2004 : nombres d'incidents de sécurité >10 : 12 %
- 2005 : nombres d'incidents de sécurité >10 : 9 %
- 2004 : nombres d'incidents (depuis extérieur) de sécurité >10 : 9 %
- 2005 : nombres d'incidents (depuis extérieur) de sécurité >10 : 8 %
- 2004 : nombres d'incidents (depuis intérieur) de sécurité >10 : 8 %
- 2005 : nombres d'incidents (depuis intérieur) de sécurité >10 : 3 %

Note : cependant, le nombre de réponses « *don't know* » augmente considérablement pour chaque partie. En fait, on ne peut dire avec certitude si les dirigeants de ces sociétés américaines pensent être moins attaqués, ou s'ils mettent d'avantage en doute l'efficacité de leurs contre-mesures. Finalement, la baisse des activités illicites pourrait simplement correspondre à un « effet d'optique ».

- Analyse des types d'attaque :



- Figure 25. Rapport CSI/FBI 2005 – Type d'attaques ou mauvaise manipulation /12 derniers mois

Attaques détectables prises en compte par l'étude :

- Accès illégal réseau.
- Virus.
- Vols PC/Mobiles portables.
- Accès illicites à l'information.
- « *DoS* » (Denial of Service).
- Pénétration Système.

- Vol d'informations propriétaires.
- Fraude aux Télécom.
- Fraude Financière.
- Sabotage.
- Abus du réseau Wireless.
- Abus application web publique.
- « *Defacement* » site web.

De l'ensemble des attaques détectées, il ressort que pour les répondants :

- dans pratiquement toutes les catégories et pour tous les répondants, les abus, depuis des années, ont amorcé un déclin notable

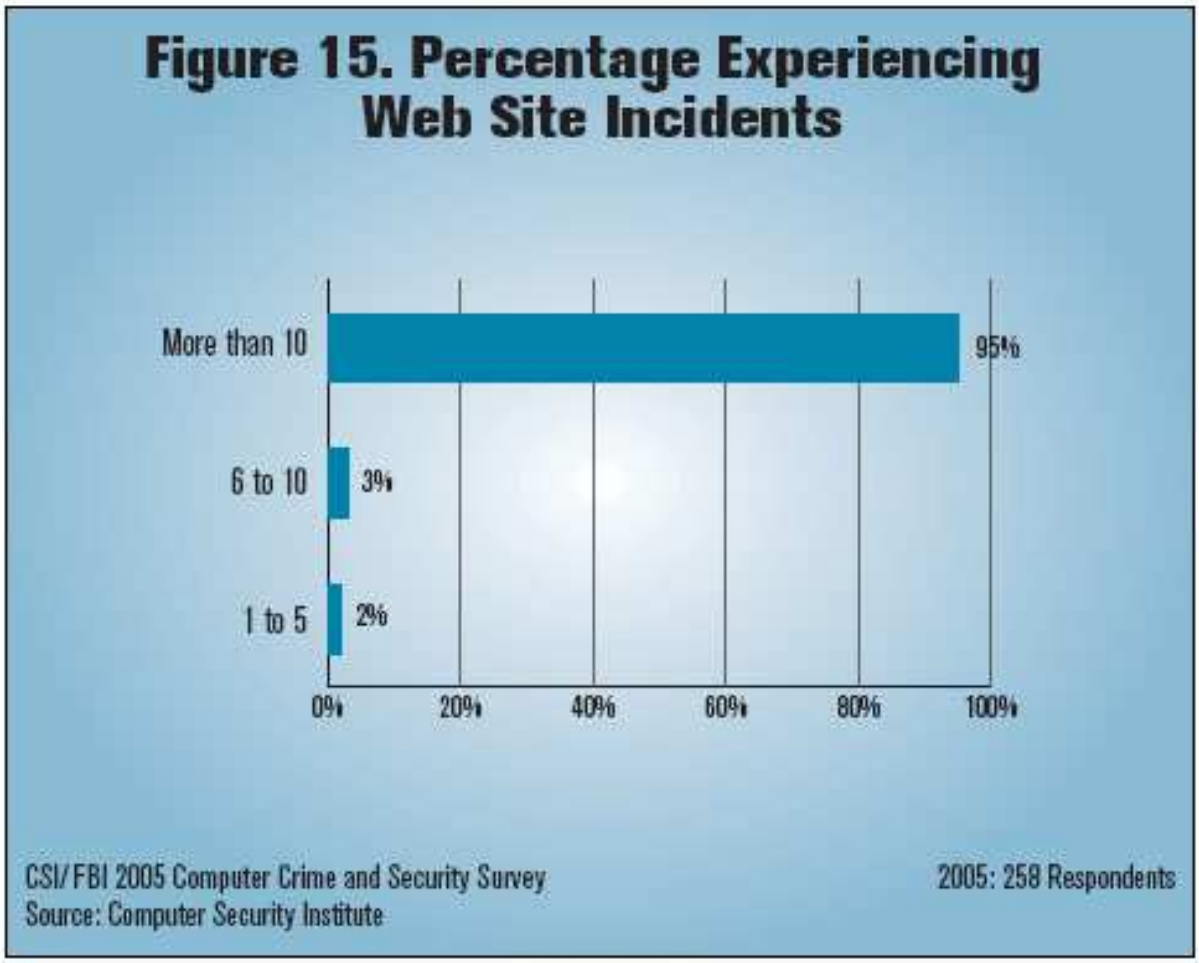
- la seule catégorie ayant véritablement progressée est l'abus de réseau de type « *wireless » (sans fil)* (« *wifi* » : catégorie ajoutée seulement depuis l'année dernière, avec les incidents sur sites web)

Note : concernant le « *wifi* », il est à noter que cette technologie est relativement récente et très convoitée par les employeurs qui y voient la possibilité de travailler sans les contraintes d'un réseau physique (absence de câblage).

Néanmoins les mesures de protection basiques telles que la clé « *WEP »* ne sont pas toujours utilisées alors qu'elles offrent une protection déjà mineure et les paramétrages demeurent trop souvent ceux par défaut.

Actuellement, la sécurité des technologies « *wifi* » au sein des sociétés n'est pas considérée avec suffisamment d'intérêt. Concernant les attaques de type « *defacements* » les auteurs du rapport mettent en avant le laxisme des sociétés qui pour une question de *ROI* préfèrent subir et réparer que protéger. Il est enfin à noter que les attaques par virus et les *DoS* restent en tête malgré des baisses significatives.

- Incidents sur les sites Web des sociétés :



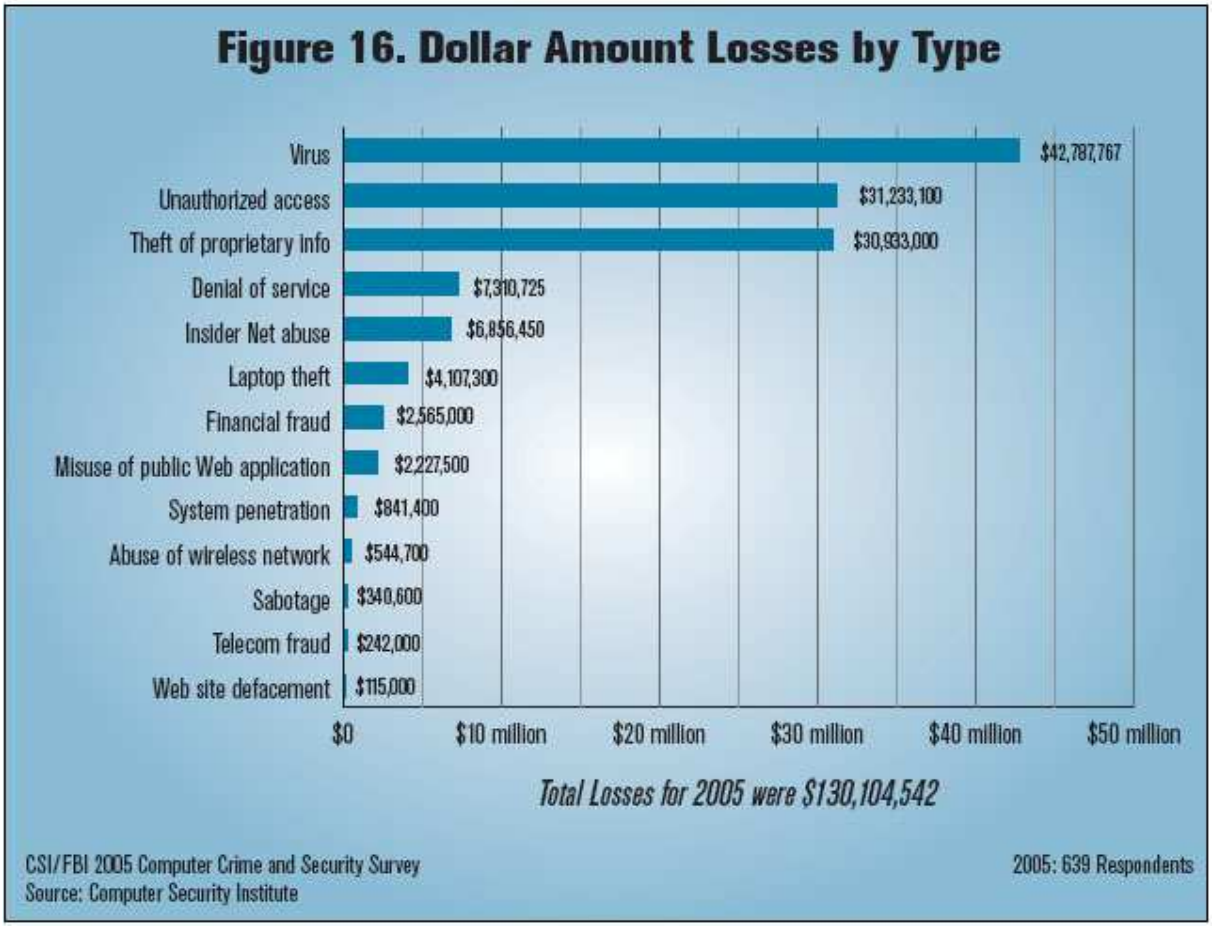
- Figure 26. Rapport CSI/FBI 2005 – Relevés d'expérience d'incidents sur site web

2004 : attaques de 1 à 5 : 89 % ; attaques>10 : 5 %

2005 : attaques de 1 à 5 : 2 % ; attaques>10 : 95 %

La quasi-totalité des sondés subissent de nombreux incidents sur leur site web. Cela s'explique tout d'abord par l'exposition au grand public des pages web, en effet plus la visibilité est large, plus le nombre potentiel d'attaquants est important, plus la menace est grande.

- Analyse des estimations des pertes :



- Figure 27. Rapport CSI/FBI 2005 – Montant des pertes par type d'attaques

Rappel : les résultats de cette étude sont à considérer avec précaution, et doivent toujours être remis dans le contexte.

Les pertes totales rapportées par les répondants sont en baisse :

2004 : 141.496.560 $ (269 répondants)
2005 : 130.104.542 $ (639 répondants)

Les pertes par répondants sont les suivantes :

2004 : 526.010 $
2005 : 203.606 $
(Soit une baisse de 61 %)

Le « top 3 » des pertes est le suivant :

1 – Virus : 42.787.767 $
2 – Accès illicites : 31.233.100 $
3 – Vol d'informations propriétaires : 30.933.000 $

Le *web site defacement* (défiguration de site web) est la menace qui montre le taux de perte le plus bas sur les 13 menaces relevées. Les entreprises concernées semblent avoir pris des mesures économiques rationnelles pour contrer cette menace.

Cependant, face à la tendance générale de la baisse des coûts engendrés par les menaces, qui peuvent s'expliquer par l'augmentation des sensibilisations ciblées et dédiées aux menaces (virologie par exemple), deux catégories augmentent tout de même fortement (par rapport à 2004) :

- Accès illicites aux informations :

2004 : 51.545 $
2005 : 303.234 $

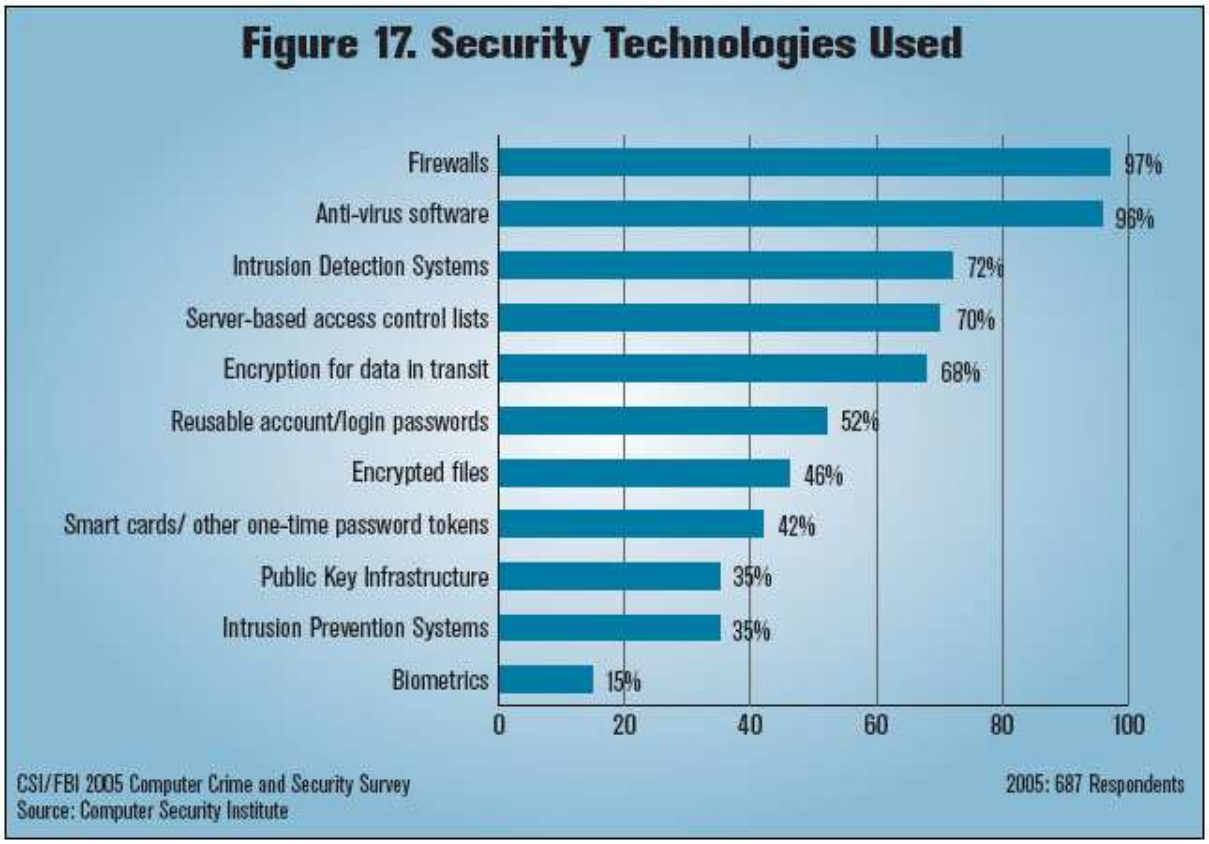
- Vol d'informations propriétaires :

2004 : 168.529 $
2005 : 355.552 $

De plus, les consultants sécurité des systèmes d'information indiquent que les outils actuels d'attaques peuvent permettre une saturation du réseau possible en moins de 15 minutes (pouvant entraîner des pertes financières « gargantuesques »).

Note : Le CSI indique que les répondants semblent capables de mesurer facilement les pertes « explicites » (réinstallation de software, reconfiguration d'ordinateurs…), mais pas les menaces de type « implicites » (couverture média des faiblesses vis-à-vis d'un piratage) et ces dernières, difficiles à mesurer, sont non représentées dans le rapport, cependant elles pourraient être marquées *via* une baisse de capitalisation boursière, par exemple.

- Outils de la sécurité mis en place :



- Figure 28. Rapport CSI/FBI 2005 – Technologies de sécurité utilisées

Les outils classiques de type « *Firewall* », « antivirus » et « *IDS* » sont les plus prisés. Cela correspond-il à la véritable réalité des menaces ? En effet, la maîtrise de la face technique du cybercrime ne peut occulter la face sociale de la problématique et

notamment la réalité sociale des cyberdélinquants[282], dépassant souvent cette réalité de contre-mesures techniques.

(2005 : résultats idem 2004).

La plupart des organisations utilisent des systèmes de défense contre les attaques réseau :

- utilisation de firewall : 97 %
- anti-virus : 96 %
- *IDS* : 72 %
- *IPS* (*Intrusion Prevention System*) en baisse de 45 % à 35 %, ce dispositif agît en temps réel à la différence d'un *IDS* (vu *supra*)).

- Audit de sécurité et programmes de formation à la SSIC :

Depuis l'année dernière CSI/FBI a introduit de nouvelles questions relatives aux différents aspects d'amélioration de la sécurité informatique (la littérature a longtemps indiqué en première étape d'un programme de sécurité de l'information : l'audit de sécurité (tel que par exemple le diagnostic qualité de type sécurité dans la méthode d'analyse de risques française MEHARI (MEthode Harmonisée d'Analyse de RIsques)).

Audit de sécurité :

- 2004 : 82 %
- 2005 : 87 % (technique qui est plus diffusée aujourd'hui, la maîtrise des concepts et des outils devenant notamment plus compréhensible[283]).

[282] Http://jph.cases-cc.com

[283] J.-P. Humbert, N. Mayer, *La gestion des risques pour les systèmes d'information*, Misc 24, Mars-Avril 2006

F. Hermann, J-P. Humbert, D. Khadraoui, Y. Lanuel, N. Mayer, E. Wies, *Paroles de Professeurs : Gestion de la sécurité : les défis*, Mag Securs, Juin-Août 2006

Il a été largement reconnu que la sécurité informatique est plus un problème de management qu'un problème technologique. Ainsi, en lien avec des audits de sécurité, les organisations ont investi dans la mise en place de programmes de sensibilisation à la SSIC. Deux questions ont été injectées dans l'étude à ce propos quant à l'étendue et l'importance du programme de sensibilisation SSIC dans l'entreprise.

- Le partage d'informations relatives aux incidents réseaux :

La médiatisation de nombreuses failles de sécurité découvertes et les impacts associés formalisent un besoin de plus en plus reconnu de partager ce type d'informations, notamment sur les intrusions de sécurité. Cependant, il n'appert aucune augmentation de volonté de partager de telles informations avec la Police ou encore avec d'autres autorités légales.

Bien que 63 % des répondants partage ce type d'informations (il s'agit du plus fort taux de partage depuis une période de sept ans), les « *reporting* » vers la police sont en baisse continuelle. Les raisons identifiées sont simples :

- perception d'un résultat de mauvaise publicité associée (51 %),
- avantage concurrentiel possible d'une telle information (33 %).

Les organisations semblent au courant du rôle de combat mené par les forces de l'ordre, mais choisissent cependant pour ces raisons évoquées de ne pas rapporter les faits.

- Conclusion :

L'importance des systèmes d'information informatisés croît considérablement depuis une vingtaine d'année. Depuis 1995, Internet joue aussi un rôle crucial pour le développement économique des organismes modernes.

La sécurité informatique a donc trouvé sa place en se focalisant au départ sur la question d'ordre technique comme le chiffrement, les contrôles d'accès ou encore les systèmes de détection d'intrusion.

Annexe 3 – Statistiques Panorama Cybercrime Clusif 2005

Résultats : Panorama cybercrime 2005 :

- L'économie souterraine

a) La persistance des robots

Rappel : un robot est un programme malveillant permettant une prise de contrôle à distance de machine vulnérable afin de former un réseau d'attaque caché.

Pour s'implanter, il existe plusieurs méthodes pour être déposé au cœur de sa cible, cela *via* :

- un courrier électronique,
- un vers ou virus,
- un cheval de Troie,
- un autre robot déjà présent.

Chaque robot est créé dans un but précis : on en découvre entre 25 et 50 par jour, en moyenne.

Il s'exécute silencieusement sur chaque système piraté et se connecte automatiquement à un serveur *IRC* (*Internet Relay Chat*) prédéfini pour rejoindre son « *botnet* » (Réseau robot). Dès lors, chaque système piraté peut être piloté à distance par son concepteur ou par celui qui « loue » le « *botnet* ».

Exemple :

En octobre 2005 : la police hollandaise interpelle trois hommes soupçonnés de diriger un réseau de « *botnet* » de 100 000 ordinateurs.

En novembre 2005 : un groupe de pirate basé au Moyen-Orient serait parvenu à prendre le contrôle de 17 000 ordinateurs.

L'utilisation de programmes malveillants dans la diffusion de logiciels pirates de type « *adwares* » ne se limite pas seulement à ces quelques exemples. En effet, pour des personnes peu scrupuleuses c'est un moyen facile de gagner de l'argent, cependant, pour les sociétés publicitaires, la conséquence peut correspondre à une nouvelle atteinte à leur image de marque.

b) <u>La vitalité des chevaux de Troie</u>

Les chevaux de Troie sont toujours à la mode, qu'il s'agisse de porte dérobée ou de « *keylogger* » (logiciel de capture de frappes clavier).

En 2005, par exemple, une escroquerie de type cheval de Troie, qui durait depuis de plus d'un an, fut mise à jour : chaque « cible » faisant l'objet d'une attaque *via* un cheval de Troie de dernière génération et à usage unique, ce qui avait pour conséquence l'absence de détection par l'anti-virus du méfait. Celui-ci était intégré à un CD ou envoyé *via* un mail contenant une proposition commerciale fictive. Une fois le cheval de Troie installé, le concepteur fournissait à son client piraté les informations afin que celui-ci puisse se connecter de nouveau, contre la « modique » somme de 3000 euros (sic).

Dans le registre des « *keyloggers* », une vaste escroquerie a également été mise en évidence en mars 2005 dans les bureaux londoniens de la banque japonaise « Sumitomo ». Dans un premier temps, les soupçons se sont portés vers un « *keylogger* » logiciel, mais quelques jours plus tard, il fut découvert qu'il s'agissait de « renifleur » de clavier de type matériel (dont le coût varie seulement actuellement de 20 à 200 dollars en fonction de la capacité de la mémoire).

Via ces quelques exemples, on remarque que les attaques sont de plus en plus ciblées. Même si les détections génériques sont efficaces, si un programme est crée spécifiquement pour une attaque ciblée, celui-ci risque de passer inaperçu. Cependant, il est à retenir que, en plus des solutions d'espionnages de type logiciel, il faut aussi faire attention aux solutions matérielles, de plus en plus difficiles à détecter.

Ces informations renforcent le nécessaire besoin de partage des connaissances en lien avec le domaine des attaques de type cybercrime (voir conclusion rapport CSI/FBI *supra*).

c) « *The rootkits stike-back* »

Ceux-ci permettent une meilleure furtivité pour des programmes malicieux déjà recensés (robots, renifleurs de mot de passe, portes dérobées…).

Diverses sociétés commerciales utilisent le concept comme un outil de dissimulation et le monde « *underground* » le récupère aussi (« *rootkit adware »,* Sony BMG). Des sociétés peu scrupuleuses n'hésitent pas non plus à les mettre en vente sur internet.

Dans le « top 10 » des « *rootkits* » (outil intégré d'attaques à distance), on retiendra des noms tel que « *FURootkits* », « *IsPro* », « *Hacker Defender* »…

Prenons en exemple le « *rootkit* BMG Sony », qui a été découvert le 31 octobre 2005. Le 3 novembre 2005, Sony indique que le système existe depuis environ 8 mois. Il propose alors des outils de détection et de désinstallation. Diverses vulnérabilités sont mises à jours. Ce « *rootkit* » est réutilisé par la scène « *underground* » (et permet entre autre de contourner les systèmes anti-triche du célèbre jeu en ligne « *World of Warcraft* »). Ce « *rootkit* » est maintenant détecté par les anti-virus.

Vu le fonctionnement des « *rootkit* », ils sont très difficiles à détecter mais divers outils permettent néanmoins de les mettre en évidence comme « *RootkitRevealer* ». Pour ce faire il effectue plusieurs opérations successives :

- il effectue une première détection qui lui permet d'obtenir la liste de tous les fichiers du système utilisant l'API normale de Windows,

- une seconde mesure est alors effectuée, où le logiciel construit une nouvelle liste de fichiers, en lisant directement le contenu du disque sans passer par les *API* de Windows. La comparaison des deux états permet alors de mettre en valeur les fichiers cachés (qu'ils soient légitimes ou non).

Il existe d'autres outils de détection comme « *BlackLight* », « *UnHackMe* » ou bien encore « *HijackThis* » qui fonctionne sur le même principe.

Les anti-virus constituent aussi une bonne solution à la détection de ce phénomène :

- les recherches actuelles mettent en évidence qu'il est possible de mettre en œuvre des détections génériques,
- pour le moment, la meilleure solution de détection consiste à rechercher les processus cachés en mémoire,
- il sera toujours nécessaire pour le « *rootkit* » de se lancer à la « re-connexion » de la machine. C'est à ce moment là qu'il faut alors le détecter.

- L'espionnage économique

Plusieurs cas d'espionnage économique présumé ou avéré ont marqué l'actualité en 2005, avec par exemple le piratage de la société Ericsson en Suède, la transmission de secret de fabrications à des concurrents aux Etats-Unis, l'affaire Valéo en France, ou bien encore l'affaire d'espionnage avec cheval de Troie en Grande Bretagne et Israël concernant divers pays.

L'affaire Valéo mérite plus de détails. En France en avril 2005, une stagiaire est soupçonnée d'avoir volé des informations confidentielles.

Note : l'affaire n'ayant pas encore été jugée, cette personne est pour l'instant présumée innocente.

Les faits : une étudiante chinoise est soupçonnée d'avoir copié des données de l'entreprise d'équipement automobile Valéo sur un disque dur personnel. Elle est mise en examen fin avril 2005 et placée en détention provisoire pendant 53 jours. C'est l'AFP qui révèle l'affaire dans une dépêche qui signale l'incarcération d'une jeune fille « *soupçonnée d'espionnage industriel* » (sic).

La justice a été saisie pour accès frauduleux dans un système automatisé de donnée et abus de confiance (qualification de « cybercrime »). Selon les informations parues dans différents médias, la jeune stagiaire aurait sorti des données de l'entreprise et

les auraient ramenées chez elle. La jeune femme explique à la presse qu'elle les a copiées pour son rapport de stage.

Celle ci explique dans une interview accordée au quotidien « Libération », que les étudiants ont pris l'habitude d'apporter leur disque dur à l'université, qu'elle en a fait de même en entreprise. Elle affirme qu'elle aurait récupéré 30 à 40 fichiers auxquels elle a eu accès sur le réseau intranet et pensait donc qu'il n'y avait rien d'illégal à cela. Elle explique également avoir effacé des données d'un PC pour obtenir un gain de place afin de pouvoir travailler.

En conclusion, il paraît inquiétant que la politique de sécurité au sein de l'entreprise soit aussi laxiste quant à la gestion des droits d'accès aux informations « jugées confidentielles». Cela pose également, de manière générale, la question de la sécurité du patrimoine informationnel dans les entreprises.

- Vol et pertes de données

De nombreuses affaires de divulgation de données personnelles (y compris bancaires) ont été mises en évidence, au cours de l'année 2005, et concernent entre autre :

- Les vols d'ordinateurs.
- La perte de support de sauvegarde.
- La compromission de systèmes.

Les différentes affaires évoquées, du fait du volume et du type de données divulguées, mettent en avant non seulement les risques de fraudes financières mais aussi d'usurpation d'état civil. Les exemples cités proviennent essentiellement des Etats Unis, du fait des lois imposant aux entreprises victimes de divulgations de prévenir les personnes concernées par ces « fuites » de données.

<u>- Vols d'ordinateurs</u>

Le groupe médical « San José » (en mars 2005), constate une perte de données personnelles concernant 185 000 patients.

Les données de facturations étaient transférées depuis les serveurs du réseau vers deux postes de travail pour les besoins de l'audit annuel de la structure. On constate que les deux ordinateurs ont été dérobés. Les patients sont alors contactés par l'hôpital (seulement une partie des données avaient été cryptée sur les disques durs).

- Concernant la perte de supports de sauvegarde :

« Bank of America » constate en février 2005 la perte de bandes magnétiques (ou vol ?) contenant des informations bancaires relatives à 1,2 millions d'employés de gouvernement. Les données contenaient des informations sur l'ensemble de ces personnes (numéro de compte bancaire, adresse,…).

« Citigroup » est victime, en avril 2005, de la perte par UPS de bandes contenant les données de 3,9 millions de clients. La perte est occasionnée lors du transfert vers une institution de vérification de l'historique.

- Concernant la compromission de données :

Le « *cardsystems* » (avril 2005) : les prestataires technique de Visa et de MasterCard assurent le traitement de transactions, et l'on découvre la compromission du réseau de « *cardsystems* » avec comme champs d'actions possible environ 40 millions de numéro de cartes de crédits (qui auraient dû ne pas être conservés). 68 000 numéros ont été récupérés, et divers établissements bancaires internationaux indiquent que cette divulgation aurait entraîné des transactions frauduleuses.

La société « LexisNexis », entreprise spécialisée dans l'édition et l'information professionnelle, est victime en avril 2005 de plusieurs incidents de sécurité qui ont eu lieu au sein d'une de leur succursale (« Seisint ») de leur groupe. Il en résulte une fuite concernant quelque 32 000 personnes avec à la clé des informations contenant leur nom, adresse, numéro de sécurité sociale, permis de conduire…

Quels sont donc les enjeux et les conséquences liés à ces actes frauduleux ?

Il est important de remarquer que les données personnelles sont devenues un bien recherché et monnayable. Ces informations peuvent être obtenues de deux manières différentes :

- soit directement, l'attaque est dirigée afin d'accéder à ces données,
- soit indirectement, dans la mesure où la récupération de ces informations n'était pas l'objet premier de l'attaque (dans le cas vol d'ordinateurs par exemple).
- Les risques liés à la divulgation sont encore aggravés par la faible sensibilisation du public vis-à-vis de ces menaces.

Il existe cependant diverses méthodes pour se prémunir contre ce type d'attaque tel que :

- des mesures techniques : sécurisation des systèmes et des réseaux, chiffrement des données sensibles sur les supports de sauvegarde ainsi que sur les ordinateurs portables,
- des mesures organisationnelles : sensibilisation des collaborateurs sur les mesures de sécurité, avec la mise en œuvre de procédure de contrôle et d'évaluation de la sécurité.

<u>- Du harcèlement jusqu'aux violences physiques</u>

Il s'agit ici d'agressions et de violences qui ne sont plus virtuelles. De multiples cas ont été révélés ou résolus au cours de l'année écoulée. Ces faits nous rappellent que la criminalité informatique est le fait d'être humain et pas seulement de machines. Le degré de souffrance engendré peut aller, dans les cas extrêmes, jusqu'à la mort.

L'outil informatique sert ici aux agresseurs à se défouler, à porter atteinte à l'intimité d'autrui, inciter à la haine, se vanter de leurs méfaits, appâter les victimes et dans quelques cas extrêmes peut déboucher sur des crimes, qui eux peuvent être bien réels. Lors de la présentation du panorama cybercrime CLUSIF à Metz, il a été annoncé un aspect très « passionnel – émotionnel » dans ces actes.

Il existe de nombreux faits relevés :

En Grande Bretagne, une femme harcèle pendant plus de trois ans son ex-amant d'une nuit. Il en découle un piratage de sa messagerie, la diffusion de faux mails, la création d'un site web proclamant qu'il est homosexuel, l'inscription à son insu sur des sites, dont une liste de discussion de prisonniers homosexuels, la diffusion de rumeurs affirmant qu'il est atteint de MST, etc… La jeune femme est condamnée pour ces faits en janvier 2005.

En France, l'ex-femme d'un magistrat et son fils sont condamnés en avril 2005 pour avoir diffusé sur Internet des photos de sa nouvelle épouse nue, et contacté divers journaux les invitant à se connecter au site web où les photos étaient exposées.

Toujours en France, en novembre 2005 : interpellation de « bloggueurs » dans les Bouches du Rhône et en Seine Saint-Denis au moment des émeutes urbaines. La provocation à une dégradation volontaire du climat social *via* le biais d'Internet est alors mise en cause (voir partie « services de répression » *supra*).

Il est à noter néanmoins une action pédagogique récente intéressante :

- pour aider les internautes à éviter les dérapages lors de la rédaction de leur blog, le forum des Droits sur Internet publie un document intitulé « *Je blogue tranquille* ».

Au Japon en novembre 2005, une jeune fille mineure est arrêtée suite à la publication dans son blog dans lequel elle raconte la dégradation progressive de l'état de santé de sa mère. Elle est soupçonnée de l'avoir empoisonnée.

Depuis quelques temps une nouvelle pratique est à l'œuvre : le « *happy slapping* ». Il s'agit de filmer une séquence avec son portable puis de la rediffuser à des connaissances par téléphone ou sur Internet. Pour l'instant seuls quelques cas sont signalés. Ce n'est pas la technologie qui est mise en cause mais l'usage qu'il en est fait. Le fait d'amplifier l'agression par sa captation filmée peut être considéré comme aggravant.

En Suisse en juin 2005, deux écoliers de 13 ans frappent un enfant et filment la séquence sur leur téléphone portable.

En France, en Novembre 2005, dans la Vienne, trois jeunes hommes sont mis en examen pour viol en réunion, captation et diffusion d'images pornographiques de mineurs. Ils auraient filmé la scène avec un téléphone portable.

En Grande Bretagne, en avril 2005, un adolescent de 14 ans se pend après avoir subi une agression filmée par ses camarades de classe.

En France, en octobre 2005, un homme est mis en examen pour provocation à la commission d'un crime par voie de presse. L'homme se serait fait passer sur des forums pour une femme dont le phantasme serait de se faire violer, pour recruter des personnes allant violer l'une de ses voisines. (Affaires en cours).

En France, en avril 2005, un homme est mis en examen à Nancy (54) pour offre de commettre un assassinat. Il aurait cherché à faire éliminer le concubin de sa maîtresse par un tueur à gages en faisant maquiller l'élimination du rival en accident.

Au Japon, une femme dépose plainte contre un homme qu'elle avait engagé sur Internet comme tueur à gages pour éliminer la femme de son amant et qui n'avait pas « exécuté » son contrat. Il est condamné pour escroquerie volontaire en décembre 2005 !

- Conclusion

Internet est un fabuleux outil de communication et de connaissances. Dans certains cas, il est devenu aussi un nouveau vecteur de violences. Les récents actes de cybercrime relevés par le panorama sont nombreux et même affolants. Ils sont l'œuvre majeure de l'être humain, il s'agit désormais d'une réalité sociale, parfois peu comprise.

L'aspect humain des souffrances engendrées chez les victimes à causes de ces offenses ou violences doit être considéré. Les atteintes, offenses, violences psychologiques sont longues à guérir, sans compter que les conséquences sont parfois irréparables. Il existe un réel besoin d'information et de prévention contre certaines de ces atteintes. Cependant, il est impossible d'en prévenir encore certaines formes…mais elles font clairement partie des nouvelles tendances de la cybercriminalité.

Annexe 4 - Liste des membres du CAP PFI Sécurité (Liste à jour 11 décembre 2006)

Monsieur Fred ARBOGAST, Computer Security Research and Response Team (CSRRT)

Monsieur Nico BINSFELD, Association des Professionnels de la Société de l'Information (APSI)

Monsieur Steve BREIER, Chambre de Commerce

Monsieur Cédric Mauny, remplaçant Monsieur Gérard HOFFMANN, Fédération des Industriels Luxembourgeois (FEDIL)

Monsieur Franck LEPREVOST, Université du Luxembourg,

Monsieur Jean-Yves KAYSER, Chambre des Métiers

Monsieur Charles DELBRASSINE, Association des Professionnels de la Société de l'Information (APSI)

Monsieur Eric DUBOIS, Centre de Recherche Public Henri Tudor

Monsieur Alexandre DULAUNOY, Computer Security Research and Response Team (CSRRT)

Monsieur David HAGEN, Commission de Surveillance du Secteur Financier (CSSF)

Monsieur Jean-Philippe HUMBERT - Centre de Recherche Public Henri Tudor

Monsieur Jean-Pol MICHEL, Centre de Recherche Public Henri Tudor

Monsieur Thomas TAMISIER, Centre de Recherche Public Gabriel Lippmann

Monsieur Pierre ZIMMER, Centre Informatique de l'Etat (CIE)

Monsieur Gérard HOFFMANN, Fédération des Industriels Luxembourgeois (FEDIL)

Monsieur Jean TRIMBOUR, Luxinnovation

Monsieur Fernand FELTZ, Centre de Recherche Public Gabriel Lippmann

Monsieur Pierre WEIMERSKIRCH, Commission Nationale pour la Protection des Données (CNPD)

Monsieur Carlo HARPES, Club de la Sécurité des Systèmes d'Information (CLUSSIL)

Monsieur François THILL, Ministère de l'Economie et du Commerce Extérieur

Monsieur Pascal STEICHEN, Ministère de l'Economie et du Commerce Extérieur

Annexe 5 – Exemples de techniques de piratage informatique

Les différentes catégories de balayages TCP/IP & la prise d'empreinte de pile TCP/IP

(Source : Etudes des Menaces IT – Rapport du projet de recherche R2SIC)

- Les différentes catégories de balayage :

A) Balayage type TCP (facilement détectable) : ce type de balayage passe par une connexion avec le port de communication cible et met en œuvre une poignée de main complète (principe du « *Three-way handshake* »), il est facile à détecter par le système cible. De nombreux outils Unix permettent ce type de fonctionnalités :

- « Strobe » (permettant d'enregistrer les bannières associées aux ports ftp://ftp.freebsd.org/pub/freebsd/ports/disfiles). Cependant, « Strobe » ne permet pas le balayage UDP.

- « Udp_scan » (balayeur UDP).

- « Netcat » permettant les balayages TCP et UDP (option –u).

- « Nmap » (Network mapper) permettant les balayages TCP et UDP.

- « Nessus » qui constitue le plus populaire des logiciels de type scanner réseaux (www.nessus.org).

« Nessus » permet d'auditer à distance un réseau donné et déterminer si quelqu'un (ou quelque chose tel un ver) peut le pénétrer ou en abuser illégalement.

Note : Nessus ne prend pas de configuration type par défaut (notamment indexation port de communication), il envisage tous les scénarios possibles.

B) Balayage type UDP : cette technique consiste à envoyer un paquet de type UDP vers le port cible. Si le port cible répond par un message « port ICMP »

inaccessible, cela signifie que le port est fermé. A l'inverse, si aucun message n'est reçu, il s'avère que le port est ouvert. Ce balayage peut s'avérer long et pas forcément stable en terme de résultat.

- La prise d'empreinte de pile :

Les failles de sécurité sont souvent propres à un système d'exploitation (OS) particulier. C'est la raison pour laquelle l'identification de l'OS est de première importance pour le pirate.

La technique d'empreinte de pile exploite les différences entre les implémentations de cette pile dans les différents OS. Les éditeurs constituent leur pile TCP/IP selon leur interprétation des directives RFC (« *Request for Comments* »). L'idée est d'envoyer des paquets TCP spécifiques à la cible et d'observer la réponse. En fonction de ces différences, en les recherchant, la prise d'empreinte de pile vise à déterminer le système d'exploitation de la machine cible. La réponse permettra de cerner un groupe d'OS voire un seul OS.

En l'occurrence, l'outil « Nmap » (*Network mapper*), permettant les balayages TCP et UDP, utilise des tactiques différentes pour découvrir l'OS de la cible distante. « Nmap » parvient grâce à elle à récupérer des informations qu'il compare avec sa propre base de données, sans cesse réactualisée. Voici ces six techniques.

1 - « Test FIN » - Il consiste à envoyer un paquet FIN à un port ouvert. La RFC793 stipule que le comportement adéquat est de ne pas répondre à un tel paquet. Cependant, de nombreuses implémentations de pile TCP/IP renvoient un « RST ». C'est le cas notamment de MS Windows.

2 - « Echantillonnage TCP ISN (Initial Sequence Number) » - On tente de déduire des choses intéressantes du numéro de séquence initial choisi par l'implémentation TCP distante quand elle répond à une demande de connexion.

3 - « Fenêtre TCP initiale » - On peut facilement tirer des conclusions de la taille de la fenêtre TCP choisie initialement par l'implémentation TCP distante, car celle-ci est plus ou moins constante suivant les types d'OS. Il s'agit d'un test utile car certains OS

sont identifiables par cette seule tactique. Exemples : AIX est le seul OS utilisant la valeur 0x3F25, OpenBSD et FreeBSD utilisent Ox402E.

4 - « Citation de message ICMP » - Les RFC spécifient qu'un message d'erreur ICMP doit toujours citer une partie du message ICMP à l'origine de l'erreur. Pour un message *ICMP « port unreachable »*, presque toutes les implémentations renvoient l'entête IP + 8 octets. Par exemple, Solaris renvoie un peu plus et Linux encore un peu plus. Nmap parvient donc à les reconnaître, même s'ils n'ont pas de ports à l'écoute.

5 - « Intégrité des messages d'erreurs ICMP » - Comme signalé juste au-dessus, les machines doivent joindre une partie du message original quand elles retournent un message d'erreur ICMP. Certaines machines utilisent les en-têtes IP comme espace de travail et les altèrent donc. *FreeBSD* et *OpenBSD* par exemple, altèrent le champ « ID » envoyé. Alors que le *checksum* doit changer à cause de la modification du champ TTL (Time To Live), certains OS (AIX, FreeBSD,...) renvoient un *checksum* inconsistant ou nul.

Note **:** « Nmap » fait 9 tests différents sur les erreurs ICMP.

6 - « Options TCP » - Elles fournissent des informations très précieuses. En effet, toutes les machines ne les implémentent pas. De fait, celles qui les implémentent le signalent. Quand le pirate envoie une requête avec une option mise à une cible, celle-ci placera ladite option dans la réponse uniquement si elle supporte cette option.

On peut positionner beaucoup d'options dans un seul paquet pour tout tester en une seule fois. En effet, quand le pirate reçoit la réponse, il regarde quelles options sont retournées et donc supportées.

Note : Il existe également des outils de découverte automatisée qui permettent de cartographier graphiquement des réseaux ciblés avant attaque. Par exemple l'outil Cheops : http://www.marko.net/cheops.

Annexe 6 – Questionnaire sondage (Version 1)

« Mondes de la cyberdélinquance et image sociale du pirate informatique »

Merci de prendre le temps de répondre à ces quelques questions. Elles s'inscrivent dans le cadre d'un travail en cours de Doctorat en « sciences de l'information et de la communication » qui vise à déterminer ***les mécanismes de construction de l'image sociale du pirate informatique*** *(…à travers les réseaux d'acteurs de la cyberdélinquance).*

Ces questions visent dans un premier temps à mesurer l'opinion publique vis-à-vis des pirates informatiques.

1) Qui êtes vous ?

- Un pirate ?
- Un citoyen ?
- Un institutionnel (secteur public, banque…) ?
- Un expert sécurité ?
- Un journaliste ?
- Autres : précisez.

2) Comment vous représentez-vous le pirate informatique ?

- Personnage sympathique ?
- Personnage dangereux ?
- Personnage génial ?
- Ne sais pas.

3) Associez-vous au pirate informatique un degré de dangerosité :

- Faible ?
- Moyen ?
- Important ?
- Ne sais pas.

4) Qui vous permet principalement de fournir cette représentation du pirate informatique ?

- Les médias ?

- Les pirates informatiques ?
- Les experts en SSIC ?
- Autres : précisez ?
- Sans commentaire.

5) Trouvez-vous les pirates informatiques :

- Innovants ?
- Déviants ?
- Délinquants ?
- Ne sais pas.

6) Trouvez-vous l'image du pirate informatique, plutôt :

- Positive ?
- Neutre ?
- Négative ?
- Ne sais pas.

7) Pensez-vous que cette image est largement dominante au cœur de la société :

- Oui ?
- Non ?
- Ne sais pas.

8) Les actions des pirates informatiques sont-elles :

- Répréhensibles de manière criminelle ?
- Répréhensibles de manière délictuelle ?
- Répréhensibles de manière contraventionnel ?
- Non répréhensibles ?
- Ne sais pas.

9) Comment définiriez-vous la cyberdélinquance ?

- Le moyen d'utiliser un médium informatique pour un crime ou délit conventionnel ?
- Le moyen d'attaquer un médium informatique en tant que cible ?
- Les deux sont possibles ?

10) Un *hacker :* c'est un pirate qui vise à détruire ou voler des données disponibles sur un site victime ?

- Vrai
- Faux

11) Un *cracker* : c'est un pirate qui recherche des failles de sécurité afin de progresser au niveau technologique ?

- Vrai
- Faux

12) Les pirates informatiques forment-ils une véritable communauté au niveau international ?

- Vrai
- Faux

13) Connaissez-vous cette classification des acteurs de la cyberdélinquance :

- «*Script kiddies*» : jeunes pirates informatiques de bas niveau
- «*Crackers*» : pirates qui attaquent un site pour destruction ou vol de données
- «*Hackers*» : pirates qui visent à découvrir des failles de sécurité pour en comprendre le fonctionnement

Cette classification vous semble t-elle :

- Juste ?
- Fausse ?
- Restrictive ? Pourquoi ?

14) Le dernier rapport « *e-crime watch survey* » du *Computer Emergency and Response Team CC* (CERT CC) faisait état de pertes estimées, relative à la cyberdélinquance, et relevées par cet organisme, à :

- 111 millions $?
- 222 millions $?
- 666 millions $?

***
*

Contact : jean-philippe.humbert@tudor.lu

Annexe 7 – Questionnaire sondage (Version 2)

Merci de prendre le temps de répondre à ces quelques questions. Elles s'inscrivent dans le cadre d'un travail en cours de Doctorat en « sciences de l'information et de la communication » qui vise à déterminer ***les mécanismes de construction de l'image sociale du pirate informatique*** *(…à travers les réseaux d'acteurs de la cyberdélinquance).*

Ces questions visent dans un premier temps à mesurer l'opinion publique vis-à-vis des pirates informatiques.

Note : *David L. Carter[284], professeur au département de justice pénale de l'Université de l'Etat du Michigan, établit une définition de la cyber-criminalité en fonction de l'utilisation faite du médium informatique.*
Soit l'instrument informatique est utilisé par le délinquant comme outil d'un crime conventionnel (escroquerie, menaces…etc), soit l'ordinateur est la cible visée par le délinquant (vol ou destructions de données…etc).
Nous considèrerons ***ce délinquant comme définissant le pirate informatique****.*

1) Dans quel pays résidez-vous ?

- Précisez :

2) Qui êtes vous ?

- Un citoyen
- Un employé du secteur privé
- Un employé du secteur public
- Un expert sécurité
- Un journaliste
- Un pirate
- Autres : précisez

3) Pour vous la cyberdélinquance est :

- Un acte peu grave ?
- Un délit sans plus ?
- Un délit grave ?

[284] *Computer Crime Categories : How Techno-Criminals Operate* (Carter, 1992).

4) A vos yeux quels qualificatifs décrivent le mieux le pirate informatique (plusieurs réponses sont possibles) ?

- Un personnage compétent en informatique ?
- Un personnage potentiellement dangereux ?
- Un personnage moyennement dangereux ?
- Un personnage très dangereux ?

5) Pour vous quels sont les risques du pirate informatique au niveau économique ?

- Aucun préjudice ?
- Préjudice financier ?
- Manque de confiance en Internet ?
- Des pertes graves ?

6) Cette image que vous vous faites du pirate informatique a été nourrie par :

- Les médias ?
- Les pirates informatiques ?
- Les experts en SSIC ?
- Autres : précisez ?
- Sans commentaire

7) Considérez-vous que l'action des pirates informatiques est :

- Une innovation pour l'informatique ?
- Un acte de délinquance ?
- Un acte malveillant ?
- Un acte criminel ?
- Ne sais pas

8) Trouvez-vous l'image du pirate informatique, plutôt :

- Positive ?
- Neutre ?
- Négative ?
- Ne sais pas

9) Pensez-vous que cette image est largement dominante au cœur de la société :

- Oui ?
- Non ?
- Ne sais pas

10) Les actions des pirates informatiques doivent-elles être sanctionnées par une peine :

- De prison ?
- Une amende ?
- Des travaux d'intérêts généraux ?
- Rien ?

11) Les actions des pirates informatiques doivent-elles être sanctionnées par :

- Un juge ?
- Un cyberpolicier ?
- Une inscription au casier judiciaire ?

12) Un *hacker* est un pirate qui vise à détruire ou voler des données disponibles sur un site victime ?

- Vrai
- Faux

13) Un *hacker* est un pirate qui recherche des failles de sécurité afin de progresser au niveau technologique ?

- Vrai
- Faux

14) Un *cracker* est un pirate qui recherche des failles de sécurité afin de progresser au niveau technologique ?

- Vrai
- Faux

15) Un *cracker* est un pirate qui vise à détruire ou voler des données disponibles sur un site victime ?

- Vrai
- Faux

16) Les pirates informatiques forment-ils une véritable communauté au niveau international ?

- Vrai
- Faux

17) Connaissez-vous cette classification des acteurs de la cyberdélinquance ?

- «*Script kiddies*» : jeunes pirates informatiques de bas niveau
- «*Crackers*» : pirates qui attaquent un site pour destruction ou vol de données
- «*Hackers*» : pirates qui visent à découvrir des failles de sécurité pour en comprendre le fonctionnement

Cette classification vous semble t-elle :

- Juste ?
- Fausse ?
- Restrictive ? Pourquoi ?

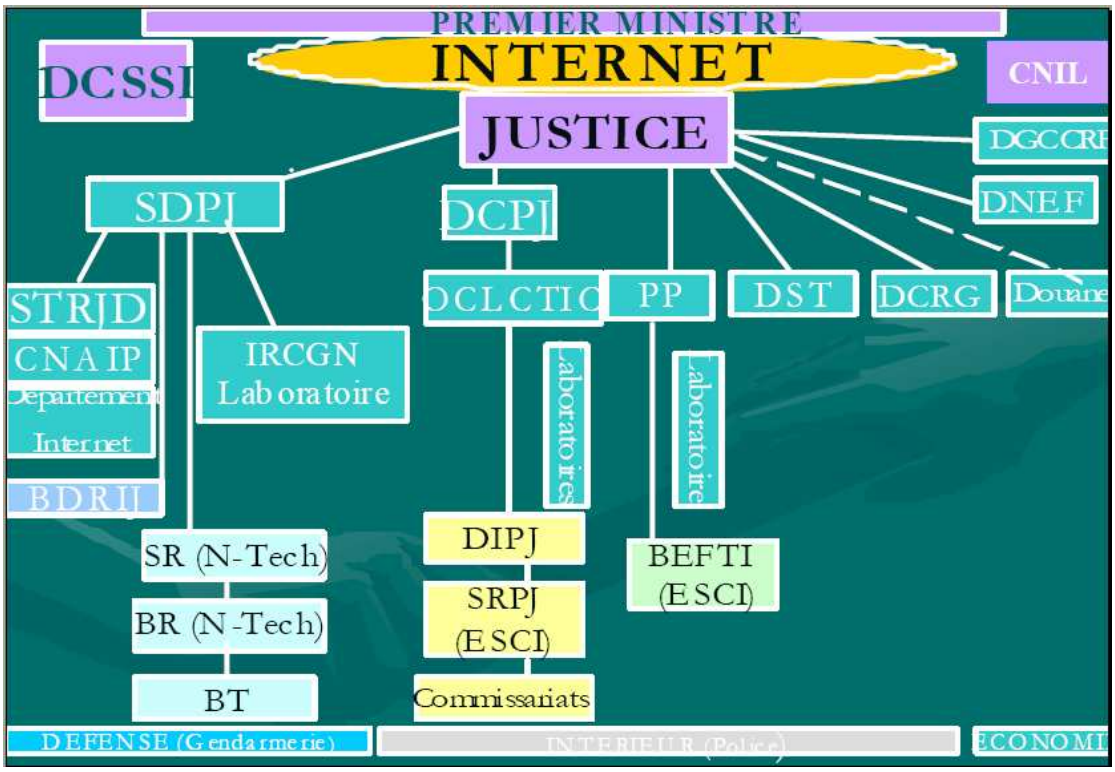
18) Le dernier rapport « *e-crime watch survey* » du *Computer Emergency and Response Team CC* (CERT CC) faisait état de pertes estimées, relative à la cyberdélinquance, et relevées par cet organisme, à (plus proche de) :

- 5000 $?
- 50 000 $?
- 500 000 $?
- 150 millions $?
- 500 millions $?
- 1 milliard $?
- Plusieurs milliards $?

***
*

Contact : jean-philippe.humbert@tudor.lu

Annexe 8 – Roadmap des acteurs de la répression informatique en France



- Figure 29. Roadmap des acteurs de la repression en France

Annexe 9 - Corpus d'articles de la presse écrite française (1995-2003)

1) Baroux D., 1995, « Systèmes d'Information : la sécurité, une urgence », *La Tribune Desfossés, p. 15.*
2) Carbonnier J., 1994, *Sociologie juridique*, Paris, Quadrige/PUF.
3) Guisnel J., 1995, « Pirates en treillis », *Libération, Cahier multimédia*.
4) Eudes Y., 1995, « L'odysée des pirates dans la jungle Internet », *Le Monde diplomatique*.
5) Non signé, 1995, « Pirates en vue ! », *Joystick*, pp. 34-40.
6) Guisnel J., 1995, « Pirates de guerre », *Libération*.
7) Inciyan E., 1995, « Le site Internet de Polytechnique a été fermé à la suite d'intrusions », *Le Monde*.
8) Alberganti M., 1995, « Le jeu dangereux du piratage informatique », *Le Monde*.
9) Tavoillot P-A., 1996, « Les espions investissent le cyberespace », *La Tribune Desfossé*, pp. 16-21.
10) Vidamment G., 1996, « Sécurité sur Internet : la grande désillusion », *Le Quotidien de Paris*, p. 8.
11) Doré C., 1998, « Des pirates français poursuivis par les Etats-Unis », *Le Figaro*.
12) Latrive F., 1998, « Analyser, pirate et technohéros des ados », *Libération*.
13) Jullien E., 1998, « Internet, c'est pire ! », *L'Evènement du Jeudi*, p. 41.
14) Non signé, 1998, « Les menaces de la cyber-criminalité », *Le Figaro*.
15) Berrivier A., 1998, « Les pirates à l'abordage d'Internet », *Sciences & Vie*, pp. 122-125.
16) Non signé, 1998, « Les interdits du Net », Net@scope, pp. 20-21.
17) Lindivat A., 1999, « Comment on vous espionne sur Internet », *l'Ordinateur Individuel*, pp. 88-92.
18) Pisani F., 1999, « Penser la cyberguerre », *Le Monde diplomatique*.
19) Dufresne D., 1999, « Jospin annonce une loi pour débrider l'Internet », *Libération, Cahier multimédia*.
20) Cassel D., Koerner B., Houston J., 2000, « INTERNET contre l'ordre établi », *Courrier International*, pp. 21-29.

21) Non signé, 2000, « Des criminels professionnels s'infiltrent dans la communauté des *hackers* et se servent des petits jeunes pour faire leur sale boulot », *Hackerz Voice*.
22) Quéau P., 2001, « Nous sommes tous des cyber-criminels », *Le Monde diplomatique*.
23) Riché P., 2001, « Big Brother est arrivé », *Libération*, pp. 1-3.
24) Fozzi, 2001, « HACKER LEGAL », *Le Manuel de Hackerz Voice*.
25) Hes, 2001, «Le 2600 français, version revival, s'est réuni en douce à Paris », *Hackerz Voice*.
26) Brotha, 2002, « Devenir Hacker », *Hackerz Voice*, pp. 2-3.
27) Non signé, 2002, « Matignon Piraté », *Zataz Magazine*, pp. 14-19.
28) Non signé, 2002, « Comment devenir un hacker », *Pirat'z*, pp. 8-14.
29) Non signé, 2002, « Comment Internet a failli s'écrouler… », *Hackmania*, p. 3.

Annexe 10 – Listes des relevés « Google » à partir des mots-clés « cybercrime » et « pirate informatique » (janvier-juin 2006)

1) « En 2005, les bots étaient à la mode », par Ange-Gabriel, le 30/01/2006, Information Week
2) Par Guy hervier, le 15 mars 2006, étude sur les DSI (responsables informatiques), source inconnue
3) Interview : Jean-Paul NEY, par Cali Rise, le 1/02/2006
4) « L'ISIQ s'attaque à la cybercriminalité », par Lise Fournier, le 01/02/2006, source inconnue
5) Texte sans titre, non signé, source inconnue ; thème : condamnation par le Tribunal correctionnel de Bastia de « Dany Corsica », auteur de plusieurs sites de téléchargement illicites
6) texte sans titre sur l'inculpation par la justice américaine d'un groupe de pirates nommé RISCISO, pour vol massif de logiciels ; par Bruno Cormier, le 02/02/2006, source inconnue
7) « La Bourse russe attaquée », par Benoît Parriaud, le 06/02/2006, News Scientist
8) « Un pirate condamné à deux ans de prison pour cyberattaques », par Jean-Charles Condo, le 07/02/2006, BRANCHEZ-VOUS
9) « Après le phishing, les cyber-criminels attaquent avec l'e-gène », par José Diz
10) « Ces cyber crimes qui nous menacent », le 06/02/2006, par la Rédaction, source inconnue
11) « 19 pirates d'une « warez team » ont été arrêtés aux USA », le 06/02/2006, par la Rédaction, source inconnue
12) « Deux membres d'un réseau britannique de falsification de cartes bancaires devant la justice », le 08/02/2006, source inconnue
13) « Sécurité. Caricatures : plusieurs centaines de sites danois tombés sous le feu des pirates », Atelier groupe BNP Paribas – 09/02/2006
14) « Le Président égyptien s'entretient avec le Directeur du FBI de la coopération contre le terrorisme », le 09/02/2006, source inconnue

15) « Happy new year Microsoft », par azeus – Mohammed Slimani, le 28/12/2005, Cyber-Tech
16) « L'empoisonnement du DNS, ou l'attaque informatique totale : le « *pharming* » plus redoutable que le « phishing », article publié dans Mag Securs n° 11, déc. 2005 – janv./fevr. 2006
17) « La grande offensive », Société – lutte contre la criminalité, le 12/02/2006, non signé, source inconnue
18) « Monde arabe : conférence à Beyrouth sur la cybercriminalité, le 21/02/2006, article non signé, source inconnue
19) « Cybercriminalité : des textes de loi en cours d'élaboration », par Nassima Oulebsir, texte non daté, source inconnue
20) Texte sans titre sur le thème des déclarations du directeur du FBI concernant la cybercriminalité ; par Florian, le 22/02/2006, source inconnue
21) « Le cyberpunk, une contre-culture des années 90 », mars 2006, Hacktivist
22) « Etude du Groupe Lexsi sur les réseaux de cybercriminalité », mars 2006, texte non signé, source inconnue
23) « Les cyberpharmacies dans la ligne de mire », mars 2006, texte non signé, source inconnue
24) « Téléchargement. Les pirates sous peine d'amende », par Pauline Lecuit, le 11/03/2006, source inconnue
25) « Propos de Pascal Clément, Garde des Sceaux, Ministre de la Justice à l'issue de la réunion avec son homologue américain, Alberto Gonzales, Secrétaire à la Justice, attorney general des Etats-Unis », le 3/03/2006, l'Express, Chancellerie
26) « Piratage informatique : aperçu, motivations des pirates, quelques conseils pour se protéger », le 4/03/2006, article non signé, source inconnue + forum de l'article
27) « Lexsi : les ravages du phishing dans les institutions bancaires », mars 2006, article non signé, source inconnue
28) « 15$ pour fabriquer son spyware », par Jean-Sébastien Zanchi, le 27/03/2006, source : Sophos
29) Texte sans titre sur le thème d'une nouvelle loi allemande sur le téléchargement ; par Bruno Cormier, le 27/03/2006, source de l'information : timesonline

30) « La cybercriminalité : droit, intervention et profiling », Isabelle Tisserand – le Cercle de la Sécurité, mars 2006
31) « Le CLUSIF publie une étude sur les virus informatiques », le 28/03/2006, texte non signé, source inconnue
32) « Veille internationale. Piratage : l'Europe sort l'artillerie lourde », Atelier groupe BNP Paribas, le 28/03/2006
33) « Clearstream : le corbeau et le général. Le domicile de Philippe Rondot, ancien de la DST et de la DGSE, a été perquisitionné hier », par Renaud, le 29/03/2006, Libération – Société (www.liberation.fr)
34) « Contrôle parental : la cyberguerre est déclarée ! », non signé, non daté, source inconnue
35) « L'Algérie prépare une loi contre la cybercriminalité », synthèse de Ahlem, d'après le Quotidien d'Oran, le 30/03/2006
36) « Des infos belges permettent de coincer un *hacker* », non signé, non daté, source inconnue
37) Texte sans titre sur les effets nuisibles de Googlebot, le 02/04/2006, non signé, source inconnue
38) « Des étudiants condamnés pour hacking », par Maître Isabelle Pottier, le 31/03/2006, Micro Hebdo
39) « Yahoo pourrait être poursuivie pour divulgation d'infos personnelles », par Simon-Pierre Goulet, le 31/03/2006, www.branchez-vous.com
40) « Des experts internationaux l'ont plaidé hier. Pour une loi spécifique sur la cybercriminalité en Algérie », par Nadia Mellal, le 05/04/2006, rubrique Actualité, source inconnue
41) « Un *hacker* arrêté en australie grâce à la Federal Computer Unit belge », la 30/03/2006, texte non signé, source inconnue
42) « Le phishing devient de plus en plus subtil », par Marc Olanié, le 05/04/2006, (www.reseaux-telecoms.net)
43) « Un *hacker* australien arrêté grâce à la police belge » (troisième texte sur le même thème), non signé, non daté, source inconnue

44) « Jugé pour avoir piraté le blog de son ex-copine », le 05/04/2006, Reuters (Marseille)
45) « Pédocriminalité sur Internet : action de la police valaisanne », le 05/04/2006, non signé, source inconnue
46) « Le phishing en France, peu de victimes mais une menace grandissante », par Arnaud Devillard, le 10/04/2006, 01Net
47) « Escroquerie par phishing ciblant les clients de la banque LCL », le 21/03/2006, Phishing folder
48) « Escroquerie par phishing ciblant les clients de la banque Société générale », le 20/03/2006, Phishing folder
49) « Escroquerie par phishing ciblant les clients de la banque BNP Paribas », le 19/03/2006, Phishing folder
50) « Faux site Windows Update malicieux », le 13/03/2006, Phishing folder
51) « Escroquerie par phishing ciblant les clients de la banque LCL », le 07/03/2006, Phishing folder
52) « Escroquerie par phishing ciblant les clients de la société Visa », le 24/0/2006, Phishing folder
53) « Escroquerie par phishing ciblant les clients de la banque LCL », le 01/02/2006, Phishing folder
54) « Le pirate informatique Gary McKinnon sera-t-il extradé ? Aller simple pour Guantanamo », par Marc Rees, le 14/04/2006, source inconnue
55) Rapport hebdomadaire de Panda Software qui résume les événements les plus marquants dans le secteur des intrusions et des virus informatiques, non daté, www.pandasoftware.com/pandalabs.asp et www.pandasoftware.fr
56) Texte sans titre sur le thème des pirates informatiques ayant dérobé des données mal protégées sur des sites bancaires britanniques, non signé, non daté, www.echosdunet.net/news
57) « Un réseau de criminalité transnationale opère en Russie (responsable) », le 20/04/2006, RIA Novosti – Moscou
58) « Un *hacker* de San Diego risque 10 ans », le 21/04/2006, Silicon.fr

59) « Une enquête de Websense : les employés menacent le plus la sécurité des données et les dirigeants en sont responsables », avril 2006

60) Texte sans titre sur un pirate anglais, Briton Gary McKinnon, qui s'est introduit sur le serveur du Pentagone, www.pcinpact.com/actu/news

61) « La cybercriminalité : un fléau en pleine expansion », par Nicolet, le 30/04/2006, LCN

62) « Bienvenue à Hack Académie », par Arnaud Dimberton, le 05/05/2006, Silicon.fr

63) « Les USA dénoncent le piratage de jeu video par les islamistes », par David Morgan, le 05/05/2006, Reuters

64) « Envahisseurs yankees », non daté, non signé, source inconnue

65) « Cinq ans de prison pour le maître de PC zombies », par Julie de Meslon, le 10/05/2006, source inconnue

66) Texte sans titre sur le thème de la deuxième semaine nationale de la sécurité informatique, non signé, non daté, source inconnue

67) « Réponse à un lecteur : « *hacker* » et Jean-François Revel », non signé, le 06/06/2006, rubrique Bloc-Notes, www.dedefensa.org

68) « La cybercriminalité de mieux en mieux organisée », par Mathieu Pagura, www.metrofrance.com

Annexe 11 – Veille documentaire du domaine de la réponse sur incidents

- Carnegie Mellon University, 2002, *CSIRT Services*; Stelvio bv, The Netherlands; PRESECURE Consulting GmbH, Germany.

- ENISA, 2006, *A step by step approach on how to set up a CSIRT* (Deliverable WP2006/5.1 (CERT – D1/D2).

- ENISA, 2006, *ENISA ad hoc Working Group on Cert Cooperation and Support,* Final Report and deliverables.

- M. J. West-Brown, D.Stikvoort, Klaus-Peter K., 2003, *Handbook for Computer SecurityIncident Response Teams (CSIRTs),* Carnegie Mellon University - CMU/SEI-2003-HB-002.

- Information Security Team DePaul University, 2002, *A framework for Incident Reponse* [https://infosec.depaul.edu/].

- P. Steichen, 2006, *A global Approach to network and Information Security* – Intervention / CERTs, Université Paul Verlaine de Metz – France.

- T. Grance, K. Kent, B. Kim., 2004, *Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology (NIST - Technology Administration – U.S. Departement of Commerce), Special Publication (SP) 800-61.

- E. Guttman, 1998, *Request for Comments (RFC): 2350,* Network Working Group N. Brownlee, The University of Auckland, BCP: 21, Category: Best Current Practice Sun Microsystems, *Expectations for Computer Security Incident Response.*

- T. R. Osborne, 2001, *Building an Incident Response Program To Suit Your Business*, GIAC Security Essentials (v 1.2e), SANS Institute.

- B. Kaskina, 2005, *Collaboration of Security Incident Response Team – Update*, TF-CSIRT.

- M. Borodkin, 2001, *Computer Incident Response Team,* GIAC Certification Version, SANS Institute.

- K. P. Kossakowski, J. Allen, C. Alberts, 1999, *Responding to intrusions,* Carnegie Mellon University Software Engineering Institute, CMU/SEI-SIM-006.
- M. Miqueu, O. Castant, 2004, 16ème conférence, FIRST, Etats-Unis.
- D. Crochemore, 2006, *Présentation du CERT-Administration France*, CERT-A.
- C. Dubois, 2006, *Réagir aux incidents de sécurité informatique*, CERT-A.
- D. Crochemore, 2006, *La réaction sur incidents de sécurité informatique*, CERT-A.
- J. Patzakis, 2003, *New Incident Response Best Pratices,* Guidance Software.
- R. Cummings, J. Lowry, 2003, *Guidance Software Computer Forensic 101 & Incident Response.*
- M. K., Prosise C., 2004, « *Incident Response – Investing Computer Crime* », Etats-Unis.
- Pipkin D., 2000, *Sécurité des systèmes d'information,* Paris, Campus Press.
- ENISA Inventory, http://www.enisa.eu/ENISA%CERT/index.htm

Annexe 12 – « Panorama Cybercrime Luxembourg – Partie I » (2005-2006)

« *Le cybercrime est désormais un véritable état de fait. L'ensemble des nations a tôt fait de réagir en mettant en place des contre-mesures, (le plus souvent d'envergure), vis-à-vis de cette menace. De nombreux pays se sont sérieusement organisés dès le développement exponentiel d'Internet, notamment lorsque les offres de connexion sont devenues possibles vers le citoyen. Ainsi, la France a, par exemple, dès 1994, mis en place des services de police spécialisés pour non seulement lutter contre la cybercriminalité, mais aussi pour sensibiliser les entreprises à la nécessité de se protéger contre ces nouvelles menaces à l'encontre de l'information et de la communication publiquement mises en réseau. Très tôt, le basculement de l'économie vers le numérique, associé à sa mise en ligne vers des réseaux publics, rencontra les inquiétudes étatiques, les gouvernements craignant concrètement une menace pour ce modèle de développement économique via les réseaux, devant plutôt globalement être soutenu (Initiative e-Europe de l'Union Européenne), et non soumis aux diverses tentatives possibles de dégradations/détériorations/destructions. La multiplication des affaires de piratages informatiques (vol d'informations, espionnage d'informations, « défiguration » de sites web, mise hors service de sites,…) a donc considérablement renforcé les initiatives de protection des pouvoirs publics.*

La première loi concernant directement la criminalité informatique et la répression de la cyberdélinquance a été adoptée en 1984 aux Etats-Unis (Comprehensive Crime Control Act), et rapidement amendée par le Computer Fraud and Abuse Act de 1986 qui criminalise six types d'accès frauduleux aux systèmes informatiques, en fonction de la finalité de l'opération d'intrusion réalisée.

En France, les enjeux de la sécurité informatique ont été pris en compte dans la loi Godfrain du 05 janvier 1988, reprise dans le Nouveau Code pénal sous les articles 323-1 et suivants. En cette matière l'arsenal juridique est formé de trois délits distincts, visant les atteintes aux systèmes et les atteintes aux données.

Au Luxembourg, la loi du 15 juillet 1993 détermine les infractions pénales informatiques, s'inspirant fortement de la loi Godfrain (France) :

article 509.1 : Accès frauduleux ou maintien non autorisé dans un système de traitement ou de transmission de données.

- article 509.2 : Entrave intentionnelle au fonctionnement d'un système de traitement de données

- article 509.3 : Introduction intentionnelle, directe ou indirecte, de données dans un système de traitement de données, suppression ou modification de données, suppression ou modification des modes de traitement ou de transmission de données.

Pour ces trois infractions les peines encourues varient de 2 mois à 3 ans d'emprisonnement et de 500 à 25 000 Euros d'amende.

- Qu'est-ce que la cybercriminalité ? (http://www.cases.lu)

La cybercriminalité se définit communément, comme toute action illicite, visant l'intégrité d'un site informatique déterminé, ou bien menée à l'aide d'un outil informatique. Cette définition se décline selon l'utilisation faite du médium informatique. En effet, soit ce dernier est utilisé par le délinquant comme outil d'un délit ou d'un crime conventionnel (escroquerie, menaces…), soit l'ordinateur est la cible même visée par le délinquant (vol, utilisation frauduleuse, ou encore destructions de données,…). »

- Qui est concerné ?

Tous les citoyens, PME et administrations, connectés *via* leur ordinateur sur Internet, peuvent être victimes d'un, voire de plusieurs cas de piratages informatiques.

Les caractéristiques peuvent être variées et correspondre soit à un délit, soit à un crime conventionnel, soit en utilisant l'ordinateur comme relais, ou soit en prenant véritablement l'ordinateur pour cible. Ainsi, le simple fait de connecter sa machine à Internet suffit pour ouvrir une porte d'accès potentielle à toutes ces menaces. Actuellement, les statistiques établissent un court délai d'environ quinze minutes de connexion, avant de subir au moins une tentative de connexions illicites (de type scan) ou tout du moins non sollicitées.

- Comment cela fonctionne-t-il ?

La cybercriminalité se divise en actions utilisant le médium informatique (attaques « conventionnelles ») ou bien s'attaquant à l'intégrité même du médium (attaques « technologiques »).

· Attaques dites « conventionnelles » :

Ces attaques utilisent les réseaux d'information et de communication en tant que support, il s'agit de profiter de ce type d'innovation technologique pour en tirer profit de manière illicite. Le plus souvent, le but est de profiter de la crédulité des personnes victimes pour obtenir des informations confidentielles et les utiliser ensuite de manière illégale. Exemple : c'est le cas des escroqueries dites « à la nigérienne ou encore SCAM 4-1-9 (du nom de l'article pénal prévoyant cette escroquerie au Nigéria) ». Il s'agit d'un mail proposant de manière urgente le dépôt d'une somme importante sur votre compte bancaire moyennant une rétribution non négligeable « pour service rendu » ! Le but est, bien entendu, de récupérer vos données bancaires pour un usage illégal. C'est également le cas des diverses tentatives maquillées, d'obtention de données bancaires, *via* la technique dénommée « *phishing* ».

Il existe toutes sortes d'infractions classées dans cette catégorie, et ce type de menaces est en constante augmentation ; nous pouvons notamment citer :

les extorsions de fond, la fraude à la carte de crédit, les menaces répréhensibles diverses, de type « vengeance », la fraude commerciale, les abus de confiance et escroqueries diverses, les détournements de mineurs…etc.

Il s'agit véritablement de l'ensemble des crimes et délits « traditionnels » se transposant *via* les réseaux numériques d'information et de communication. Les motivations quant à ces attaques sont essentiellement de type cupides (le but est la recherche d'un gain, qu'il soit financier ou matériel) ou bien encore immorales, « malsaines » et maladives (pédophilie, réseaux de prostitution, racisme, révisionnisme, etc…).

Attaques dites « technologiques » :

Ce type d'attaques apparaît non négligeable en regard de leur évolution. Elles concernent essentiellement celles qui visent l'intégrité du médium informatique. A ce titre, elles sont nombreuses et corrélatives au nombre des vulnérabilités à exploiter.

Elles se déclinent, principalement, ainsi :

- usurpation d'adresses I.P, - dépôt de programmes espions (spywares),

- dépôt de programmes pirates (adwares, rootkits, sniffers,…),

- intrusions,

- détériorations diverses,

- destruction de sites,

- vol d'informations,

- saturations de sites,

- rebond à partir de sites informatiques victimes, etc.

Les motivations diffèrent quant à l'attaque numérique du médium, elles peuvent être :

- stratégiques (visant des informations sensibles classifiées), - idéologiques (transformations de pensées prédominantes ou de courant d'idées en actes illicites), - terroristes (toute action visant à déstabiliser l'ordre établi), - cupide (le but est la recherche d'un gain, qu'il soit financier ou matériel), - ludique (agissements par amusement ou loisir), - vengeur (réaction à une frustration quelconque).

Souvent, plusieurs de ces motivations peuvent être combinées lors d'une attaque de ce type. Elles visent soit la confidentialité, soit l'intégrité mais aussi la disponibilité d'un système informatique (voire une combinaison des trois).

Le pirate informatique use généralement de procédures diverses pour attaquer une ressource visée. Les pratiques les plus souvent rencontrées sont les suivantes :

- la prise d'empreinte : généralement, avant d'attaquer une cible particulière, le pirate procède à un relevé de toute information pouvant mener à une cartographie (photographie détaillée) de l'organisation ou de l'individu qu'il vise,

- le balayage systématique de réseau : correspond à la recherche d'informations au sens large (image consistant à « clencher » chaque porte pour déterminer celles qui peuvent s'ouvrir). Les pirates testent des systèmes cibles pour vérifier s'ils sont actifs, et déterminer quels ports de communications peuvent être en veille,

- le recensement : après la prise d'empreinte et le balayage de réseau, le pirate va ensuite chercher à identifier des comptes d'utilisateurs valides ou des ressources partagées

mal protégées. Ces opérations sont appelées les opérations de « recensement ». Il s'agit véritablement de la phase précédent celle plus active de pénétration et d'intrusion.

Généralement, lorsqu'un nom d'utilisateur (ou de ressource partagée) est recensé, le délai est court avant que l'intrus ne parvienne à deviner le mot de passe correspondant ou à identifier une faille associée au protocole de partage de ressources,

- le fichier piégé : le pirate peut tenter une attaque en envoyant un e-mail piégé, contenant un « cheval de Troie » (voir fiche CASES « Cheval de Troie ») masqué dans un programme de type lambda, qui pourra lui permettre si le destinataire l'active, de prendre par la suite, à distance, la main sur le micro-ordinateur victime,

- le « social-engineering » : dans ce cas précis la victime n'est pas confrontée à une manipulation technique mais directement à un pirate qui se fait passer pour une personne identifiée afin d'avoir accès à des informations tel qu'un mot de passe par exemple. Ce scénario est pratique courante ; les pirates agissent souvent par pression psychologique et/ou invoquent l'urgence pour obtenir rapidement des renseignements sur la victime.

- Pourquoi se protéger ?

La cyberdélinquance constitue une menace considérable sur Internet, les pertes peuvent être véritablement conséquentes, pouvant entraîner des pertes financières directes, de réputation ou encore de temps, que l'on soit un particulier, une entreprise ou bien une administration. Elle affiche des visages multiples et ne connaît pas de frontières. Ce caractère générique et instable exige une nécessaire prise de conscience ainsi que la mise en place de contre-mesures adéquates.

- Comment se protéger ?

La protection passe par une nécessaire prise de conscience du phénomène et par le choix et la mise en place de contre-mesures adéquates :

- penser au phénomène de la cyberdélinquance dès que l'on se connecte, mais surtout dès qu'un élément particulier non prévu survient,
- mettre en place des réflexes de sécurité de base tels que :

- ne pas ouvrir des e-mails en provenance d'inconnus et ne pas exécuter de pièces-jointes associées,
- mettre à jour son OS, son anti-virus et son firewall,
- ne pas surfer sur des sites « trop » underground,
- se méfier des inconnus, etc,
- effectuer une veille quant aux menaces courantes,
- faire un usage raisonné et adapté d'Internet,
- ne pas faire « trop facilement confiance au premier venu »…

Autant de règles simples qui pourront vous permettre d'éviter de devenir trop aisément un catalyseur de la « menaçante » cyberdélinquance.

- Qui sont les cyberdélinquants ? (http://www.cases.lu)

Note : Pour décrire ces mêmes acteurs sociaux, est souvent également utilisé, et de manière très générale, voire abusive, le terme « cybercriminels », nous préfèrerons celui de cyberdélinquants, plus global.

Les actes de piratage informatique, au cœur des réseaux d'information et de la communication, sont l'œuvre d'acteurs sociaux, communément dénommés « cyberdélinquants », qu'il convient de connaître et de comprendre, notamment afin d'appréhender correctement les caractéristiques de ce type de menaces,

- Les cyberdélinquants

Les cyberdélinquants se définissent communément, soit comme acteurs commettant un délit ou crime conventionnel à l'aide d'un outil informatique, soit comme acteurs, visant l'intégrité d'un site informatique déterminé. Nous trouvons dans cette première catégorie des cyberdélinquants de type :

- cyber-escrocs, - cyber-fraudeurs, - cyber-voleurs, - cyber-abuseurs, - cyber-déviants - cyber-pédophiles…etc. Quant à la seconde catégorie, les acteurs s'attaquant au médium informatique, ils jouissent depuis l'avènement d'Internet, d'un véritable succès médiatique conduisant à une véritable catégorisation, qui, en terme de recherche, demeure critiquable, mais qui en terme de compréhension permet d'appréhender les

formes possibles de menaces effectives. Les cyberdélinquants se caractérisent par des capacités techniques certaines et des motivations diverses, tout en provenant d'horizons sociaux multiples. Afin d'en faciliter la compréhension, il est d'usage de procéder à leur classification. Ainsi, sont principalement catégorisés au cœur de la cyberdélinquance, trois communautés bien distinctes, aux relations tendues, à savoir les *hackers*, les *crackers* et les *script-kiddies*.

De plus, si ces différentes communautés ont bien pour point commun l'illégalité reconnue dans laquelle elles agissent ; leurs motivations respectives, quant à elles, divergent fortement.

- Les *hackers*

Le terme de *hacker* est souvent utilisé à mauvais escient par la presse écrite pour couvrir l'ensemble des pirates informatiques. Cet amalgame contribue à propager une image fantasmée et alarmiste des menaces informatiques.
Situation fortement paradoxale, quand on sait que les *hackers* constituent certainement ; la communauté la moins nuisible au sein de l'univers encore très méconnu de la cyberdélinquance. En réalité, si tout *hacker* peut être « étiqueté » en tant que cyberdélinquant, tous les cyberdélinquants ne sont pas des *hackers*.

Les *hackers* ou « chapeaux blancs » sont certainement les plus connus, mais aussi les plus incompris des cyberdélinquants. Ils se démarquent des *crackers* et des *script-kiddies* par leur sens de l'éthique. Contrairement à ces derniers, ils n'attaquent pas leurs cibles, mais se contentent d'enfreindre la sécurité de leurs systèmes pour en souligner les failles. Il s'agit pour le *hacker*, à travers des moyens, illicites il est vrai, de relever un « challenge » technologique tout en agissant pour le bien des organisations attaquées, puisqu'il permet l'amélioration de la sécurité du système d'information concerné.

Hautement qualifiés et compétents, les *hackers* sont quasiment indétectables. Leurs actions sont motivées par une idéologie commune, à savoir, la conviction que la propriété intellectuelle doit appartenir à tous ceux qui en ont la compréhension et que toute tentative de légiférer en matière de cyberespace doit être combattue. La communauté *hacker* partage une culture commune rassemblant des programmeurs expérimentés, des spécialistes réseaux et des passionnés des technologies de

l'information et de la communication, au sens large du terme. L'histoire de cette communauté date de plusieurs décennies, remontant aux premiers développements du concept d'ordinateur, et aux premières expériences du réseau ARPAnet.

Ce sont les propres membres de cette communauté qui se sont dénommés *hackers* (du verbe to hack, littéralement « hacher » : pour mieux comprendre, mieux développer, et par extension mieux sécuriser). Ils sont à l'origine du développement d'Internet et ont, entre autre, également permis le développement des systèmes d'exploitation tels que Unix, et récemment Linux. Il convient d'associer ces acteurs sociaux au concept de bâtisseurs plutôt que de destructeurs, dernier terme d'importance qui différencie, respectivement et définitivement les *hackers* des *crackers*.

Note : Eric S. Raymond, célèbre auteur de « *Jargon File* » et de « *New hacker's dictionnary* », permet de définir très finement la terminologie relative au *hacker*, avec le respect de l'ensemble de la communauté concernée. Un célèbre article « *How to become a hacker* » permet de mieux comprendre ce contexte. Pour aller plus loin : http://www.catb.org/~esr/

- Les *crackers*

Le *cracker* ou « chapeau noir », pénètre, au contraire du *hacker*, les systèmes informatiques avec l'intention de nuire. Il peut arriver que le *cracker* attaque pour des raisons ludiques, mais en général, il essaye de tirer un gain de ses exactions, comme le fait de nuire à un concurrent, de s'enrichir personnellement ou d'acquérir des données confidentielles. Bien souvent, il s'agit de véritables criminels, fonctionnant dans des réseaux mafieux, pour leur propre compte ou le compte d'autrui. Souvent très compétents techniquement, ils peuvent égaler les compétences des *hackers* ; cependant, ils en représentent véritablement le côté sombre, puisqu'ils ne font pas profiter une victime de leur savoir et que celle-ci ne peut en profiter pour améliorer ses paramètres de sécurité. Bien au contraire, leur but est de maximiser cette connaissance à leur propre profit.

Aucune éthique n'est présente dans la réalisation des actes des *crackers*, au contraire des *hackers*. Souvent, la presse fait état des actes de *crackers* : il s'agit généralement de piratages de serveurs web (transformation de pages), de saturation de sites, de transformations de données, de rebond pour pirater d'autres sites, etc. Mais, chaque

action révèle toujours une volonté de nuire à une victime potentielle. En terme de cracking, d'autres acteurs sociaux sont catégorisés comme étant particulièrement dangereux : les « enfants du *script* » ou encore « *script kiddies* ».

- Les *script kiddies*

Les *scripts kiddies* forment le bas de gamme du piratage informatique. Si les deux communautés précédentes se focalisent sur des cibles spécifiques, les *script-kiddies* eux, lancent leurs attaques de manière totalement aléatoire, en utilisant des listes de commandes groupées dans un *script*, d'où leur nom.

Ce type d'attaque ne demande pas un très haut niveau de connaissance informatique ; c'est pourquoi le *script kiddy* est souvent un adolescent voire parfois un enfant. Ce dernier utilise des logiciels « prêt à l'emploi », ne maîtrisant nullement les conséquences de l'action entreprise, ni même son fonctionnement. Le comportement des scripts kiddies est totalement irresponsable, pouvant atteindre n'importe quelle ressource informatique, y compris les ressources informatiques de la compagnie où travaillent leurs parents, par exemple. Dans l'ensemble, ces communautés ne se mélangent pas. Les *hackers* ont très peu de considération pour les *crackers* (qu'ils considèrent comme de véritables pirates informatiques) et inversement. Quant aux *script-kiddies*, ils font partie d'un monde totalement à part, ne bénéficiant d'aucune considération.

A partir de cet état des lieux, la possibilité pour une commune ou une PME de se faire attaquer par un *hacker* apparaît pratiquement nulle. Cette communauté ne comporterait par ailleurs que quelques centaines de membres au niveau mondial ; et n'est attirée que par les sites hautement sécurisés, représentant un véritable défi technologique. Si les *crackers* sont plus nombreux, ces derniers se concentrent généralement sur les grandes compagnies, n'ayant aucun intérêt à viser une cible de moindre importance. Cependant, cette menace générique n'est pas nulle.

En fait, la masse nuisible, qu'une petite entité ou que le citoyen est susceptible de rencontrer très régulièrement, (car ils se comptent par centaines de milliers et attaquent de manière complètement aléatoire), est constituée par les *script-kiddies* (et surtout les malfrats qui les manipulent). Cependant, leurs attaques étant courantes et connues, il est relativement facile de les prévenir ; en appliquant les patchs de sécurité relatifs aux

systèmes d'exploitation utilisés, en surveillant les accès aux réseaux et en mettant en place un plan de réponse sur incidents. Ainsi organisée, la sécurité devient une garantie de gestion surveillée des attaques potentielles connues. En quelque sorte, c'est le respect du minimum requis des règles en terme de sécurité des systèmes d'information et de la communication.

- Comment sensibiliser ?

Les pouvoirs publics tentent difficilement de « réguler » les menaces *via* le cadre de la répression, mais aussi idéalement *via* celui de la sensibilisation. L'organisation de type privée peut simplement « sonder » la menace associée à son contexte, *via* notamment, par exemple, la mise en place de leurres réseaux de type Honeypots, ou bien encore en analysant les traces de logs de différents mécanismes de sécurité réseau, et de leur corrélation.

Ainsi, même si l'information devient perceptible pour une entreprise privée, il demeure toujours impossible d'agir directement sur cette dernière, il est ainsi hors de question de répondre à un acte cybercriminel en ré-attaquant cet agent menaçant ; c'est une règle fondamentale de droit, mais surtout d'éthique.

Dans ce cas : deux possibilités s'offrent alors à la société :

- réaliser une médiation en contactant le(s) agent(s) menaçant(s) détecté(s) pour tenter de stopper leurs attaques, voire de vérifier s'ils ne sont pas eux-mêmes des victimes de type « rebond » ou interdire une connexion en provenance de cette cible. – ou enfin, exercer une répression en déposant plainte contre l'agent menaçant (sans être véritablement efficace en terme de résultat, cette démarche permet tout de même de montrer son engagement contre tout type de permissivité cybercriminelle).

Toute externe qu'elle soit, la menace doit surtout aussi être perçue en interne ; pour ce faire, une troisième voie associée à la gestion des risques de sécurité, devient fondamentale, à savoir la sensibilisation aux menaces adaptée à la politique sécurité de l'organisation. En effet, la prise en compte du phénomène en interne est majeure si l'on veut éviter de créer des points d'accroches aux agents menaçants. Cette conscience doit être parallèle à celle développée lors de l'analyse de risque de sécurité vis-à-vis des bases de connaissance des menaces. Parallèlement au « sondage » technique vu *supra*, et en

ligne avec la politique de sécurité, le RSSI se doit de sonder également les représentations mentales des employés quant aux menaces. Ainsi, il peut percevoir les absences de connaissance flagrante et dangereuse pouvant nuire à l'organisation, car traduisant notamment une incompréhension de la politique de sécurité en place. Pour ce faire, des questionnaires adaptés peuvent être proposés, aux fins de mesure, reprenant les images associées aux menaces et véhiculées par les médias, les experts sécurité et les pirates informatiques. Ces types de questionnaires (par exemple : http://jph.cases-cc.org) peuvent être déroulés durant une séance de sensibilisation à la sécurité des systèmes d'information, et en fonction des réponses, créer le débat, apporter des réponses concrètes et objectives permettant de faire le lien avec la politique de sécurité en cours et sa justification. Le RSSI pourra aussi bénéficier utilement de l'aide didactique fournie par la structure CASES (http://www.cases.lu).

Annexe 13 – Bilan individuel de recherche : Jean-Philippe Humbert

- Bilan individuel 2004-2007
  Nom : Humbert
  Prénom : Jean-Philippe
  Année de première inscription en thèse : 2004

1. Articles dans des revues avec comité de lecture (ACL)

Internationales

- 2006 : Béatrix Barafort, Jean-Philippe Humbert, Sébastien Poggi, « *Process Reference Model & Security* » - SPICE 2006 (Software Process Improvement and Capability dEtermination), Grand-Duché de Luxembourg.

- 2007 : Claire Lombard, Jean-Philippe Humbert : « *L'apport du e-learning dans la e-strategie luxembourgeoise pour la sensibilisation aux risques liés à la sécurité des systèmes d'information* » - iLearning Forum Conference – eStratégies et Territoires – Paris.

Nationales

- 2006 : Jean-Philippe Humbert, Nicolas Mayer : « *La gestion des risques pour les systèmes d'information* » - MISC Magazine N°24 – Avril-Mai 2006. France

- 2006 : Jean-Philippe Humbert, Nicolas Mayer : « *La méthode de gestion des Risques de sécurité EBIOS* »- MISC Magazine N°27 – Septembre-Octobre 2006. France

- 2007 : Jean-Philippe Humbert, Nicolas Mayer : « *ISO 2700x : une famille de normes pour la gouvernance sécurité*» - MISC Magazine N°29 – Mars-Avril 2007. France

2. Articles dans des revues sans comité de lecture (SCL)

- 2006 : Francine Herrmann, Jean-Philippe Humbert, Nicolas Mayer « *Gestion de la sécurité : les défis* », Mag SECURS, 12, Juin-Juil.-Août 2006, pp. 18-23, France.

- 2007 : Nicolas Mayer, Jean-Philippe Humbert – « *Certification ISO/IEC 27001* », Journal AGEFI – Dossier spécial sécurité, janvier 2007, Luxembourg.

- 2007 : Jean-Philippe Humbert – « *La Plate-forme d'Innovation Sécurité du Centre de Recherche Public Henri Tudor – G-D de Luxembourg*) », Journal AGEFI – Dossier spécial sécurité, janvier 2007, Luxembourg.

3. Conférences invitées (INV)

4. Communications avec actes (ACT)

Internationales

- 2004 (31/03/2004), Jean-Philippe Humbert - « *Luxembourg e-Commerce Certified – Guide Sécurité des Systèmes d'Information* », Conférence, Luxembourg, Centre de Recherche Public Henri Tudor – Conférence dans le cadre du réseau des professionnels de l'IT (Information Technology) SPIRAL, du Grand-Duché de Luxembourg.

- 2004 (07/12/2004), Jean-Philippe Humbert - « *ISO JTC1/SC27 & CNLSI* », Conférence « Organisation internationale de standardisation ISO & Sécurité de

l'Information et de la Communication », Luxembourg, Centre de Recherche Public Henri Tudor – Conférence dans le cadre du réseau des professionnels de l'IT (Information Technology) SPIRAL, du Grand-Duché de Luxembourg.

- 2005 (24/03/2005), Jean-Philippe Humbert – « *Cyberdélinquance et classification de ses acteurs sociaux* », Conférence « La Sécurité informatique, risques techniques et enjeux juridiques », Luxembourg, Chambre des Métiers.

- 2005 (08/06/2005), Jean-Philippe Humbert – « *Cartographie des référentiels de risques et sécurité des systèmes d'information et de la communication* », Conférence « Du bon usage des méthodes dans l'analyse des risques », Luxembourg, Centre de Recherche Public Henri Tudor – Journée SPIRAL-CLUSSIL.

- 2005 (07/10/2005), Jean-Philippe Humbert – « *Menaces et systèmes d'information* », Conférence, Banque Centrale du Luxembourg, Luxembourg.

- 2005 (29/11/2005), Jean-Philippe Humbert - « *Comité d'accompagnement Plate-Forme d'Innovation Sécurité – Enquêtes, Normalisation et Certification SSIC – Quels choix pour Luxembourg ?* », Luxembourg, Centre de Recherche Public Henri Tudor.

- 2005 (02/12/2005 – Pour les membres présents de l'Université de Genève), Jean-Philippe Humbert - « *Panorama des Référentiels de la SSIC* », Luxembourg, Centre de Recherche Public Henri Tudor.

- 2005 (08/12/2005), Jean-Philippe Humbert, Nicolas Mayer – « *Panorama des référentiels d'analyses et de gestion des risques* » & « *Le Mini-Guide Sécurité - Luxembourg e-Commerce Certified* », Conférence, Luxembourg, Centre de Recherche Public Henri Tudor – Conférence dans le cadre du réseau des

professionnels de l'IT (Information Technology) SPIRAL, du Grand-Duché de Luxembourg.

- 2006 (15/02/2006), Jean-Philippe Humbert - « *Normalisation Qualité des Systèmes d'Information (SC7 Luxembourg) & Sécurité des Systèmes d'Information et de la Communication (SC27 Luxembourg)* », Centre de Recherche Public Henri Tudor – Réunion de Normalisation ISO.

- 2006 (07/03/2006), Jean-Philippe Humbert - « *Comité d'accompagnement Plate-Forme d'Innovation Sécurité – Enquêtes, Normalisation et Certification SSIC – Les choix pour Luxembourg* », Luxembourg, Centre de Recherche Public Henri Tudor.

- 2006 (23/05/2006), Jean-Philippe Humbert - « *CNLSI – Comité de Normalisation Luxembourgeois pour la Société de l'Information* », Conférence, Luxembourg, Centre de Recherche Public Henri Tudor – Conférence dans le cadre du réseau des professionnels de l'IT (Information Technology) SPIRAL, du Grand-Duché de Luxembourg.

- 2006 (26/09/2006), Jean-Philippe Humbert - « *S'il-te-plaît…Dessine-moi un pirate informatique* », Conférence, Luxembourg, Centre de Recherche Public Henri Tudor – Conférence dans le cadre du réseau des professionnels de l'IT (Information Technology) SPIRAL, du Grand-Duché de Luxembourg.

- 2006 : (10/11/2006) : Jean-Philippe Humbert - « *Standards et SSII – Le cas luxembourgeois* » in « *Les normes, éléments moteurs de l'Economie de la Connaissance* » - Colloque « En route vers Lisbonne », Centre de Recherche Public Henri Tudor – Luxembourg.

- 2006 : (17/11/2006) : Jean-Philippe Humbert - « *Qualité et Sécurité des Systèmes d'Information : l'intégration par la normalisation* » in « Semaine de la Qualité »,

Chambre des Métiers (Mouvement Luxembourgeois pour la qualité), Luxembourg.

- 2006 (11/12/2006), Jean-Philippe Humbert - « *Comité d'accompagnement Plate-Forme d'Innovation Sécurité – Prospective Métiers SSIC – Présentation Résultats Etude de faisabilité de la mise en place d'un Observatoire des Menaces IT au G-D de Luxembourg*», Luxembourg, Centre de Recherche Public Henri Tudor.

- 2007 (06/02/2007), Jean-Philippe Humbert - « *Le champ de la Sécurité de l'information* » - Centre de veille technologique in « *La sécurité économique et la protection du patrimoine de l'entreprise* » - Centre de Recherche Public Henri Tudor – Luxembourg.

- 2007 (26/03/2007), Jean-Philippe Humbert - « *La Normalisation pour la Sécurité de l'Information*» - dans le cadre du « *Internet Security Day »* – Chambre de Commerce – Luxembourg.

Nationales

5. Communications sans actes (COM)

- 2004 (16/10/2004), Jean-Philippe Humbert – « *Qui sont les pirates d'aujourd'hui ? Eclairage sur les pirates informatiques réseaux* », Table-ronde « Savoir(s) en commun : rencontres universités – société », 67 - Strasbourg, Universités Robert Schuman, Marc Bloch et Louis Pasteur.

- 2005 (20/05/2005), Jean-Philippe Humbert – « *Plan Directeur National de la Sécurité des Réseaux et Structure de sécurité des systèmes d'Information CASES »,* Conférence groupe de travail « Sécurité des Systèmes d'Information », MEDEF, 75 - Paris.

- 2005 (28/06/2005), Jean-Philippe Humbert - « *Comité d'accompagnement Plate-Forme d'Innovation Sécurité – Définition des objectifs métiers et technologies SSIC nationaux luxembourgeois* », Luxembourg, Centre de Recherche Public Henri Tudor.

- 2005 (19/09/2005), Jean-Philippe Humbert - « *Comité d'accompagnement Plate-Forme d'Innovation Sécurité – Choix des objectifs métiers et technologies SSIC nationaux luxembourgeois* », Luxembourg, Centre de Recherche Public Henri Tudor.

- 2006 (02/06/2006), Jean-Philippe Humbert - « *Comité d'accompagnement Plate-Forme d'Innovation Sécurité – Présentation des rapports de veille « DRM » & « Forensic Analysis » - Planification Etude de faisabilité de la mise en place d'un Observatoire Cybercrime au G-D de Luxembourg*», Luxembourg, Centre de Recherche Public Henri Tudor.

- 2006 (21/09/2006), Jean-Philippe Humbert - « *Comité d'accompagnement Plate-Forme d'Innovation Sécurité – Prospective Métiers SSIC – Les choix pour Luxembourg* », Luxembourg, Centre de Recherche Public Henri Tudor.

- 2006 (12/10/2006 – pour les membres présents du CETIC), Jean-Philippe Humbert - « *Plate-Forme d'Innovation Sécurité – Objectifs – organisation – projets de recherche – produits et services*», Luxembourg, Centre de Recherche Public Henri Tudor.

- 2007 (23/01/2007), François Thill, Jean-Philippe Humbert – « *CASES – Une initiative luxembourgeoise pour réduire la fracture numérique dans le domaine de la sécurité de l'information* », Conférence groupe de travail « Sécurité des Systèmes d'Information », DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information), 75 - Paris.

6. Ouvrages scientifiques (ou chapitres) (OS)

7. Ouvrages de vulgarisation (ou chapitres) (OV)

8. Directions d'ouvrages (DO)

9. Autres publications (AP)

10. Autres activités internationales (AI)

- Membre du comité scientifique/lecture conférences « hack.lu » (19-21 octobre 2006). (Review de 19 articles).

- Membre du comité de Programme conférence «Eurosec » (23 au 25 mai 2007). (Review de 30 articles – 2 propositions de communications annexes retenues).

11. Information et culture scientifique et technique

- 2003-2004 : 40 heures de cours pour Master SSIC – Université Paul Verlaine de Metz.

- 2004-2005 : 36 heures de cours pour Master SSIC – Université Paul Verlaine de Metz.

- 2005-2006 : 40 heures de cours pour Master SSIC – Université Paul Verlaine de Metz. Responsable Scientifique module « Audit de sécurité et évaluation des risques ».

- 2005-2006 : 3 heures de cours pour Master MSSI – Université de Luxembourg - Responsable Scientifique module « Politique de sécurité ».

- 2006-2007 : 48 heures de cours pour Master SSIC – Université Paul Verlaine de Metz. Responsable Scientifique module « Méthodologie avancée de la sécurité ».

- 2006-2007 : 18 heures de cours pour Master MSSI – Université de Luxembourg - Responsable Scientifique module « Politique de sécurité ».

12. Valorisation : contrats de recherche

- 2004, Jean-Philippe Humbert - « *Rapport d'étude sur les menaces des systèmes d'information et de la communication pour le Ministère de l'Economie et du Commerce Extérieur - Luxembourg* », Luxembourg, Projet de Recherche R2SIC (Recherche en Sécurité des Systèmes d'Information et de la Communication - Centre de Recherche Public Henri Tudor).

- 2005, Jean-Philippe Humbert – Nicolas Mayer – Sébastien Poggi - « *Meilleures pratiques pour la gestion des risques SSI – Utilisation de la méthode EBIOS® dans le cadre d'une démarche BS 7799* », document édité par le Bureau conseil de la DCSSI.

- 2006, Jean-Philippe Humbert – Irina Vassileva – (sous la responsabilité de M. Arnaud Mercier) - «*Vers la connaissance de la cybercriminalité – Etat de l'art* », Rapport de Recherche INHES « *Espaces publics et sécurité – Thème : la cybercriminalité* » (131 pages).

- 2006, Jean-Philippe Humbert – Sébastien Poggi – Pascal Steichen – (sous la responsabilité de M. François Thill) *« Analyse des Risques de SSIC du Ministère de l'Economie et du Commerce Extérieur (selon la méthode EBIOS)*».

- 2006, Jean-Philippe Humbert - « *Panorama Cybercrime du G-D de Luxembourg* » (Partie I), structure CASES - Luxembourg.

- 2006, Jean-Philippe Humbert – François Thill – Pascal Steichen « *Etude de faisabilité de la mise en place d'un Observatoire des menaces IT au G-D de Luxembourg* » (86 pages).

Jean-Philippe HUMBERT

Les mondes de la cyberdélinquance et images sociales du pirate informatique

La cyberdélinquance constitue un phénomène indissociable du monde numérique, depuis les premiers *hackers* recherchant la compréhension des mécanismes innovants de communication, jusqu'aux pirates informatiques majoritairement voués désormais à la criminalité. L'évolution et l'état actuel de ce phénomène déterminent, dès lors, un véritable questionnement sur la réalité sociale du pirate informatique responsable des faits de cyberdélinquance. En effet, comment l'appréhender et en atteindre la connaissance ? Afin d'en dégager les clés de compréhension, ces interrogations sont abordées par l'étude qualitative de cet acteur social responsable des actes de malveillance informatique. Cette recherche porte spécifiquement sur l'identification des processus de construction des significations sociales du pirate informatique. Nous répondrons principalement à cette question : peut-on parler, non pas d'une image sociale normalisée, mais plutôt de l'existence de plusieurs images sociales du pirate informatique? Afin d'en permettre une étude compréhensive, l'objet sera décliné *via* le cadre de référence du concept de « monde social ». L'analyse porte en premier lieu sur la représentation sociale de la cyberdélinquance, en déterminant son image construite. Un second moment est consacré à l'approche communicationnelle du contexte social de la cyberdélinquance, déclinant l'image médiatique dominante quant aux significations du pirate informatique. Enfin, afin d'anticiper la représentation sociale en construction du pirate informatique, une dernière partie se consacrera à une approche intégrée possible des images sociales du pirate informatique, *via* différents mondes sociaux de la cyberdélinquance. Ces trois clés de compréhension visent à mieux comprendre le phénomène de la cyberdélinquance et ses acteurs principaux, en construction socialement, à travers une dimension interculturelle.

Mots-clés : Cyberdélinquance, représentation sociale, risque, Internet, pirate, informatique, *hackers*, *crackers*, sécurité.

The cyberdelinquency's worlds and the social images of the computer pirate

The cyberdelinquency constitutes an inseparable phenomenon from the numerical world, since the first hackers seeking comprehension of the innovating mechanisms of communication, to the recent computer pirates being posed as true criminals. The evolution and the current state of this phenomenon determine a true questioning on the social reality of the computer pirate responsible for the facts of cyberdelinquency. Indeed how to arrest it and attain knowledge? To clear the keys of it of understanding, these questionings are approached by the qualitative study of this social actor responsible for acts of computer spitefulness. This research carries specifically the identification of the building processes of the social signification of the computer pirate. We'll answer mainly this question: can we speak, not of a normalized social picture, but rather the existence of several social pictures? To allow an understanding study, the object will be declined *via* the reference frame of the concept of "social world". The analysis concerns firstly the social perception of cyberdelinquency, by determining its constructed picture. A second instant is dedicated to the communicative approach of this social context of the cyberdelinquency, declining the media picture predominant as for the signification of the computer pirate. Finally, to anticipate social perception in building of the computer pirate, a last party dedicates itself to a possible integrated approach of social pictures of the computer pirate, *via* different social worlds of the cyberdelinquency. These three keys of understanding aim at determine the phenomenon of cyberdelinquency better and his main actors, in building socially, across an intercultural dimension.

Keywords : Cyberdelinquency, social representation, risk, Internet, pirate, computer science, hackers, crackers, security.