Université de Montréal

Kevin Mitnick : contre-iconographie d'un *superhacker*

par
Jean-Sébastien Coutu

Département de Communication
Faculté des Arts et Sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de maîtrise
en communication

Août 2001

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :
Kevin Mitnick : contre-iconographie d'un *superhacker*

présenté par :
Jean-Sébastien Coutu

a été évalué par un jury composé des personnes suivantes :

Thierry Bardini
directeur de recherche

Line Grenier
membre du jury

Brian Mussami
membre du jury

Résumé

Ce mémoire questionne la tolérance de la presse vis-à-vis des symptômes qui supposent qu'un pouvoir surnaturel soit à l'origine de certains accomplissements *hacker*. L'auteur retrace les faits saillants de l'histoire du phénomène *hacker* et théorise le *hack* en repérant et démontant certains mythes ayant cour dans la presse. Il étudie la démarche professionnelle du journalisme et étudie les mécanismes impliqués dans la prise de consistance de l'icône populaire *hacker* en repérant ses forces et ses faiblesses. Il compare ensuite les couvertures de trois reporters (John Markoff, Jonathan Littman et Jeff Goodell) qui ont enquêté sur les activités du célèbre *hacktiviste* californien Kevin Mitnick et examine l'impact de leur adhésion aux hypothèses paranormales dans l'échafaudage de leurs conclusions (iconographies). En reprenant ces couvertures mais les dépouillant de toutes leurs considérations pour le surnaturel, ce mémoire aboutit à une contre-icône *hacker* plus vraisemblable de Kevin Mitnick que celles dépeintes par les trois reporters.

Liste des mots clés

Iconographie
Icône populaire
Mythe
Symbole
Hacker
Script Kiddie
Hacking
Hack
Hacktivisme
Journalisme

Abstract

This thesis raises the question of the media's ability to tolerate those symptoms which suppose that a supernatural power is at the origin of certain *hacker* exploits. The author reviews the highlights of the history of the *hacker* phenomenon and theorizes on the *hack* by identifying and dismantling certain myths circulating in the media. The author examines the professional approach taken by journalists and studies the mechanisms involved in understanding the popular icon of the *hacker* by identifying his strengths and weaknesses. The author proceeds to compare the news coverage provided by three reporters (John Markoff, Jonathan Littman and Jeff Goodell) who inquired into the activities of the famous Californian *hacktivist* Kevin Mitnick and examines the impact of their support of paranormal hypotheses in the construction of their conclusions (iconographies). Upon reviewing the news coverage but stripping them of all their supernatural considerations, the present thesis leads to a more probable counter-icon *hacker* description of Kevin Mitnick than that depicted by the three reporters.

Keywords

Iconography
Popular icon
Myth
Symbol
Hacker
Script Kiddie
Hacking
Hack
Hacktivism
Journalism

TABLE DES MATIÈRES

Avant-propos

J'ai connu une fin d'adolescence agitée. Fasciné par l'informatique, je l'étais aussi par l'excitant univers du piratage qui prit dans ma vie la forme d'intrusions heureusement restées impunies. Je reconnais d'ailleurs que cela aurait pu m'attirer quelques sérieux désagréments avec la justice de l'époque. Comprenez bien : il était fort excitant de s'introduire de s'en prendre impunément à des institutions maudites qui venait pourrir de leur unique présence les territoires les plus prometteurs de mon cyberespace. Étudiant sans le sou, je menais une vie d'enfermé et je consacrais l'essentiel de mon temps à pitonner le clavier de mon micro-ordinateur. J'étais véritablement fada d'informatique. En 1995, le personnage *hacker* représentait à mes yeux le summum de l'exotisme. Je le pressentais comme le grand seigneur d'une civilisation numérique en pleine ascension. A dix-neuf ans, bien sûr, mon idée de cette civilisation était encore imprécise. Celle des *hackers* aussi. Mais si les *hackers* de mon imagination restaient obstinément invisibles, je gardais la foi. Il existait sûrement des *superhackers* dont la puissance ferait bientôt trembler la planète *Cyber*. Mon intuition se révéla fondée. A quelques encablures de réseau s'agitaient des gens dont j'allais bientôt lire les noms dans la presse. Mitnick, Poulsen, Tannenbaum, Helsingius, Abene et plusieurs autres encore devenus les icônes populaires d'un phénomène qui commençait véritablement à capter l'attention des médias.

Je découvris entre-temps que je n'avais rien d'un *hacker* bien redoutable. J'étais seulement un *script kiddie* parmi tant d'autres, c'est-à-dire un petit malin dont l'essentiel de l'activité consistait utiliser des logiciels d'intrusion programmés par d'autres. Le temps passa quelque peu et j'en profitai pour m'assagir. Mais si je restais très épris de la pratique informatique, je n'imaginais pas que tout cela allait bientôt m'inspirer une carrière, encore moins un mémoire.

En 1998, j'avais vingt-trois ans et je décrochais un baccalauréat en communication à l'Université de Montréal. Je décidais ensuite de poursuivre dans le même domaine en m'inscrivant au programme de maîtrise. J'obtenais la même année deux places de chroniqueur (*hacker* et *techno-païen*) dans le

magazine d'informatique *Québec Micro*. Le rédacteur en chef me confia la tâche de suivre l'actualité *hacker* et de la commenter. Ce que je fis avec le plus grand sérieux. Avec le recul, je me rends compte que j'étais vraisemblablement l'unique chroniqueur *hacker* en ville, toutes publications confondues.

En octobre 2000, je quittais *Québec Micro* pour démarrer E-MedHosting avec deux partenaires d'affaires. Le projet : fabriquer des logiciels de pointe pour l'industrie pharmaceutique. Nous visions le monde du *e-cme* (formation médicale continue en ligne) et celui du *e-learning* (processus d'accréditation en ligne). L'entreprise semble réussir au-delà de toute espérance puisque nous comptons aujourd'hui plusieurs gros clients dont Shire Biochem, GlaxoSmithKline, Roche Diagnostic, Global Medic et même la Faculté de Médecine de l'UdM qui vient de prendre entente avec nous pour tester un projet pilote. Dans l'aventure, six employés enthousiastes sont aussi venus se greffer à nous, dont deux excellents programmeurs.

Mon expérience de E-MedHosting m'a cependant permis de connaître un autre point de vue : celui de l'hébergeur. Puisque tous nos logiciels fonctionnent en ligne, nous subissons régulièrement les attaques de *hackers*. Loin de me contrarier, cela a précisé mon intérêt pour le phénomène.

Ce mémoire est donc l'aboutissement d'un cheminement inhabituel qui m'a amené à examiner plusieurs fois le phénomène *hacker* de l'intérieur.

Introduction

> Temps restant avant la libération complète et définitive de Kevin Mitnick : 0 année, 07 mois, 25 jours, 20 heures, 56 minutes, 39 secondes, 38 secondes, 37 secondes... (www.freekevin.com)

Sur le frontispice du site web *Free Kevin*, un sablier égrène les secondes depuis bientôt sept ans, date de la dernière incarcération du *superhacker* Kevin Mitnick pour « délit de curiosité informatique » (Richard, 1999). Noyau dur d'une résistance à l'américaine qui dénonce le mauvais traitement fait à un mythe vivant, ce site collectionne et affiche l'ensemble des nouvelles les plus révoltantes susceptibles d'entacher la crédibilité d'un département américain de la Justice qui persécute Mitnick par intermittence depuis maintenant vingt ans. La crédibilité aussi de certains journalistes qui auraient contribué à diaboliser un *hacker* aux intentions innocentes qui, la cour elle-même le reconnut, ne profita jamais de ses aptitudes surnaturelles pour s'enrichir personnellement. Les auteurs y passent à tabac un certain John Markoff, un journaliste du *New York Times*, pour sa complicité avec l'accusation. Aussi, pour sa notoriété et sa richesse acquises sur le dos d'une mystérieuse créature : Kevin Mitnick, le premier « *dark side hacker* » ou le côté obscur de la force (Rosenberg, 1995).

A l'origine de l'affaire, des pertes financières évaluées à quatre-vingts millions de dollars en dommages « collatéraux ». En effet, Mitnick aurait déjoué certains des dispositifs de sécurité les plus sophistiqués, obligeant les victimes à colmater les brèches en y affectant des ressources humaines extraordinaires. Motorola, Fujitsu, Nokia, Sun, Novell et Nec se présentèrent à la barre pour témoigner du génie maléfique d'un *superhacker* fou qui les avait foudroyés pour le seul bon plaisir de hacker leur système. Ni revendication, ni fanfaronnade. Que la foudre bête et brutale (Christensen, 1999).

Les peuples de l'Antiquité craignaient leurs dieux en partie à cause des phénomènes climatiques dont ils les croyaient responsables. Cette croyance établie, les Grecs, par exemple, s'exerçaient à reconnaître les humeurs de

certains dieux. Que ces humeurs aient été sages ou non importait peu puisque de toute façon les hommes étaient bien incapables de s'élever devant ces caprices (Fontaine, 2001). Ne leur restait plus qu'à manifester une soumission perspicace à travers toutes sortes de rituels en espérant que ceux-ci sauraient attendrir les dieux. C'est ainsi qu'on soupçonna un jour les velléités terrestres de Poséidon après que les foudres de celui-ci eurent dévasté l'Attique (Grèce). La tempête fut si violente qu'un puits d'eau douce tourna à l'eau salée. Ce puits existe encore aujourd'hui dans les ruines d'Athènes. La déesse Athéna, dont c'était le fief qu'on attaquait, réagit en faisant pousser un énorme olivier, le premier de la région, qui narguait le fameux puits de son ombre méprisante. Les Athéniens tergiversèrent longtemps sur le sens à donner à tout ça et après de vaines querelles concédèrent finalement leur allégeance à Athéna (Coquelle, 2000).

Poséidon Dieu de la Mer armé d'un trident ou Kevin Mitnick Dieu du Cyberespace armé d'un micro-ordinateur, même foi, même exaltation mystique. Car ce qui retient surtout l'attention dans l'affaire Mitnick, c'est justement l'absence du moindre doute par rapport aux pouvoirs surnaturels dont le jeune *hacker* serait « vraisemblablement » possédé (Markoff, 1996). La justice d'abord imposa au jeune homme une incarcération plutôt musclée. Chevilles menottées, dépossédé de toute forme de culture informatique, il fut même envoyé au trou durant deux semaines pour avoir été surpris en train de collectionner des boîtes de thon. Invité à s'expliquer, le directeur de la prison confia aux journalistes qu'il avait reçu l'instruction de ne prendre aucune chance avec cet individu doté de pouvoirs fantastiques. En effet, le directeur songea que Mitnick aurait pu utiliser ses boîtes de thon pour se bidouiller un émetteur capable de détraquer le système d'intercom. Cet épisode valu aussi à Mitnick la confiscation définitive de son baladeur (Fonseca, 2000). La défense, loin de contester les pouvoirs fantastiques de son client, choisit de les encenser et d'innocenter leur usage en reprenant à son compte une ribambelle d'arguments idéologiques empruntés aux supporters de la liberté en ligne. Par exemple, que dans une civilisation des NTIC triomphantes (Nouvelles Technologies d'Information et de Communication), l'activité *hacker* ferait partie des mécanismes de surveillance nécessaires à la

régulation du chaos internet. Également, que la gestion du réseau des réseaux ne devrait pas rester le privilège de quelques politiques intéressés. Kevin Mitnick serait donc un *hacktiviste* (contraction des mots *hacker* et activiste) et non un *hacker* dégoupillé. Elle finit par gagner son point en contestant les pertes financières reprochées à son client (quatre-vingts millions de dollars). Il apparut justement que les victimes avaient inventé, sinon exagéré, les coûts réels associés aux intrusions de Mitnick. Fait digne de mention, Motorola, Fujitsu, Nokia, Sun, Novell et Nec ne purent établir quelque perte que ce soit dans leurs rapports annuels remis aux actionnaires. Ni fournir des rapports détaillés de ces pertes au *Securities and Exchange Commission* comme la loi les y obligeait pourtant, dixit Donald C. Randolph, avocat de l'accusé et aussi collaborateur occasionnel du site www.freekevin.com (Randolph, 2000). Bref, Kevin Mitnick fut tout bonnement relâché au terme d'une incarcération de cinquante-quatre mois sur la promesse de ne plus retoucher à un ordinateur avant d'avoir complété ses trois années de probation. La cour lui imposa aussi une amende de 4125$ (Deutsch, 2000).

Depuis, une masse d'admirateurs voue un culte au martyre. Un culte qui s'exprime notamment à travers une sorte de fétichisme de l'artefact. Les sites de ventes aux enchères e-Bay, Yahoo Auctions! et Amazon.com se sentent d'ailleurs obligés de freiner quelque peu la circulation de certains souvenirs relatifs au *hacker* en prétextant que cela nuit à leur « image corporative », au même titre que les souvenirs du *IIIème Reich* ou de ceux témoignant des belles années du *Ku Klux Klan* (Sédallian, 2000). Des dizaines de milliers d'autres continuent de « taguer » le web avec les « *Free Kevin* », petits bandeaux jaunes dont le but avoué est de rappeler aux internautes le calvaire enduré par le plus torturé des mythes *hacktivistes*. La *scène hacker* elle-même se garda bien de dénigrer le mythe. Une critique qui ne vint jamais puisque les pièces à conviction démontrant la toute ou fausse puissance de Mitnick manquèrent aux *hackers* comme elles manquèrent à la cour elle-même. Ne restait plus que le mythe et ses icônes dérivées, symboles d'une liberté en ligne à gagner pour les admirateurs, symboles de délinquance pour les détracteurs.

Mais Kevin Mitnick est-il vraiment doté d'une force paranormale qui lui permet de déjouer des systèmes inviolables et de transgresser les lois naturelles de l'informatique? J'expliquerai dans le premier chapitre qui suivra que le *hack* n'est pas l'aboutissement d'un phénomène surnaturel. Il s'agit plutôt d'une réalisation remarquable obtenue au terme d'un effort et d'une ingéniosité acharnée. Nulle magie dans cette réalisation suprêmement technique. C'est son originalité et son efficacité qui détermineront la valeur du *hack*. Le *hacking* est d'ailleurs une activité qui a accouché des meilleures applications informatiques depuis une quarantaine d'années (Tremblay, 2000).

Néanmoins, cette fascination pour l'aspect paranormal du phénomène *hacker* continue toujours de se manifester dans l'imaginaire médiatique. Contraint à décider de l'indécidable, car la cause d'un *hack* n'est ni démontrable, ni observable, ni réfutable, le journaliste en vient à adopter une représentation du *hacker* basée sur une puissance exclusivement mesurée à partir de symptômes. En effet, cette représentation s'opère à partir de symptômes factuels alors que les causes de ces symptômes restent du domaine du plausible. Dans le deuxième chapitre, je décrirai les réflexes (mécanismes) professionnels qui conduisent le journaliste à devenir un allié objectif dans la fabrication d'icônes *superhacker* vraisemblablement possédées de pouvoirs surnaturels.

Le troisième chapitre consistera en une étude de cas impliquant les livres de trois journalistes qui se sont étroitement attardés au mythe Mitnick et qui en ont chacun proposé l'iconographie. Je comparerai ces icônes en contrastant leurs points communs et leurs différences. J'évaluerai ensuite les forces et les faiblesses de ces icônes par rapport à une problématique *hacktiviste* qui considérera le naturel du *hack* d'intrusion, c'est-à-dire son caractère accidentel et ses réelles conditions (techniques et humaines) de réussite. Je concentrerai mon examen sur la place de la plausibilité dans les désaccords exprimés par les trois journalistes pour démontrer à quel point le *hack* d'intrusion demeure un phénomène soumis à la plus incertaine des interprétations.

Finalement, je proposerai à mon tour une icône de Mitnick dont le portrait correspondra mieux à sa véritable pratique et à son rôle à l'intérieur du phénomène *hacker.* Le dernier chapitre prendra la forme d'un article de presse dont la démarche respectera les codes de la profession journalistique. Le seul changement se situera dans le point de vue adopté par rapport au phénomène du *hack* en lui-même. Je ne proposerai pas au lecteur une représentation édulcorée (ou aggravée) d'un Kevin Mitnick dégringolé de l'Olympe *hacker* mais plutôt celle d'un *script kiddie* vraisemblablement dépourvu de pouvoirs surnaturels. J'opérerai donc une variation sur trois icônes, en les dépeignant et en les confrontant, pour aboutir à une contre-icône dont le fondement pourrait orienter plus fidèlement la couverture de la presse.

Chapitre 1 - Une histoire du *hack*

Ce premier chapitre relate l'histoire du *hack* de 1960 jusqu'à aujourd'hui. En retraçant quelques éphémérides, je démontre que si la représentation du *hack* a souvent changé en quarante ans, son essence est demeurée la même. J'y explique que le *hack* est un accomplissement informatique, dans son sens technique le plus pur, et non un pouvoir surhumain capable de commander à un ordinateur la création d'un *output* surnaturel. J'illustre aussi pourquoi la démocratisation constante de l'informatique a suivi une courbe ascendante comparable à celle de l'augmentation des cas de *hacks*. Je termine avec le *hack hacktiviste* en le présentant essentiellement comme un *hack* d'intrusion.

1- Les pionniers du *hack*

En 1957, *Digital Equipment Corporation* (DEC) démarre ses activités à Meynard, Massachusetts. Une petite entreprise de trois employés que personne n'avait vu venir mais qui allait marquer durablement l'histoire de l'informatique. A ce moment-là, l'électricité représente un coût considérable dans l'opération des ordinateurs. Un coût qui peut atteindre annuellement un million de dollars pour une seule machine. DEC saisit donc l'opportunité et se lance dans la production de composantes miniaturisées à faible exigence électrique (Supnik, 2000). En 1960, ils parviennent même à construire un ordinateur complet qu'ils nomment le PDP-1. Un engin de quelques centaines de kilos, peu dispendieux et qui offre des performances étonnantes (Graetz, 1981). Le *Massachusetts Institute of Technology* (MIT), célèbre institution universitaire de Cambridge, s'intéresse au PDP-1 et décide d'en acheter un premier modèle. Un groupe d'étudiants se prend immédiatement d'affection pour cette superbe machine. Mais puisque tout le monde se bouscule pour l'utiliser, la direction décide d'établir un système de cases horaires pour obliger des temps d'accès égaux. Les étudiants les plus débrouillards commencent alors à préprogrammer des tâches informatiques dans le but de sauver sur le temps d'installation personnelle quand leur tour vient. Ces bouts de programmes ingénieux étaient appelés des « *hacks* » (Levy, 1985).

Au MIT, toute une communauté d'esprit se rassemble autour du PDP-1 : c'est le *Tech Model Railroad Club*. Un membre du club accouche de *Spacewar*, sans aucun doute le premier jeu vidéo jamais conçu sur un ordinateur (Graetz, 1981). Mais ses collègues retirent davantage de plaisir à améliorer le jeu qu'à y jouer. Les meilleures applications attirent le respect des pairs et le terme *hacker* est introduit pour titrer les plus doués de la bande. Le plaisir du *hack* se popularise naturellement dans d'autres universités qui à leur tour découvrent qu'il est possible de se doter d'installations informatiques à un prix raisonnable. Il devint habituel à Stanford et Carnegie Mellon d'utiliser le mot *hacker* pour féliciter les plus compétents. L'histoire rapporte que le privé utilisa aussi le vocable à partir de 1965 (Darwin, 2000). De jeunes programmeurs allumés de chez AT&T, Xerox et Bell Labs inventent le *hacker attitude* en plus de léguer quelques-uns de leurs noms à la postérité. Ed Fredkin, Brian Reid, Jim Gosling, Brian Kernighan, Dennis Ritchie et Richard Stallman notamment s'imposent comme les premières icônes d'une culture informatique qui commence véritablement à fasciner une partie de la presse américaine (Himanen, 2001).

Durant les années 1960, tout le monde n'a malheureusement pas la chance de travailler sur un PDP-1. Auteur de *Hackers - Heroes of the Computer Revolution*, Steven Levy appelle cette époque la « dictature IBM ». En effet *International Business Machines* (IBM) règne en maître aux États-Unis. Les modèles 704, 709 et 7090, malgré un prix de vente de plusieurs millions de dollars, trouvent preneurs. De grosses machines capricieuses qui s'obstinent à fonctionner occasionnellement. Levy raconte :

> Quand pour une impénétrable raison l'air conditionné cessait de fonctionner, un gong assourdissant se faisait entendre et trois ingénieurs surexcités surgissaient d'un local attenant. (...) Ces gens faisaient partie d'un clergé. Ils étaient les seuls à pouvoir entrer les données et les usagers devaient d'abord s'adresser à eux chaque fois qu'ils avaient une quelconque requête. Il s'agissait presque d'un échange rituel (Levy, 1985 : 19).

Bogues hardware, fichiers corrompus, erreurs de lectures, troubles de compilation/programme, saturation des mémoires, rupture des disjoncteurs de

protection électrique, toutes les raisons sont bonnes pour expliquer les déboires des IBM. C'est dans ces conditions que les *hackers* des *sixties* font leurs patientes premières armes. Nelson Winkless, fondateur de *Personal Computing Magazine*, se souvient :

> L'installation et le dépannage était une activité angoissante. (...) Le jour où tout le monde souriait enfin après des mois de travail... c'était quand le système tournait plus de 24 heures sans crasher. C'était en 1964... peut-être en 1965 (Winkless, 1996).

L'essentiel de l'activité *hacker* consiste donc à faire tourner des machines qui ne fonctionnent qu'au prix d'un acharnement à toute épreuve. Malgré ces désagréments, la communauté développe, bon an mal an, tout un lot d'applications. Des applications que les *hackers* ont à la fois le mérite de programmer et celui de faire tourner. En 1965, le *hack* est bel et bien synonyme d'accomplissement.

Le *hack*, le savoir-faire, l'ingéniosité, la réussite. Au MIT, un dérapage de sens amène la clientèle étudiante à nommer *hackers* les auteurs de blagues de potache qui ont marqué la réputation de l'établissement. Des blagues douteuses toujours, savamment orchestrées et qui ont le chic de mettre la direction dans l'embarras. A la fin des années 50, par exemple, une bande de farceurs entreprend de gravir l'un des principaux édifices et d'en recouvrir entièrement le toit avec des feuilles d'aluminium. Un vrai travail d'ouvrier, sérieusement planifié et réalisé en dépit des nombreuses rondes des gardiens au sol justement embauchés pour empêcher ces folies. Les jeunes du *Tech Model Railroad Club* n'y échappent pas. Dehors comme à l'intérieur des labos, la farce (prank) constitue un divertissement de tous les instants (Rheingold, 2000).

Mais les années 1960 sont surtout le théâtre de *hacks* plus sérieux qui sont aujourd'hui considérés comme de véritables pièces d'anthologie. En 1966 par exemple, Richard Greenblatt crée un jeu d'échec commandé par une amorce d'intelligence artificielle. Herbert Dreyfus, chercheur réputé mais aussi grand détracteur de l'avancée informatique en matière d'intelligence artificielle, raille la

création de Greenblatt et accepte de l'affronter: L'homme est battu (Rheingold, 2000). Quelques années plus tard (1969), Dennis Ritchie et Ken Thompson, de sympathiques barbus qui seront bientôt affectionnés par la presse, étonnent les admirateurs du *hacking* en programmant *UNIX*, un système d'exploitation universel pouvant tourner sur n'importe quel ordinateur. Le même Ritchie lance ensuite son *langage C*, aujourd'hui encore parmi les plus polyvalents et populaires du monde (Peter, 1994).

Avec une bécane entre les poignes, les premiers *hackers* deviennent des explorateurs, des pionniers, des conquérants. Ils croient défier la machine en la poussant jusqu'à son ultime limite. Au MIT, les meilleurs challengers portent des badges honorifiques. Pris à son jeu incompréhensible, le gang du PDP-1 choisit de s'isoler des autres étudiants en s'érigeant en élite. La majorité de ses membres sont de jeunes ingénieurs ou physiciens de formation. Le gang s'improvise même un costume ; chemise blanche, bas blancs, épaisses lunettes et cravate sombre, laissez passer le *hacker*! L'informatique devient aussi une discipline universitaire à part entière. La *University of Pennsylvania* diplôme Richard Wexelblat en 1968 (Kantrowitz, 2000).

Avec les années 1970 arrive une nouvelle génération de *hackers*. L'informatique continue d'être une aventure toute américaine et les jeunes de la nation, très inspirés par le mouvement contre-culturel, décident de mettre l'informatique au service du peuple. Les chemises à cravate font place aux frusques hippie et la machine cesse d'être un adversaire pour devenir un allié. En Californie surtout, de nombreux projets voient le jour semaine après semaine. En 1970, par exemple, quatre étudiants signent le bail du *Project One*, un vieil entrepôt situé en banlieue de San Francisco. L'idée : acheter un ordinateur et monter une immense banque de données urbaines accessible au grand public. Une première au pays qui pourrait faire boule de neige. La bande n'a pas d'argent, ni moyens, ni programme précis. Elle s'en remet à la providence. Les quatre étudiants diffusent ensuite quelques pubs de recrutement à partir d'une station de radio locale : « Si vous êtes intéressés à bâtir une communauté de partage là où ça ne coûte pas cher, venez au *Project One* » (Brand, 1972).

L'entrepôt s'encombre de deux cents personnes en deux semaines. Des artistes, des artisans, des informaticiens, des électriciens, etc. Certains débarquent même avec toute la famille. Pam Hart, un jeune diplômé de Berkeley à la barbe courte, commande le navire. Ne manque plus que l'ordinateur.

Pam harcèle Trans-America, un important transporteur aérien oublié depuis sa faillite de 1986 (Bullock, 1998). La compagnie, a-t-il appris, stocke trois ordinateurs XDS 940 dans la poussière d'un hangar à l'aéroport de San Francisco. Pam leur demande de faire une bonne action corporative et de leur céder une machine. Trans-America finit par céder, à la surprise de Pam lui-même. Un cadeau important estimé à 120,000$ (Freiberger et al., 2000). Le XDS 940 est transporté par les fidèles médusés et c'est une subvention de 10,000$ accordée par une obscure fondation qui permet à la bande de se procurer les dernières pièces manquantes (câbles, fusibles, ventilateurs, etc.). Rebaptisé *Resource One*, le projet démarre, arrête, repart, fonctionne, connaît quelques ratés puis tout le monde retourne finalement chez soi en abandonnant un ordinateur complètement mutilé (Brand, 1972).

De telles initiatives, les années 1970 en ont connu de nombreuses. Malgré la compétence certaine des protagonistes, les moyens techniques manquent cruellement et l'informatique coûte trop cher. L'armée, le gouvernement, les grandes entreprises et les universités restent les seuls à pouvoir se la payer. Les *hackers* attendent quelque chose : une révolution hardware. Elle vient du Nouveau Mexique (Albuquerque) en 1975 quand *Micro Instrumentation Telemetry Systems* (MITS) lance l'Altair 8800, premier vrai micro-ordinateur. Il est équipé d'un microprocesseur Intel 2 MHz et traite ses données dans un espace RAM de 256 octets. Le kit se vend 395$. Même si l'entreprise est acculée à la faillite en trois ans (des problèmes de liquidité combinés à des ventes décevantes : seulement 5000 modèles vendus), l'Altair décide de l'architecture des micro-ordinateurs. La formule : carte maîtresse, processeur, bus, unités de sauvegarde, mémoires *RAM* et *ROM*, ports, cartes en série et boîtier rigide. L'Altair inspire aussi plusieurs acteurs importants de la future

informatique, dont Paul Allen et Bill Gates, fondateurs de *Microsoft*, qui écrivirent pour lui une version du compilateur *BASIC* (Sanderson, 1998).

Vient ensuite l'Apple II (1977), étrange machine assemblée par des bidouilleurs au fond d'un garage californien. Encore une fois, les ventes tardent à décoller. Mais une irrésistible tendance se dessine : l'avenir de l'informatique sera personnelle. 1978 : le TRS-80. 1979 : l'Atari 800. 1981 : l'Apple 3. 1982 : le TRS-80 en couleurs. 1983 : l'Apple 2. 1984 : le Commodore 64 et le Macintosh. A partir de cette dernière année, les machines se vendent par millions et les enfants demandent un ordinateur pour Noël (Tal, 2000).

2- Les *phone phreakers*

Les années 1970 sont aussi celles des *phone phreakers*. Le phénomène prend véritablement son envol en 1970 quand un vétéran de la guerre du Viêt-nam (John Draper) s'aperçoit qu'un sifflet distribué en promotion dans les boîtes de céréales Cap'n Crunch émet la tonalité 2600 hertz. Cette tonalité correspond au code analogique d'accès pour les appels interurbains d'AT&T. En sifflant dans le combiné, une voix lui répondait immédiatement : « *Thanks for using AT&T* » (Slatalla, 2001).

Puisque les appels interurbains coûtent chers, toute une panoplie de gadgets sonores plus ou moins sophistiqués et fabriqués par les *phreakers* se répand dans la population. Les grandes centrales téléphoniques démontrent une totale incapacité à contrôler leurs réseaux et les pertes occasionnées par ce petit trafic sont considérables (Massey, 2000).

Stimulés par la rentabilité du business, les *phreakers* explorent les systèmes téléphoniques avec une patience de *hacker*. Ils réussissent d'ailleurs à développer certaines applications plutôt surprenantes pour l'époque, dont des *party lines* capables de réunir simultanément des dizaines d'interlocuteurs

éparpillés aux quatre coins du pays. Aux frais des grandes centrales téléphoniques bien sûr (Massey, 2000).

En 1980, la majorité des micro-ordinateurs sont vendus avec un port pour modem. Des babillards électroniques (BBS) commencent à voir le jour au Canada et aux États-Unis. Ils deviennent des lieux d'échanges et de discussions très populaires. Des *phreakers* comprennent qu'en combinant leurs connaissances du téléphone aux possibilités éclectiques du micro-ordinateur, ils pourront se doter d'une compétence redoutable. Pour la première fois, *hackers* et *phreakers* convergent et se rejoignent (Walleij, 1994).

3- Le phénomène *WarGames*

En 1983, c'est la sortie du film *WarGames* . Le grand public découvre pour la première fois le visage obscur du *hacking.* Un adolescent, qui joue d'astuces pour dérober des jeux vidéo, pénètre par hasard le système de défense de l'Armée américaine. Un film culte qui propose une image facile de l'intrusion en réseau. Ennuyer les entreprises connectées devient subitement le passe-temps favori de plusieurs jeunes Nord-Américains. De petits logiciels *phreaker* de *scanning* sont disponibles sur les babillards électroniques pour téléchargement. Ils utilisent le modem pour balayer une gamme de numéros de téléphone et bloquent automatiquement sur ceux qui semblent correspondre à des portes d'accès mal protégées. Le pied dans la porte, il suffit maintenant d'utiliser d'autres logiciels capables de coller les bons mots de passe. Pour beaucoup de *hackers* aujourd'hui célèbres (dont Kevin Mitnick), c'est le premier *hack* (Williams, 1998).

En 1984, Steven Levy, brillant journaliste fada de l'activité *hacker*, publie un ouvrage fondateur : *Hackers - Heroes of the Computer Revolution*. Il exhorte les *hackers* à jouer un rôle social et à respecter un code d'éthique dont les points principaux sont les suivants:

1- L'accès aux ordinateurs doit être total et illimité

2- Se consacrer à toujours maintenir son propre rendement

3- Toute l'information doit être gratuite

4- Ne jamais faire confiance à l'autorité (promouvoir la décentralisation)

5- Les hackers doivent être jugés par la qualité de leurs hacks (le mérite)

6- Devoir créer de l'art et de la beauté avec un ordinateur

7- Devoir utiliser les ordinateurs pour rendre la vie meilleure

(Levy, 1985 : 40)

Levy, admirateur de la genèse du phénomène *hacker*, rêve en 1984 d'une nouvelle communauté *hacker* responsable. Mais le code d'éthique reste le credo des puristes, pas nécessairement des *hackers*, qui le brandissent pour lutter contre cette association de sens entre *hacking* et malveillance informatique. Si les puristes réussissent finalement à introduire le terme *cracker* dans la presse pour désigner les délinquants du réseau, le code d'éthique de Levy reste méconnu. D'ailleurs, il devient de plus en habituel que les *hackers* les plus capables soient aussi les plus déconnectés médiatiquement parlant. La genèse du phénomène *hacker* (de l'informatique aussi), Levy et les discours tenus par les phares idéologiques reconnus de la présumée communauté *hacker* restent d'ordinaire des choses qui n'intéressent pas le *hacker* (Eads, 2001). En revanche, Levy demeure un document idéologique important pour d'autres personnalités *hacker* moins crédibles mais justement très sollicitées par la presse.

Carolyn P. Meinel, une Américaine controversée au passé *hacker* invérifiable, se réclame justement des puristes. Personnalité flamboyante, démarche pimpante, excellente conférencière, elle a su durant les années 1990 se bâtir une étonnante notoriété. Elle publiait en 1998 *The Happy Hacker*, ni plus ni moins un guide technique et idéologique destiné aux *hackers* en herbe. Elle y reprenait les idées de Levy en les encadrant d'un discours *WarGames*. Selon elle, il serait légitime de s'en prendre à l'ordre établi et de lutter obstinément contre toutes les institutions qui s'imposent en mur contre la liberté d'accès à

l'information. Même si une collection de sites lui est aujourd'hui consacrée par des détracteurs, qui à défaut de critiquer son discours souhaitent prouver sa véritable nullité informatique, elle reste l'une des icônes *hacker* les plus sollicitées par la presse. Réputée mesquine, colérique et détestable, Carolyn Meinel continue pourtant en 2002 de diffuser son discours et de vendre ses livres aux adolescents (Martin, 2000).

Durant les années 1980, les *hackers* s'entourent aussi de sympathisants, de fans, de collaborateurs. Des gens qui n'ont pas nécessairement de grandes compétences en informatique mais qui sont intéressés par la chose. Parmi eux se trouvent des sociologues, philosophes, journalistes, universitaires, écrivains, etc. Ils deviendront la voix mais aussi les ambassadeurs de la philosophie *hacker*. Ces gens de tous les horizons publient une abondante littérature. Beaucoup font un excellent travail de vulgarisation technique en recueillant des informations à la source. Alors que les *hackers* des années 60 étaient mystérieux, inaccessibles et incompris, c'est tout le contraire pour ceux des années 1980. N'importe quel débutant dispose désormais de vastes ressources techniques qui ont aussi le mérite d'être écrites dans un langage compréhensible. L'autodidacte peut maintenant réussir son premier *hack* à partir de sa chambre (Eudes, 1995).

4- Le code source sur le net

En 1984, le *hacker* Richard Stallman s'insurge contre l'impossibilité pour le programmeur d'obtenir le code source des logiciels vendus par les géants de l'informatique. Le code source est le programme derrière l'application. Ouvert, il permet à l'usager de modifier le logiciel. Stallman rêve d'un système d'opération (OS) gratuit et ouvert que l'usager pourrait retaper à sa guise. Le *hacker* quitte donc son employeur (un laboratoire de recherche au MIT) et se retire chez lui avec le projet ambitieux de développer un système d'opération. Tandis que *UNIX* se vend à un prix que seules les institutions peuvent se permettre, il reprogramme entièrement le cœur de l'OS et parvient à faire circuler son clone

(GNU's Not Unix) gratuitement au bout de six mois. GNU se répand comme une traînée de poudre et des centaines de programmeurs volontaires décident de se réunir autour de Stallman pour poursuivre le développement du clone. Un développement qui se poursuit encore aujourd'hui. Le populaire système d'opération *Linux* est d'ailleurs un rejeton du projet de Stallman (Garfinkel, 1993).

Le principe de la gratuité fait son chemin. C'est l'idée du partagiciel (*shareware*). L'usager essaie le logiciel et s'il juge qu'il vaut quelque chose, il est libre d'envoyer un chèque à son concepteur. Ce genre d'initiative provoque un boom sans précédent. Tout le monde peut mettre la main sur des logiciels de toutes sortes. Cela permet à beaucoup de néophytes d'utiliser leurs micro-ordinateurs pour des applications inimaginables autrement et à des *hackers* de diffuser tout leur génie. Plagiats et piratages deviennent cependant légion et il suffit au *hacker* d'entretenir son réseau de contacts pour mettre la main rapidement sur une foule d'applications qu'il n'a plus à programmer lui-même (Ford, 2000).

Au début des années 1980, beaucoup d'usagers ont accès aux BBS ou aux FTP pour transférer des données. Mais le réseau est fragile, le débit est lent et naviguer entre les nœuds (*hosts*) sans s'égarer exige de bonnes connaissances. Pour le débutant, rien n'est facile. Dans la grande majorité des cas, le micro-ordinateur demeure un outil de travail ou de divertissement coupé du monde extérieur. Il faut attendre 1990 pour que l'accès aux réseaux se simplifie véritablement. D'abord, c'est la fin d'ARPANET (la vieille toile de télécommunications américaine démarrée en 1969 et financée à même les miettes du programme spatial). Jamais le réseau des réseaux ne s'est porté aussi bien. Il compte plus de 313,000 serveurs hôtes comparé à 5089 en 1986 et 213 en 1980. Au Canada, au Royaume-Uni et aux États-Unis (la France s'accroche à son Minitel), l'État subventionne toutes sortes de projets. Le privé aussi commence à imaginer des avenues et consacre des argents en recherche et développement. Les politiques rafraîchissent leurs discours avec des concepts qui ratissent large : autoroute de l'information, commerce électronique, industrie multimédia, etc. En six mois, le nombre de *hosts* passe à 535,000. Puis fracasse

la barre du million en 1991 (Internet Software Consortium, 2000). Trois étudiants de *McGill University* (Montréal) développent le premier navigateur (*browser*) qu'ils baptisent *Archie* pour faire sympa (Brody, 1994). *Archie*, c'est à la fois le nom du héros d'une bande dessinée américaine qui s'adresse aux adolescents et aussi le diminutif du concept « explorateur d'archives » (Wheeler, 2001). Ce navigateur permet des déplacements beaucoup plus intuitifs sur le net. Viendront ensuite *Mosaic*, *Netscape*, *Explorer*, *Opera* et bien d'autres encore.

Déjà en 1945, Vannevar Bush avait imaginé une toile hypertexte. Dans un article intitulé *As we may think* et publié dans *Atlantic Monthly*, Bush proposait une interface de navigation entre plusieurs machine qu'il avait proposé d'appeler le *Memex*. C'est en 1965 que Ted Nelson, auteur et essayiste, introduisit finalement le mot *hypertext* en s'inspirant des travaux de Bush. En 1990, l'année clé de l'Internet, Tim Berners-Lee commence à travailler sur un projet d'hypertexte global. Avec deux collègues, il écrit le programme du premier serveur *httpd* et son premier client, le *World Wide Web*. Sur les httpd, c'est *what you see is what you get.* Littéralement : ce que vous voyez c'est ce que vous obtenez. Le standard est adopté et en moins de deux ans le web devient la hauteur virtuelle la plus populaire de l'Internet (Berners-Lee, 1999).

1990, c'est aussi l'année de la consécration du télécopieur. L'avènement de la technologie V.17 fixe la vitesse de transmission à 14 400 octets par seconde (quatre pages / minute). Pour la première fois aussi, le télécopieur se vend sous la barre des 200$ pour le modèle externe autonome. Une carte fax/modem interne (avec son logiciel) pour micro-ordinateur, qui exige une installation de quelques minutes, se vend 100$. Le télécopieur devient un argument de plus qu'utilisent les détaillants d'ordinateurs lorsqu'il s'agit de recommander l'achat d'un modem (Davidson Consulting, 2000). Désormais, les consommateurs achètent des micro-ordinateurs parés à l'accès. Par le fait même, les *hackers* ajoutent le télécopieur à leurs champs d'intérêt et viendront bientôt les cas de piratages (interceptions, suppression, falsifications, etc.).

Le branchement en réseau décuple le potentiel du micro-ordinateur. Celui de l'usager aussi. Il a maintenant accès à d'immenses facilités et surtout à tous ces codes sources qui traînent. Les nombreuses ressources disponibles en ligne peuvent à elles seules amener un néophyte intéressé à maîtriser rapidement l'ordinateur. Des documents explicatifs aux logiciels gratuits en passant par les groupes de discussion, une conjoncture favorable se dessine : n'importe qui est maintenant à deux clics de souris de se découvrir une compétence informatique. A partir de 1990, de plus en plus de gestes traditionnellement posés par des *hackers* diplômés le sont maintenant par des amateurs. Des néophytes qui viennent d'acheter leur premier micro-ordinateur sont arrêtés pour des actes de *mailbombing*, action qui consiste à paralyser un serveur en le bombardant de courriers électroniques (Jud, 2000).

Des plaisantins profitent aussi de l'anonymat relatif du net pour faire du vandalisme. *Internet Relay Chat* (IRC), réseau de discussion en mode texte fréquenté par des centaines de milliers de personnes, est continuellement parasité par des plaisantins. Les usagers sont victimes de déconnexions forcées (*nukes*) et les opérateurs perdent régulièrement le contrôle de leurs canaux (*channels*). Inutile de posséder de vastes connaissances en informatique pour perturber le réseau. Suffit de s'équiper aux bons endroits. Des logiciels sont disponibles sur les sites de *WAREZ,* contraction des mots *software* et *easy.* Souvent programmés par des *hackers* à la recherche de notoriété, ces logiciels sont d'une facilité d'utilisation déconcertante. Avec *Win Nuke* par exemple, une application qui exploite les failles de *Windows 95*, l'usager n'a qu'à écrire l'adresse réseau (*IP*) de sa victime pour figer son micro-ordinateur, l'obligeant à redémarrer (Arquilla, 1998).

Mais sur les *WAREZ*, il est possible de trouver bien pire encore. Toutes sortes de trucs allant des constructeurs de virus (incluant vers et bombes logiques) aux générateurs de numéros de cartes de crédit, en passant par les briseurs de mots de passe et les chevaux de Troie capables de prendre le contrôle d'autres machines à distance. Pour stimuler les visites, les webmestres saupoudrent leurs WAREZ avec des recettes de bombes chimiques, de drogues

dures et aussi une effroyable quantité de logiciels développés par de puissantes institutions (Adobe, Macromedia, Corel, etc.) tout bonnement piratés et rendus disponibles pour tous ceux qui font l'effort de cliquer. La seule motivation de ces sites réside dans l'augmentation de leur achalandage. Dans les faits, ils sont devenus des lieux privilégiés pour les annonceurs de matériel pornographique qui placardent les WAREZ de bannières publicitaires. Les exploitants du site www.warezdimension.com sont aujourd'hui considérés comme des pionniers dans le domaine (McCandless, 1997).

5- *The lamer way of life*

Pendant deux ans, Christian Valor s'est vanté de nettoyer le net de plusieurs de ses pédophiles. Aussi connu sous le pseudonyme *Se7en*, Valor pénétrait serveurs et ordinateurs personnels, les explorait et quand il trouvait une photo compromettante, il formatait (effaçait) les disques durs. Il signait ses nettoyages en laissant des photos de pythons. Le cyber-justicier tenait à se faire connaître des médias et il multipliait les contacts. Sa croisade suscita l'intérêt de nombreux journalistes qui acceptèrent d'en faire un sujet de reportage. Valor fit la une de publications importantes dont le *Florida Today*, *The Independent of London*, *Popular Mechanics* et même *Wired News*. Mais un *hacker* américain reconnut Valor et contacta la presse pour l'informer qu'il s'agissait sans doute d'un canular. Brian Martin (alias *Jericho*) raconta qu'il avait connu Valor autrefois dans une entreprise de sécurité californienne. Il avait conservé de lui le souvenir d'un incapable tout juste bon à classer la paperasse. Un technicien de très bas niveau qui n'aurait certainement jamais pu être crédité du moindre *hack*. Les gens de *Wired News* furent les premiers à réagir et envoyèrent un journaliste pour harceler Valor de questions. Ce dernier finit par avouer son canular. Ses prétendues attaques avaient été simulées artificiellement sur son ordinateur. Les journalistes n'y avaient vu que du feu. Gênés par leur propre crédulité, ils dénoncèrent Valor en bloc et lui firent perdre la face. Des associations de *hackers* se moquèrent aussi du justicier déchu en lui décernant le titre de *lamer of the year* (Silberman, 1999).

Le mot *lamer* est tombé des nues quelque part durant les années 1980. Les premiers à l'avoir utilisé sont vraisemblablement des gangs de *skateboard* qui s'en servaient pour se moquer des moins doués. Il est un dérivé direct de *poser*, autre mot qui servait à désigner celui qui se donnait l'allure d'un vrai *skater* (vêtements cool, *skateboard* de qualité, attitude décontractée, langage alerte, etc.) mais qui n'avait aucun talent pour sortir les tripes de sa planche à roulettes. Bref, un fumiste qui excellait pour prendre un air assuré lorsqu'il s'agissait d'aller voir les filles mais qui avait intérêt à garder sa planche sous son bras plutôt que sous ses pieds (Treble, 1999).

En vieillissant, cette génération de skaters aurait troqué le *board* pour le *motherboard* (carte maîtresse) et certains d'entre eux, choc des générations oblige, seraient devenus des *hackers* aussi talentueux que respectés. Le *lamer* aurait donc quitté les trottoirs pour s'installer définitivement dans le cyberespace où curieusement le mot s'est répandu. Des vieux de la vieille comme Eric Raymond (auteur du *New Hacker's Dictionary*) l'ont trouvé amusant et ont contribué à sa popularité. Le *lamer* désigne aujourd'hui le *wannabee* (je veux être!) sans scrupules qui cherche la reconnaissance à tout prix. Plus précisément : un nul qui dissimule son incompétence technique derrière un talent évident pour le baratin (Raymond, 2001).

Parmi les *lamers* se trouvent les *script kiddies*, sous-groupe spécialisé dans l'art d'utiliser le matériel programmé par d'autres. Dans les carrefours *WAREZ*, ils commettent des razzias intempestives pour repartir en guerre armés jusqu'aux dents. Les *script kiddies* se regroupent habituellement sur des canaux de discussion. Le canal #2600 sur *Internet Relay Chat* par exemple. Ils se lancent là-bas des défis dans une atmosphère de conspiration. Mais compétence ou non, la justice ne rigole pas. Surtout pour les méfaits qui occasionnent des pertes économiques. Chaque jour dans le monde, des dizaines de *script kiddies* sont arrêtés par la police. La Chine a même décidé d'établir sa jurisprudence en condamnant à mort certains des plus crapuleux. Aux États-Unis, le FBI n'hésite plus à envoyer des *script kiddies* en prison, même s'ils n'ont que seize ans. Car justement, l'essentiel de la malveillance informatique est finalement l'œuvre de

lamers pas très futés. Bien sûr, beaucoup réussissent des coups spectaculaires, dans la mesure ou n'importe qui peut se pointer devant *Fort Knox* avec un fusil-mitrailleur et réclamer l'ouverture des coffres. « En 2002, approximativement 19 millions de personnes dans le monde posséderont les capacités techniques pour lancer une cyber-attaque » *(*Cilluffo, 1999*)*. Mais le jusqu'au-boutisme en ligne mène ordinairement à la capture du *script kiddie*. Le phénomène n'est pas seulement qu'une affaire d'adolescents car malgré son appellation juvénile, le *script kidding* renvoie à une attitude et non à un groupe d'âge. Il existe certains cas de *script kidding* impliquant des quadragénaires (Lemos, 2000).

6- *Le Pearl Harbor électronique*

Inquiétés en 1998 par les agressions répétées d'un jeune *hacker* israélien (Ehud Tannenbaum), les États-Unis commencèrent à redouter l'éventualité d'un *Pearl Harbor électronique*. Cette année-là, le président Clinton y allait de sa *Directive 63*. Cette Déclaration présidentielle libérait des fonds extraordinaires pour la mise en place d'un réseau d'information imperméable aux intrusions et qui serait fonctionnel à partir de l'an 2003. En détail : 3.6 milliards de dollars dont 2 milliards maintenant. Il fallait se doter d'une infrastructure capable de protéger la nation contre l'ennemi *hacker* (Sabatier, 2000).

Le *hacking* c'est devenu une sérieuse affaire. En 1995, le Pentagone reconnut avoir été la cible de 250,000 attaques. Dans 65% des cas, les *hackers* avaient réussi à traverser le premier niveau de sécurité. Le Pentagone se fait discret depuis sur les chiffres mais les dirigeants soutiennent que la situation ne va pas en s'améliorant. Le 24 juin 1998, le directeur de la CIA (George Tenet) déclarait que certains hauts gradés chinois estimaient que l'économie américaine pourrait être ruinée par des attaques dirigées sur quelques points sensibles du système bancaire. Il affirmait aussi que l'utilisation grandissante de l'informatique par l'Iran, l'Irak et la Libye constituait une menace pour les États-Unis (Soldevila, 1998). Bref, il était temps de réagir. Les États-Unis se précipitaient donc tête première dans une course pour la suprématie du *hacking* en ligne.

La malveillance informatique coûte cher aussi. Virus, piratages de logiciels, espionnage industriel, attaques par saturation de sites commerciaux, chantages, appels au boycott, diffamations, sabotages, utilisations frauduleuses de cartes de crédit, usurpations de comptes, tout ça occasionne des pertes mondiales qui se chiffrent en milliards de dollars chaque année. Point de vue logiciel seulement, l'organisme international *Business Software Alliance* (BSA) évalue à onze milliards le coût du piratage pour la seule année 1998, ce qui se serait traduit par une perte de 130,000 emplois aux États-Unis (Halazy, 2002).

Un peu partout dans le monde, les gouvernements de l'an 2000 réagissent violemment. Les États-Unis viennent de lancer *Carnivore*, un système supposé capable d'intercepter l'ensemble des données transitant sur son territoire et compromettant ainsi toute espèce d'anonymat pour l'internaute (Simoneau, 2000). La France a modifié sa loi sur l'audiovisuel en rendant responsables tous les serveurs situés dans l'Hexagone du contenu qu'ils hébergent (Deglise, 2000). Une mesure jugée excessive qui obligea *Altern.org*, un serveur à but non-lucratif, à fermer ses portes. 90,000 sites disparurent illico, faisant sombrer tout un pan de la francophonie sur le net. Le 28 juillet 2000, les Britanniques ont voté le *Regulation of Investigatory Powers Act*, une loi qui permet aux autorités d'utiliser tous les moyens nécessaires pour pouvoir écouter le citoyen en ligne. Depuis, comme l'avait prédit la Chambre de commerce britannique, des entreprises en commerce électronique cernées par la législation ont décidé de quitter le pays. Pertes qui pourraient s'élever pour l'économie britannique à 70 milliards de dollars selon les détracteurs (Cloutier, 2000).

7- Le *hack* aujourd'hui

Le week-end du 28 juillet 2000 se tenait à Las Vegas le 8^{ième} DefCon, sorte de congrès annuel durant lequel un millier de *hackers* sont invités à mesurer leurs compétences. Il s'agit du plus important de tous les événements *hacker*. C'est le temps pour les participants d'écouter quelques conférences, d'échanger des trucs, de boire des *smart drinks* glacés et surtout de participer au défi du *château des illusions*. Le château c'est une machine dont certains ports

de communication ont été verrouillés avec des firewalls et d'autres laissés ouverts. L'engin se comporte en réseau comme s'il était un aspirateur fou, avalant et emprisonnant tous ceux qui maraudent. Les *hackers* sont ensuite invités à s'approcher du piège. Le premier qui prend le contrôle du château est déclaré vainqueur, ce qui ne manque jamais d'arriver à chaque nouvelle édition du Defcon (Thorel, 2000).

Opérer un ordinateur SDS instable en 1965 ou prendre le contrôle du château en 2000, même *hack*, même gloire. Quarante années ont passé et la communauté *hacker* continue de célébrer les valeurs du mérite informatique. Car le *hack* est justement une réalisation informatique assistée par ordinateur. Il n'est pas une action mais un accomplissement capable de mériter à son auteur la reconnaissance des pairs *hackers* comme celle des profanes. Que cette reconnaissance inspire la crainte ou l'attirance, le *hack* était et demeure une représentation subjective soumise à supputation. Le système d'exploitation Linux du Finlandais Linus Torvalds ou le *langage C* de Dennis Ritchie sont considérés comme des *hacks* fameux et aussi comme des pièces à conviction validant leurs statuts de *hacker*. Car chez le *hacker*, il règne la loi du *hackito ergo sum* : je *hacke* donc je suis. Sans preuve, en clair ou en apparence, aucune reconnaissance possible (Hurley, 2001).

Certains observateurs ont tenté de théoriser le *hack*. Steven Levy le considère par exemple comme une interaction privilégiée avec l'ordinateur dont le produit repousse les limites de la machine jusque dans ses derniers retranchements (Levy, 1985). Pour William Gibson, très célèbre auteur de science-fiction qui a notamment introduit le terme *cyberspace* en 1984, le *hack* c'est le passage obligé de l'extrême compétence informatique et ça se vit principalement en ligne, dans les réseaux (Grimwood, 1998). Le *hack* est un accomplissement suprêmement technique. Chez Gibson c'est l'efficacité du *hack* qui détermine sa valeur. Mais efficacité ne rime pas nécessairement avec utilité. Convertir du *EBCDIC* en utilisant un programme maison pour en faire de *l'ASCII* n'est pas moins impressionnant qu'écrire un serveur en *langage C* qui tient en dix-huit lignes. Tant que ça fonctionne. Quant à Florent Latrive, chroniqueur

informatique chez *Libération*, seule une pratique obsessionnelle de l'informatique peut conduire au *hack*, une théorie qui trouve sa validation dans un article du *Psychology Today* publié en 1980. Cette année-là les gens du très sérieux magazine s'étaient penchés sur le cas d'une cinquantaine d'étudiants en informatique de *Stanford University* qui s'adonnaient au *hacking*. Ils avaient dressé d'eux le portrait d'une bande de « décrochés » qui s'étaient intentionnellement réfugiés dans le cyberespace de leur Intranet, refusant de vivre dans le monde réel. Pour communiquer, ils en étaient venus à s'exprimer dans une sorte de slang incompréhensible et se fichaient éperdument des gens de « l'extérieur ». Le *hacking* dur est une activité très prenante qui conduit inévitablement à une perte de contact avec la réalité (Silverstein, 2001).

Dans le *New Hacker's Dictionary* écrit par Eric Raymond, *hacker* c'est « typiquement travailler sur un programme », c'est-à-dire le développer soi-même ou encore l'altérer pour en tirer quelque chose de meilleur. Le *hack* c'est *l'output* (résultat) de la démarche technique. Dans cette foulée, de plus en plus de gens s'autoproclament *hackers*, dont certains artistes électroniques qui ont créé des œuvres intéressantes à partir de programmes déjà existants. Ces *outputs* deviennent autant de réalisations qui ont le potentiel d'attirer la reconnaissance d'autrui (Raymond, 2001).

Arthur C. Clarke, auteur de « *2001 : A Space Odissey* » et vulgarisateur scientifique distingué, a écrit en 1972 : « Toute technologie suffisamment avancée est indiscernable de la magie » (Martel, 1996). Bien sûr, le *hack* peut s'apparenter à de la magie dans la mesure où celui-ci demeure un *output*. En revanche *l'input* magique n'existe pas. L'ordinateur possède ses propres systèmes d'opération et de contrôle qui lui permettent d'assister l'humain en assemblant automatiquement des librairies de programmation, classant des bases de données, enregistrant des événements pour en produire ensuite des rapports détaillés, comparant des messages d'erreur/compilation, discutant des choix d'assembleurs, etc. Mais l'ordinateur reste un gestionnaire *d'inputs* incapable de *hacker* par lui-même. D'ailleurs, la machine est elle-même le résultat d'un *input*. Contrairement à la représentation qu'en avaient les jeunes du

Tech Model Railroad Club en 1960, le *hacking* ne consiste pas à défier la machine. Il s'agit plutôt d'un défi d'humain à humain. Quand un *hacker hacke* un système pour produire un *output* remarquable, il *hacke* un ouvrage humain possédant ses failles, sa structure arbitraire, son degré d'imagination et ses limites techniques, voire philosophiques. Puisqu'il est un outil, l'ordinateur demeure impuissant à contrecarrer l'intervention humaine qui le sabote ou le consolide. A moins d'être verrouillé (Coupland, 1991). Par exemple, l'efficacité et la stabilité d'un système d'opération (OS) populaire comme *Windows XP* dépend en partie de son usager. Si celui-ci installe les mauvais gestionnaires (*drivers*) pour ses périphériques, son ordinateur personnel connaîtra des ratés. Sinon, il est aussi admis de maudire l'équipe de concepteurs qui a développé un programme présumé instable et approximatif. L'informatique est strictement une entreprise d'êtres humains qui comporte son lot d'erreurs, de confusions et de jean-foutre. Cela est vrai de la conception logicielle à l'intendance en passant par l'assemblage et l'emploi. D'un bout à l'autre de la chaîne, aucun rituel occulte ne peut intervenir sur le fonctionnement de l'ordinateur. Les paroles magiques psalmodiées, l'imposition des mains comme dans *Ouija*, un sacrifice animal fait aux dieux de l'Olympe *hacker*, tout cela restera sans effet. Pour activer l'ordinateur, il faut obligatoirement une intervention humaine directe. Sinon la machine continue d'utiliser son unité de traitement logique (d'ailleurs déterminée par un être humain) pour faire tourner en boucles des fonctions et des réactions préprogrammées. Les boucles sont donc répétées à l'infini tant et aussi longtemps qu'un nouvel *input* n'a pas été imaginé et ensuite introduit par l'usager.

Cela dit, le *hack* peut prendre d'innombrables formes (virus, cryptographie, bases de données, cognition, *phone phreaking*, etc.) éparpillées en une infinité de champs techniques. D'autant que la démarche reste assistée par ordinateur. Il ratisse large et sa définition est sujette à une controverse qui pourrait à elle seule faire l'objet de plusieurs mémoires comme celui-ci. C'est pourquoi je considérerai seulement le *hack* d'intrusion comme il existe à l'intérieur de l'infrastructure Internet. Par Internet j'entends les serveurs, routeurs et tables de routage.

La réalisation d'un *hack* d'intrusion par le net passe par les étapes suivantes :

1 2 3 4 5

Un *hacker* ⇒ Un réseau ⇒ Des parades ⇒ Un serveur ⇒ Le *hack*

Au point 3 se situe l'obstacle puisque cette démarche ne se fait pas sans heurts. Des mécanismes de sécurité sont systématiquement installés par les hébergeurs pour contrer les individus mal intentionnés qui voudraient toucher aux données. Même la plus banale des pages web est protégée par un dispositif théoriquement et techniquement inviolable. Le plein succès d'un *hack* repose donc sur deux conditions :

1 : Déjouer la ou les parades

Les parades constituent des boucliers ou des leurres (matériels ou logiciels) dont l'objectif est d'empêcher le *cracker* de pénétrer un système connecté au réseau. Une liste des principales parades ayant cour sur le net depuis 1995 se trouve en annexe 1.

2 : Se retirer sans laisser de traces

Les *crackers* dont la position est détectée durant la réalisation du *hack* augmentent statistiquement leurs chances d'êtres capturés. Il s'agit donc d'opérer rapidement puis d'effacer ses traces. Aussitôt qu'une action est entreprise contre un hébergeur, les administrateurs-réseaux peuvent recevoir le signal sur des moniteurs dédiés. Mais toutes les entreprises ne sont pas aussi appliquées. Elles le verront à condition d'y porter attention. Dans cela, rien de nouveau sous le soleil puisque les gros hébergeurs sont testés jour et nuit par une horde de *script kiddies* qui perturbent le net planétaire. Avec des logiciels à balayage rapide, ils explorent les failles sur la surface des serveurs. Un adolescent équipé de l'ordinateur familial peut ainsi balayer des millions d'adresses par semaine. Les internautes eux-mêmes sont testés sans le savoir, suffit de s'équiper d'un logiciel d'observation pour le constater. *ZoneAlarm* par

exemple, développé par ZoneLabs. S'ils sont diagnostiqués vulnérables aux *chevaux de Troie*, *cocks port probes* ou *smurf attacks* par exemple, ils s'exposent à de graves problèmes (Tremblay, 2000). Les hébergeurs ont l'habitude d'assister à ces actions sans réagir. Aucune loi n'empêche un individu de tester la porte verrouillée d'un supermarché à 3h00 du matin.

Les *crackers* compétents profitent du vacarme électronique des *script kiddies*. Selon John C. Dvorak, journaliste chez *PC Magazine* :

> Notez cependant que très peu de peu de pirates sont assez habiles pour couvrir leurs traces complètement. Dans la plupart des attaques, il est possible de remonter jusqu'à leurs origines. Mais qui s'échinerait à traquer tout le monde quand des millions de sondages ou attaques sont perpétrées chaque jour ? (Dvorak, 1999)

L'activité globale d'un serveur est sauvegardée dans des rapports appelés *logs*. Après l'intrusion, ils agissent en tant que pièce à conviction. Leur démêlage peut conduire très rapidement à la capture du *cracker*, surtout si ce travail s'effectue en collaboration avec d'autres hébergeurs qui ont conservé des données relatives au bond précédent. Bref, qu'un *cracker* soit capturé ou non, cela reste un excellent indicateur de sa compétence. Des *script kiddies* peu futés ont déjà été pincés parce qu'ils étaient « stupidement » revenus contempler un site web fraîchement piraté avec leur navigateur, révélant ainsi leur adresse réseau. (Dvorak, 1999).

Il est malaisé d'évaluer la qualité d'un *hack* d'intrusion. Bien sûr, s'introduire dans un serveur barré est impossible. Pourtant les *hackers* y parviennent. Comment? La faille. Elle est humaine bien sûr et se classe en deux catégories :

1- Faille d'incompétence

Les failles d'incompétence peuvent être occasionnées par une méconnaissance de l'informatique de la part des responsables techniques, une erreur d'installation, un oubli, etc.

2- Faille organisationnelle

Les failles organisationnelles sont généralement dues à un manque de ressources humaines dédiées à la sécurité, à des problèmes de discordes entre les employés, au mode de gestion adopté par la direction, etc.

Contrairement au monde physique, il est impossible d'ouvrir une porte à la dynamite dans le cyberespace. Mais il est possible de déjouer la vigilance des gardiens. L'être humain est justement le maillon le plus faible de tout système informatisé. Il existe une technique nommée l'ingénierie sociale (*social engineering*) qui consiste à tromper la personne clé à l'intérieur d'un système de sécurité informatisé. L'utilisation du téléphone est un classique. Par exemple, le *hacker* appelle le technicien et se fait passer pour son supérieur. D'une voix autoritaire et pressante, il lui ordonne de lui révéler certaines informations confidentielles ou d'exécuter des manœuvres. Aucun ordinateur ne peut quoi que ce soit contre l'ingénierie sociale. C'est d'ailleurs en usant de cette tactique que la bande des *Hacking for Girlies* parvint à embarrasser le *New York Times* en piratant le frontispice de leur version électronique. Ils avaient envoyé un courriel sec à des administrateurs-réseaux qui leur intimait l'ordre de fournir illico certains mots de passe. Astuce qui fonctionna (Penenberg, 1998).

Bien que l'ingénierie sociale soit peu impressionnante d'un point de vue *hacker*, il conduit pourtant à des intrusions bien réelles.

8- Le *hack hacktiviste* (d'intrusion)

A l'origine du *hacktivisme* (contraction des mots *hack* et activisme) : la cause. Si l'activiste préconise l'action directe pour aider sa cause, le *hacktiviste* préconise le *hack*. L'accomplissement informatique peut devenir une arme redoutable. Par exemple, un *hacker* militant contre les organismes génétiquement modifiés (OGM) pourrait faire un casse dans le réseau informatique d'une compagnie céréalière dans le but de ralentir sa production. Les *hacktivistes* qui piratent des pages web sont animés des mêmes motivations. En 1998, deux bandes (*OLM* et *HARP*) ont uni leurs efforts pour en finir avec le site officiel du *Ku Klux Klan*. Après des semaines de travail, il parvinrent à déjouer le coupe-feu (*firewall*) et laissèrent le message suivant sur le frontispice : « Votre site et tous les comptes associés ont été jugés et effacés pour cause de crime contre l'humanité » (Dujay, 2000).

Le *hacktivisme* c'est devenu une affaire sérieuse. Le très célèbre *Cult of the Dead Cow*, un groupuscule de fanatiques du réseau qui font dans le *hacking* sérieux depuis 1984, sont à préparer *hacktivism.org*, un site dont ils veulent faire la ressource numéro 1 pour les *hacktivistes* du monde entier. Enfin, pour tous ceux qui partagent l'idéologie libertaire du *Cult*. La mondialisation des échanges commerciaux, les OGM, les droits de l'homme, la chasse aux phoques, l'équité d'emploi, la démocratie, la liberté d'expression, l'anonymat en ligne, la religion... Les causes sont innombrables (McKay, 1998).

Stanton McCandlish, directeur de programmes à la très célèbre *Electronic Frontier Foundation*, est catégorique : « Le futur du activisme est sur le net » (Richard, 1999). La *scène hacktiviste* s'organise. Oxblood Ruffian, un élément dangereux du *Cult*, a travaillé avec les mythiques *Hong Kong Blondes*, un groupe de dissidents chinois en colère. En 1998, ils ont infiltré police et réseaux de sécurité pour ensuite établir des preuves compromettant plusieurs politiciens véreux. Des actions tranquilles qui ont conduit aux condamnations bien réelles de plusieurs politiques chinois tandis que les *hacktivistes* s'évaporaient. Les

gouvernements du Mexique, de l'Indonésie et de l'Inde ont aussi été la cible de *hacktivistes* qui leur ont mené une guerre d'usure aux conséquences désastreuses, tant pour leur image dans le monde que pour la crédibilité de leur pouvoir. Des systèmes court-circuités, de l'information qui ne circule plus, des parcs informatiques saccagés, d'importantes pages web piratées... Et toujours en filigrane ces *hacktivistes* que plus rien n'arrête (Penenberg, 1998).

« Nos membres sont plus vieux, politisés et extrêmement compétents » affirme Oxblood Ruffian (Dufresne, 1999). C'est le retour aux grands élans des années 1970, sauf que cette fois-ci les moyens techniques ne manquent plus. Les *hacktivistes* ont en face d'eux un adversaire lourd et incapable, constitué de techniciens à la petite semaine, pas toujours intéressés à défendre les intérêts de leur employeur. *Milw0rm*, une bande qui a causé bien des soucis à un laboratoire de recherche nucléaire Indien (en plus de faire un casse terrible dans un laboratoire américain abritant un accélérateur de particules), a toujours agit impunément. Un membre se moque : « Ils ne paient sûrement pas leurs employés assez cher. Là-bas, vous obtenez un travail de 50,000$ pour un job qui en vaudrait 150,000$ » (Dufresne, 1999).

A la guerre comme à la guerre, chacun choisit son camp et la véritable compétence se trouve de l'autre côté. Au dire de certains observateurs, l'écart entre les niveaux de compétence est absolument quantique. Les *hacktivistes* ne cachent plus leur arrogance. Un ancien de la DST compare : « Nous sommes revenus à l'heure de la bande à Bonnot. Quand les gangsters roulaient en voiture et que la police était à pied » (Dufresne, 1999).

Le champ d'action est vaste aussi. Le réseau des réseaux (Internet), c'est 418 millions d'internautes en 2002 éparpillés sur les cinq continents. Certaines adresses supportent de forts achalandages. Les trois sites les plus fréquentés dans l'ordre :

1- Yahoo.com	*36,400,000 de visites par jour*
2- Msn.com	*32,748,000 de visites par jour*

3- Msn.com *32,748,000 de visites par jour*

(Jupiter Media Metrix, 2002)

Pirater une adresse aussi importante c'est rejoindre un immense public. Tant et aussi longtemps que le webmestre n'a pas repris le contrôle de son site, le *hacktiviste* peut commettre impunément le plus effronté des messages. Suffit d'être assez malin pour se retirer sans laisser de traces. L'effet est aussitôt exponentiel. Selon la gravité du coup d'éclat, les médias sur le net font écho et propagent la nouvelle. Il existe même des sites d'information qui se spécialisent dans l'archivage de ces attaques en copiant les pages piratées dont les très populaire www.antionline.com.

Le 30 janvier 1999, le Front National reçut la visite de *Raptor 666*, un *hacker* qui disait en avoir ras-le-bol des discours de Jean-Marie Le Pen. Il retoucha donc la page d'accueil. Pendant plusieurs heures, les internautes ébahis purent contempler une photo de monsieur Le Pen, le menton dressé et barré de l'inscription : « Cet homme incarne une valeur... le racisme ». Le reste du site fut tout bonnement effacé, ce que Raptor 666 nomma, un brin amusé, sa « solution finale » (Latrive, 1999).

En septembre 1998, une bande appelée les *Hacking for Girlies* s'empara de la version électronique du *New York Times*. Elle tapissa alors le frontispice de photos porno et de propos haineux, laissant la rédaction perplexe. Des jeunes très compétents qui se servirent d'une technique appelée le *remote root buffer overflow* pour accéder aux données du serveur après avoir facilement obtenu les mots de passe par courriel. Un reporter du magazine *Forbes* parvint à retracer deux des membres de cette bande (toujours en cavale d'ailleurs) qui acceptèrent de le recevoir à condition qu'il respecte leur anonymat. Pourquoi avoir attaqué le *New York Times*? A cette question ils répondirent, sur un ton détaché, qu'ils s'ennuyaient et ne s'entendaient pas sur le film à regarder ce soir-là. Ils s'étaient donc saisis de leurs bécanes pour lancer une attaque qui coûta en chiffres réels plusieurs centaines de milliers de dollars (Penenberg, 1998).

De tels piratages sont légions chaque année. Ce sont les *defacings.* Le site www.attrition.org a recensé 5 822 cas de defacings importants en 2000 contre 3746 en 1999. Les statistiques de 2000 ne sont pas encore parfaitement compilées. Mais celles de 2001 promettent de briser tous les records. Dans la seule journée du 30 avril 2001, 150 piratages ont été signalés aux autorités policières américaines. Le *hacktiviste* choisit ce terrain pour cause, car il oblige sa victime à reconnaître sa défaite. Mieux, il l'affiche au vu et au su du monde entier.

Antionline.org répertorie 200 cas de piratage parmi les plus spectaculaires. Une constante dans cette forme de *hacktivisme* : le geste est chaque fois revendiqué. Ces messages laissés en ligne constituent donc une référence de première main dans la démarche du journaliste qui cherche un sens (intention) au geste. Mais ces messages ne sont pas toujours univoques. En 1998, le site promotionnel du film *Titanic* a été retouché de l'inscription suivante : « Certaines compagnies n'apprennent pas de leur premier *hack*... Maintenant, elles coulent encore ». Peu de temps après, c'était le tour *d'Anglefire.com* : « Tout le monde sait que pour *hacker* une page il faut utiliser le jargon *hacker* ». De tels messages s'apparentent à des signatures sans œuvre, comme les témoignages de ces guerres de territoires que se livrent les gangs de rue à coups de graffitis maladroits (Lemos, 2001).

Mais qu'il existe ou non des *hacktivistes* sans cause, cela n'empêche pas l'avènement de créatures fantastiques. Seule la puissance du *hack* compte, car c'est elle qui devient objet de culte, qui inspire la peur comme l'attirance, qui enrage les autorités et qui capte l'attention dans l'actualité.

Chapitre 2 - Logique de l'iconographie *superhacker* dans la presse

Ce second chapitre examine les causes et les impacts de la tolérance du journaliste vis-à-vis du surnaturel *hacker*. D'une part le journaliste est forcé d'évaluer la qualité d'un *hack* en fondant son analyse sur des apparences. Puisque les causes du *hack* restent invisibles et/ou soumises à supputation, les symptômes demeurent le seul matériel avec lequel le journaliste peut travailler pour établir son jugement. D'autre part, cette tolérance conduit inévitablement à la création d'icônes *superhacker* puisque le *hack* s'impose comme l'expression d'une puissance surnaturelle. Pour illustrer à la fois ces causes et ces impacts, je cite les cas de Tannenbaum, Valor et *Mafiaboy*, trois icônes *superhackers* qui ont fait les manchettes entre 1998 et 2000.

1- L'icône *superhacker*

> « Je voudrais me marier avec lui... - Oren, seize ans, Israélienne » (Latrive, 1998).

Ehud Tannenbaum plaisait. Les jeunes filles le trouvaient craquant. Ses professeurs, brillant. Les journalistes, remarquable. Coqueluche de l'année 1998, cet Israélien de dix-huit ans s'était attiré les plus beaux compliments en pénétrant quelques ordinateurs présumés inviolables du Pentagone, du *Naval Undersea Warfare Center* et de plusieurs autres nœuds sensibles du dispositif de sécurité américain. Qu'il fallut mobiliser une coûteuse *special task force* pour le capturer, que l'affaire paniqua le gouvernement américain au point de lui faire dépenser illico deux milliards de dollars supplémentaires pour assurer la défense électronique du pays, que l'adolescent ravagea plusieurs des domaines .mil (réservés à l'armée) les plus importants d'Israël, tout ça n'empêcha pas Benyamin Netanyahou, qui avait lu les journaux, de dire à propos du jeune *hacker* impudent: « Il est diablement bon... » (Glave, 1998). Tannenbaum devint même le porte-parole d'un fabricant d'ordinateurs israélien (EIM). Le concept:

« Pour arriver loin, tu as besoin du meilleur équipement! » (Avishaï Gendelman, responsable de la publicité chez EIM explique: « La campagne a eu un effet positif sur notre image et sur nos ventes » (Le Monde, 1999). Arsène Lupin pour vendre du matériel diront certains observateurs. « C'est comme si *Smith & Wesson* faisait une pub avec un meurtrier » - Shuki Preminger, PDG de Babylon (Latrive, 1998).

Un millier de serveurs publics profanés, des dizaines de sites détruits, 120,000 comptes d'accès usurpés, 400 domaines militaire (.mil) fracturés, un nombre incalculable de Chevaux de Troie abandonnés aux quatre vents, des coûts en réparations frisant les millions de dollars et John Hamre, vice-directeur du Pentagone, dans tous ses états: « (Les ordinateurs de mon institution ont fait l'objet) de l'attaque la plus systématique et la plus organisée à ce jour » (FedCIRC Report, 1999). Jusqu'à Kenneth H. Bacon, sous-secrétaire américain de la défense, qui soupçonnant un moment un coup des Irakiens, déclara : « Nous entrons dans une époque où nous devons à nouveau être sur la brèche pour défendre notre pays contre des ennemis équipés d'ordin*ateurs* » (Le Monde, 1999). C'est le bilan de l'épopée Tannenbaum. Une épopée qui se termina le 16 mars 1998, soit au terme d'une singulière chasse à l'homme cybernétique impliquant quatre agences spécialisées dans la cybertraque et qui dura un mois. Ce jour-là, trente agents du FBI en armes soutenu par un nombre égal de policiers israéliens se saisirent d'un adolescent souriant. Un garçon paresseusement installé devant un 486 bon marché, cadeau offert par sa mère le jour de ses quinze ans (Latrive, 1998).

Arrêté, puis relâché dans l'attente d'instruction d'un quelconque procès, (qui n'aboutira finalement jamais) le garçon expliquera à un journaliste : « Euh... j'aimais le chaos et je détestais les organisations... » (CNN News, 1998) C'est que Tannenbaum n'avait vraisemblablement rien d'un *hacker* chevronné. Rendu à l'armée pour son service militaire, Israël n'a pas jugé bon de profiter des pouvoirs surnaturels du garçon. Ils l'ont plutôt affecté à l'infantrie. Après avoir glané ici et là quelques astuces de réseautique et surtout après avoir ramassé tout un kit de logiciels de piratage programmés pour le plaisir par d'autres (sur

des sites de WAREZ), Tannenbaum aura simplement profité des brèches oubliées par des administrateurs-réseaux peu consciencieux. Après avoir entraîné deux autres jeunes (localisés en Californie quelques jours avant sa capture) dont il était le guide spirituel, l'adolescent reconnaîtra s'être bien amusé au dépend du dispositif de sécurité supposé le plus puissant du monde (Mauriac, 2000).

Si la puissance *hacker* de Tannenbaum reste à démontrer, l'icône *superhacker* se porte bien. Au moment d'écrire ces lignes, Tannenbaum termine son service militaire alors que producteurs et éditeurs se bousculent pour acheter les droits d'une histoire qui va vendre. Une histoire où le meilleur rôle ne sera plus tenu par un criminels dangereux comme dans les films *The Net*, *Hackers, Takedown* ou *Operation Swordfish*, mais par un *hacktiviste*, sorte de rebelle avec une cause (AP, 1999). Qu'importe la preuve, place à l'icône.

Icône vient du grec ancien *eikonion.* Sa signification part de l'aboutement des concepts **image** et **ressemblance**. Il s'appliquait autrefois aux images religieuses ou plus précisément, à une transfiguration de la matière en une autre image chargée de symboles, voire une épiphanie (manifestation du sacré). En 1938 cependant, Charles S. Peirce proposait une théorie générale de l'icône :

> L'icône est un signe qui possède un rapport de ressemblance avec la chose qu'il représente. Les signes iconiques sont des représentations analogiques détachées des objets ou phénomènes représentés. L'icône est un signe qui posséderait le caractère qui le rend signifiant, même si l'objet n'existait pas (Peirce, 1978).

Dépendamment des types de rapports, Peirce identifie trois sortes de relations possibles entre le signe et la chose dont il est le signe : **indice**, **icône** et **symbole**.

L'indice est le signe qui entretient un rapport réel avec la chose qu'il signale. Il est la trace d'un phénomène comme l'empreinte de pas sur la neige l'est du passage. Toutefois, il n'est pas une preuve infaillible. L'indice est un

symptôme qui donne l'impression qu'une chose existe vraiment. Certes un poing brandi représente un signe de colère qui augure le coup mais il n'est pas la preuve que ce coup sera réellement porté. Son interprétation relève du débat.

D'autre part, **l'icône** est un signe qui possède un degré de ressemblance avec la chose dont elle est supposée composer la représentation. Elle est une analogie imaginaire détachée de la réalité. Plus précisément, l'icône n'a pas besoin de l'existence du réel de son référent pour exister. Dans le cas d'un mari qui adresse un poing à son épouse, l'icône créée pourrait par exemple servir à dépeindre le batteur de femme moyen. Cela même s'il s'agit d'une blague.

Le **symbole** est un signe de nature arbitraire proposé et/ou accepté par une ou plusieurs personnes. Ce signe constitue une véritable rupture avec le réel du référent. Le mot *hacker* par exemple n'a aucun rapport graphique ni phonétique avec l'individu qu'il désigne. La compréhension de son symbole nécessite l'adhésion à des codes, des conventions et des langages. En revanche, le symbole a besoin d'un interprète pour exister. Il peut s'agir d'une bouille, d'un discours, d'une signature ou de toute autre marque se rapportant au jeu de l'interprète.

Dans *La communication par la bande*, Daniel Bougnoux examine les rapports de Peirce et en propose une version plus colorée. Chez lui l'indice et l'icône représentent le pôle de l'attachement au référent réel tandis que le symbole représente le pôle du détachement. En effet, l'indice et l'icône nous enchaînent au phénomène alors que le symbole nous place à distance (Bougnoux, 1991).

En 1957, Rolland Barthes pressentait la confusion (confusion pris dans son sens commun : action de confondre quelqu'un ou quelque chose pour quelqu'un ou quelque chose d'autre) comme un principe directeur dans l'iconographie des mythes (iconographie prend un sens biographique chez Barthes). Les mythes, vecteurs d'icônes, nous débordent au quotidien et

traduisent une « parole ». Barthes pense que la parole mythique est un message et qu'elle est beaucoup plus qu'un fait oral. Il s'explique :

> (...) elle peut être formée d'écritures ou de représentations : le discours écrit, mais aussi la photographie, le cinéma, le reportage, le sport, les spectacles, la publicité, tout cela peut servir de support à la parole mythique (Barthes, 1957 : 182).

Chez Barthes, le mythe précède et entretien l'icône.

> Le mythe ne cache rien et il n'affiche rien : il déforme; le mythe n'est ni un mensonge, ni un aveu : c'est une inflexion. (...) Nous sommes ici au principe même du mythe; il transforme l'histoire en nature. On comprend maintenant pourquoi aux yeux du consommateur de mythes, l'intention, l'adhomination (ad hominem) du concept peut rester manifeste sans apparaître pourtant intéressée : la cause qui fait proférer la parole mythique est parfaitement explicite, mais elle est aussitôt transie dans une nature; elle n'est pas lue comme mobile, mais comme raison (Barthes, 1957 : 202).

Barthes décrit le mythe :

> La sémiologie nous a appris que le mythe a pour charge de fonder une intention historique nature, une contingence en éternité. (...) Ce que le monde fournit au mythe c'est un réel historique, défini, si qu'il faille remonter, par la façon dont les hommes l'ont produit ou utilisé.; et ce que le mythe restitue c'est une image naturelle de ce réel. (...) le mythe est constitué par la déperdition de la qualité historique des choses : les choses perdent en lui le souvenir de leur fabrication. Le monde entre dans le langage comme un rapport dialectique d'activités, d'actes humains : il sort du mythe comme un tableau harmonieux d'essences. Une prestidigitation s'est opérée, qui a retourné le réel, l'a vidé d'histoire et l'a rempli de nature, qui a retiré aux choses leur sens humain de façon à leur faire signifier une insignifiance humaine. La fonction du mythe c'est d'évacuer le réel : il est, à la lettre, un écoulement incessant, une hémorragie, ou si l'on préfère, une évaporation, bref une absence sensible (Barthes, 1957 : 216).

Au siècle dernier, la théorie évolutionniste considérait le mythe comme une « tentative intellectuelle », une pensée confuse, primitive, embryonnaire et

irrationnelle. Le mythe, et de là provenait le problème, ne pouvait souffrir aucune analyse capable d'éclairer la réalité d'un phénomène. A propos des ethnologues du 19ième siècle, Christian Vanden Berghen écrit :

> Il faut savoir que les ethnologues de l'époque n'avaient, le plus souvent, eu aucune relation directe avec les populations qu'ils étudiaient. Tout ce qu'ils savaient leur venait des récits des missionnaires ou des explorateurs (Berghen, 2000).

L'icône *superhacker* se bâtit sur d'apparentes données techniques dont les symptômes constituent les seuls éléments discutables. Par conséquent, la gravité de ces symptômes demeure l'unique pièce à conviction qui peut être appelée pour démontrer ou réfuter qu'un *hacker* soit doté ou non d'une force surnaturelle. Vraisemblablement car l'opération reste du domaine du plausible et du débat. Qu'un débat aboutisse à un large consensus, cela n'est pas gage d'une juste analyse. Plusieurs canulars *hacker* spectaculaires ont eu cours dans une presse concertée. L'affaire Christian Valor désenchanta plusieurs journalistes en 1998 qui perdirent ouvertement la face. Adam Penbenberg de *Forbes* et Steve Silberman de *Wired News*, supposés experts de la chose *hacker*, ont dû présenter leur pathétique *mea culpa* après s'être fait rouler par l'imposteur. Les gens de *Popular Mechanics* ont décidé de se la jouer *low profile* tandis qu'une trentaine de journalistes éparpillés dans plusieurs publications de premier plan, dont aussi *Newsday's* (Matthew McAllester) et la station de télévision canadienne *Discovery Channel*, les imitèrent (Welch, 1999).

2- Le débat de la preuve

Entre le 6 et le 14 février 2000, un certain *Mafiaboy* paralysait tour à tour les sites de CNN, Amazon, eBay, Yahoo et plusieurs autres fleurons de l'économie numérique américaine. En quelques jours, les méfaits du *hacktiviste* auraient coûté 1.7 milliards de dollars. Les victimes hurlèrent. FBI et GRC se lancèrent dans une filature qui aboutit à la capture d'un jeune Montréalais de quinze ans qui nia immédiatement sa culpabilité. Le geste? *Mafiaboy* se serait

emparé de soixante-quinze ordinateurs éparpillés au Canada, aux États-Unis, au Danemark et en Corée. Après y avoir installé un logiciel *IMP* programmé par une connaissance américaine (*Sinkhole*), il aurait donné l'ordre a sa petite armée d'ordinateurs de rafraîchir encore et encore les adresses des portails concernés jusqu'à ce que la catastrophe se produise : le débordement des capacités de traitement (Burke, 2000). Un geste à la portée de n'importe quel quidam de l'informatique, à condition d'en accepter le risque.

La presse internationale débarqua à Montréal pour contempler la présumée créature. Mais la justice canadienne eut tôt fait de freiner son élan avec sa Loi de la protection sur les mineurs. Une conférence de presse s'organisa. Mais qui était donc *Mafiaboy*? « C'est un garçon de quinze ans qui va à l'école » déclara laconiquement Yves Roussel de la section des délits commerciaux à la GRC. Quand pourrons-nous le voir ? « Il faudra attendre qu'il passe devant le juge pour ça » (Myles, 2001).

Alors que tout le monde se préparait à repartir, des élèves d'une école de Pierrefonds (Île de Montréal), souhaitant faire une bonne blague à l'un de leurs amis, contactèrent des journalistes. Ils les informèrent que le fameux *Mafiaboy* se trouvait parmi eux et ils se disaient prêts à le livrer. Des dizaines de journalistes, photographes et observateurs assiégèrent alors la résidence des parents dans l'espoir d'obtenir une entrevue (Dubé, 2000). Un père se montra pour protester tandis que la mère tentait d'expliquer que son fils n'avait rien à voir avec cette histoire. On refusa de les croire. La *Presse Canadienne* (PC) n'attendit pas et publia toutes sortes d'informations sur le caractère et les habitudes de vie du jeune pirate et de sa famille. Les écoliers pouffèrent vite de rire et confessèrent le canular, ce qui embarrassa tout le monde (Myles, 2001).

Finalement, le vrai *Mafiaboy* fit son apparition en cour quelques mois plus tard. La presse contempla alors un garçon très peu sûr de lui et manifestement repentant de son geste. Il plaida maintenant coupable à 56 des 66 chefs d'accusation et son avocat (Yan Romanowski) proposa une peine de prison de deux ans avec sursis agrémentée d'une amende de 1000$. Pourquoi avoir

commis un tel geste? L'adolescent ne sut l'expliquer lui-même. Erreur de jeunesse avança alors l'avocat (Dubé, 2000).

Les Chroniques de Cybérie écriront :

> La presse spécialisée reste curieusement muette sur ces nouveaux développements, tant du côté du *Hacker News Network*, de 2600, de *Attrition.Org*, ou de *HackInTheBox*. On se rappellera que les «purs et durs» du *hacking* (...) ne prisent pas les exploits du genre perpétré par *Mafiaboy* car ils s'effectuent à l'aide de «bombes logiques» disponibles à quiconque sur Internet, et ne font preuve d'aucune créativité ou d'adresse technique (Cloutier, 2001).

Avec un indice de puissance ridiculisé, il devint manifeste que *Mafiaboy* ne deviendrait pas une icône *superhacker*. Bien sûr, les historiens lui reconnaîtront la paternité d'un cataclysme qui ébrécha momentanément l'économie numérique américaine. En paralysant CNN, Amazon, eBay, Yahoo, etc., le pseudonyme devenait le symbole de l'ultime fragilité d'un Internet déjà passablement malmené. Le *dot com blues* (la chute en domino de nombreuses compagnies .com) finissait de purger le réseau de plusieurs utopies d'investisseurs (Broersma, 2000). Mais faute d'indice permettant d'imaginer qu'il ait pu être possédé d'une puissance surnaturelle, *Mafiaboy* resta un pseudonyme de 8 lettres sans véritable forme humaine. *Mafiaboy*, c'était comme un virus informatique s'autorépliquant mécaniquement jusqu'à la catastrophe annoncée.

3- La démarche professionnelle du journaliste

La formation d'une icône *superhacker* reste un événement rare. Il existe dans le monde tant de *script kiddies*, tant de vandales, tant de *hackers* capables d'applications et surtout tant de gestes assimilables à du *superhacking* que seule une poignée d'individus, les dieux, sont consacrés icônes *superhacker*. Cette rareté est à la fois obligée mais aussi réjouissante pour les médias de masse puisque c'est ainsi que naît la nouvelle. Le journaliste ne crée pas la nouvelle, il la choisit. La rareté est d'intérêt public. Elle s'inscrit comme un changement vis-

à-vis de l'actualité routinière. Parce que le phénomène *hacker* se répand un peu plus chaque année, la démesure de ses icônes gagne en importance. Ainsi, l'intervention du journaliste, qui se compare à celle du critique, consiste non pas à inventer le *superhacker* mais à le choisir parmi une foule de prétendants. Le journaliste Scott Rosenberg confirme : « Il fallait cimenter quelques mythes populaires. Il existait sûrement des *hackers* à donner le frisson, gros et dangereux » (Rosenberg, 1995).

Mais si le journaliste choisit ses icônes, il est aussi contraint à décider de l'archéologie d'un *hack* en procédant d'un raisonnement par récurrence basé sur des observations. Ces observations sont celles de symptômes et non de causes. En résumé, le *hack* est le symptôme et le geste *hacker* est sa cause. Comme le médecin clinique, le journaliste opère une démarche professionnelle principalement axée sur la manifestation du symptôme. Cette démarche est à la fois double et simultanée : représenter des faits et des idées. Dans le Guide de déontologie de la Fédération professionnelle des journalistes du Québec, il est mentionné :

> Les journalistes préféreront toujours la représentation de la réalité telle quelle à sa reconstitution par divers artifices. Les reconstitutions d'événements et les mises en scène peuvent néanmoins être utilisées en journalisme afin d'illustrer et de soutenir un reportage, mais avec prudence car le danger de tromper le public existe. Avant d'y recourir, les journalistes doivent évaluer s'il s'agit de la meilleure ou de la seule façon de faire comprendre une situation au public. Le public doit alors être informé clairement qu'il s'agit d'une reconstitution ou d'une mise en scène. La reconstitution se limitera à reproduire le plus fidèlement possible les faits, les opinions, les émotions qui entourent l'événement recréé (Guide de déontologie, 2002).

Malgré la bonne foi de la profession, le journalisme objectif reste une utopie.

> En ce sens, la notion d'objectivité n'est pas uniquement liée à l'interprétation des faits. Dans le processus d'élaboration de la nouvelle, il y a d'abord un processus de sélection des sujets, des objets, des sources

> et du niveau d'information souhaité ainsi que des faits significatifs. Selon les tendances politiques et idéologiques de chaque équipe éditoriale, les critères mobilisés à cette étape ont varié (Guide de déontologie, 2002).

En revanche, le journaliste se donne le devoir de faire circuler de l'information coûte que coûte. Le Guide de déontologie explique :

> Les journalistes ont le devoir de défendre la liberté de presse et le droit du public à l'information, sachant qu'une presse libre joue le rôle indispensable de chien de garde à l'égard des pouvoirs et des institutions. Ils combattent les restrictions, les pressions ou les menaces qui visent à limiter la cueillette et la diffusion des informations (Guide de déontologie, 2002).

Mais quand le journaliste construit une représentation du geste *hacker*, il s'adonne à l'induction. Pour Paul McMasters, ombudsman au *Freedom F*orum (le plus important organisme de presse agissant pour la promotion de la circulation de l'information aux États-Unis), il ne fait aucun doute que la réalité du geste *hacker* échappe entièrement aux journalistes. Les circonstances de celui-ci resteraient invisibles. Les journalistes en seraient donc réduits à imaginer des gestes de manière à ce que ceux-ci soient conséquents avec l'ampleur de leurs effets. Selon lui, cela expliquerait pourquoi les cinq dernières années ont vu des couvertures médiatiques plus moribondes les unes que les autres. McMasters s'inquiète :

> Tout cela aura un impact inévitable sur les politiques de nos gouvernements et sur la perception du grand public. Quand les dates de tombées sont perpétuelles et que l'anxiété de trouver des scoops à tout prix jour après jour devient plus forte que le professionnalisme, le journaliste arrive difficilement à faire son travail correctement. (...) Le *hacking* ne peut pas être traité de la même façon qu'une autre nouvelle (Silberman, 1999).

L'icône *superhacker* est une anomalie qui prend place dans le corps social mais aussi une créature *ad hoc* qui suscite l'intérêt quelques instants pour cesser ensuite de faire la manchette sitôt maîtrisée ou retraitée. Elle se figera alors en une même collection de souvenirs intelligibles dont les archives de presse

constitueront l'un des pans importants. La caractéristique du mythe est la déperdition de la qualité historique des choses dont il peut être tenu responsable. Les représentations proposées par la presse deviennent donc un réel historique dont l'interprétation est soumise au débat. Car le mythe, comme Roland Barthes l'a souligné, est « soumis à une lecture inductive » (Barthes, 1957).

En avril 2000, un avion-espion américain s'écrasait en Chine, provoquant un énorme brouhaha diplomatique. Tandis que les diplomates tentaient de s'accorder sur la formulation des excuses états-uniennes, une bande de *hacktivistes* chinois commença à invectiver une bande rivale américaine. Tout cela dégénéra en une guerre de sept jours. L'objectif : l'anéantissement d'un maximum de sites web hébergés dans des serveurs situés sur le territoire du pays adverse. Les *hacktivistes* américains remportèrent la première bataille du mardi par le score de 23 à 18, résultat qui fit les manchettes. Interrogés par *Wired News*, les *hacktivistes* chinois jurèrent de se venger le lendemain. Cette olympiade *hacktiviste* sino-américaine occasionna beaucoup de désagréments chez d'honnêtes serveurs qui n'avaient rien à y voir. Ce qui fit dire à un journaliste de *Attrition.org* : « C'est une compétition entre mecs pour savoir qui a la plus grosse. Une compétition aiguillonnée par des soi-disant journalistes, désireux de faire monter la sauce » (Launet, 2001).

Fort justement, les journalistes choisirent de rapporter toutes sortes de déclarations incendiaires, dont celle de Wes Marsh, un sénateur républicain, qui fit le tour du monde : « Un ordinateur portable peut causer plus de problèmes qu'une bombe nucléaire » (Latrive, 2001). Un autre sénateur, Bob Bennett, déclara que les réseaux de communication étaient à l'Amérique ce que le réseau routier était à l'Empire romain: « Ils doivent être protégés des barbares et des Wisigoths qui ont saccagé Rome » (Latrive, 2001). Une déclaration erronée : Rome n'avait pas été saccagé par les Wisigoths mais bien par les Huns.

Alexis Bautzmann, chercheur à l'Université Aix-en-Provence, se moque : « Ça ne concerne que des sites web, c'est insignifiant. » En effet, lorsqu'un site communiste est défloré par des *hackers* américains, le méfait est nettoyé en

quelques heures. Il poursuit : « Ces affaires pas très importantes sont instrumentalisées par le pouvoir politique pour pointer le futur grand ennemi potentiel dans le cyberespace, la Chine » (Latrive, 2001).

Si des gens comme Bautzmann critiquent le travail de la presse, faut-il cependant reconnaître que celle-ci est égale à elle-même : la démarche professionnelle du journaliste l'oblige à rapporter les nouvelles d'intérêt public. Le journaliste, comme le suggère le guide de déontologie, doit représenter les faits mais aussi les opinions et les émotions qui entourent l'événement. Il les tirera des communiqués de presse, des déclarations, des témoignages, des faits techniques, bref de toutes les données initialement observables. S'il effectue un suivi plus en profondeur de l'événement, il cherchera les pièces à conviction confirmant l'hypothèse du *superhack*. Au terme de cette recherche, il aura en sa possession une kyrielle de symptômes commentés par différentes personnes impliquées dans l'événement (Vautravers, 1991). Le résultat de son travail d'enquête conduira à une représentation du *hacker* et de son geste. Car justement, en pesant les discours et comparant les faits techniques, le journaliste opère finalement un jugement de valeurs. Étant donné que la cause du *hack* ne peut être filmée (au sens propre et figuré), il sera toujours forcé de recourir à une reconstitution pour en faire la représentation. Il s'agira d'une induction validée par la comparaison des données recueillies (symptômes) et des conclusions qui en ont seront tirées. La procédure demeure un exercice de vraisemblance. Le *hacking* est d'ailleurs une activité qui encourage toutes les interprétations. Même si le journaliste se retranche derrière une position apparemment solide vis-à-vis de son objet *hacker*, son argument appartient au domaine du plausible.

Il est impossible pour le journaliste de décider de la justesse absolue d'un *hack*. Ses conditions de formation sont absolument indécidables. Même si le journaliste assiste à la réalisation d'un *hack* en direct, il n'aura sous les yeux que la représentation dudit *hack*. En effet, le *hacking* est une activité mentale dont l'ordinateur ne constitue que l'interface et l'outil. L'écran n'affiche pas la cause du *hack* mais son symptôme lui-même. La base de la conception, de l'organisation ou de la manœuvre d'un programme reste une projection mentale. C'est

d'ailleurs pourquoi les machines ne *hackent* pas. D'autre part, il est aussi plausible que le *superhacker* simule sa puissance *hacker* comme cela s'est produit dans l'affaire Valor.

Durant le DefCon 2000, l'événement *hacker* de Las Vegas auquel je faisais référence au premier chapitre, un certain Kevin Poulsen débarqua pour donner une conférence. Le sujet : mise à jour sur les méthodes de capture du FBI. Ancien *phone phreaker* repenti qui se rendit célèbre en 1994 pour avoir réussi à déjouer un concours radiophonique et ainsi remporter une Porsche 944, Poulsen décida de présenter un épisode de *Unsolved Mysteries* en guise d'introduction. Il s'agit d'une émission américaine à sensations qui mêle des topos de journalistes à des reconstitutions jouées par des acteurs. De l'énigmatique Poulsen, l'émission dressait le portrait d'un dangereux criminel que l'Amérique avait bon de redouter. La pastiche était grosse : un adolescent boutonneux, le dos voûté, les doigts surexcités, le regard aliéné et qui s'affairait devant un ordinateur à pénétrer des systèmes inviolables. L'éclairagiste avait même bricolé une aura surnaturelle autour de la créature qui ne manquait pas d'être remarquée dans la pénombre de la chambre. Les invités du DefCon éclatèrent de rire. Aujourd'hui converti à l'éditorial, Poulsen demeure cependant un membre du *hall of fame* (temple de la renommée) *hacker* et son nom reste associé à la petite chronologie du délit informatique en ligne. Si l'émission a réussi à faire rigoler les gens du DefCon, n'en demeure pas moins que la reconstitution était plausible. Les producteurs avaient simplement caricaturé l'icône *superhacker* telle qu'elle existait dans l'imaginaire médiatique (Fine, 1995).

4- Le reportage

Reportage et reporter sont des termes tirés de l'anglais *to report*. Le reporter rapporte le récit de ce qu'il a personnellement vu, entendu et découvert. Il recueille des informations, expose les faits et tire des conclusions. Il devient ainsi un auteur-acteur dont le travail de recherche cautionne l'authenticité des

faits. Constant Vautravers, journaliste émérite, rapporteur du prix Pinotel, membre de l'Académie de Marseille et président de l'Association Régions Presse Enseignement Jeunesse, souligne : « Plus avant que le simple récit d'un événement, le reportage se hausse d'un cran lorsqu'il devient enquête ou - d'un terme à la mode plus valorisant - investigation » (Vautravers, 1991). Il considère que la forme et l'habillage d'un reportage sont fonction du « tempérament » (marque) du journaliste ainsi que de son média et de ses orientations stratégiques. Mais s'il est autorisé à y aller d'une impulsion personnelle, il doit cependant respecter un certain nombre de règles :

> Les faits doivent être clairement établis et vérifiés, joignant à l'observation du journaliste les témoignages qu'il recueille avec impartialité pour être aussi complet que possible. L'information ne parvient pas « toute cuite », il faut aller la chercher. La compétence du journaliste, l'appel à la documentation, aux banques de données, permettent ensuite d'élargir le champ, d'apporter une explication, d'amorcer une analyse ou un commentaire (Vautravers, 1991).

L'écriture n'est pas neutre. Hubert Beuve-Méry, le fondateur du journal Le Monde, écrivait en 1970 : « Informer un homme, lui fournir les éléments d'une conviction ou d'un jugement est toute autre chose que lui procurer un chapeau ou une paire de chaussures » (Tasca, 2000). En écrivant, le journaliste acquiert une position de médiateur : chaque mot, parole ou image pèse dans cette médiation. Il y a donc nécessité de procéder de manière à distinguer l'essentiel du secondaire, voire l'apparence de la réalité. Il doit choisir entre les faits ceux qui lui permettront d'assurer la justesse de ses conclusions. Par le fait même, il est contraint par sa déontologie professionnelle à mesurer l'impact et les conséquences de ses conclusions. Car si toute vérité est bonne à dire, le journaliste doit reconnaître qu'il opère un jugement de valeurs pouvant être débattu. Par jugement de valeurs, il faut entendre une opération qui consiste à estimer, apprécier ou accorder de l'importance à une personne, un processus ou un événement. Celui-ci s'obtient à partir d'observations et du croisement d'informations qualitatives et/ou quantitatives traitées à l'intérieur d'un processus s'apparentant à la prise de décision (Reboul, 1999).

Jean-Claude Picard, professeur au département de communication de l'Université Laval, rappelle que le premier journalisme était un métier d'opinion. Au 19ième siècle, le journaliste était un acteur, voire un propagandiste ou un pamphlétaire. Ce n'est qu'au 20ième siècle qu'est apparu le rôle d'observateur prétendument objectif. Puisque les journaux devenaient des machines à générer des revenus obligées de plaire au plus large public possible, l'industrie développa des mécanismes de contrôle pour assurer la crédibilité de son objectivité (Bernier, 1997).

L'important journal français Ouest-France a adopté une « lettre de la Rédaction » qui pose quatre principes clés, lesquels sont imposés à tous leurs journalistes :

1 - dire sans nuire

2 - montrer sans choquer

3 - témoigner sans agresser

4 - dénoncer sans condamner

(Vulser, 2002)

Il n'existe pas un code d'éthique international qui régit les activités du journalisme. Pour exercer son métier, le journaliste doit simplement être accepté par un ordre ou une association de journalisme reconnus par l'industrie et qui se portera garant de son professionnalisme et de sa crédibilité. Comme à la boxe, le journaliste peut perdre sa licence. Aux États-Unis, la société *Investigative Reporters & Editors*, un organisme qui fait la promotion de l'excellence de la profession, propose le site www.reporters.org Ce carrefour incontournable répertorie et fixe les conditions d'éthique auxquelles le journaliste américain se voit soumis. Les conditions principales qui composent le code :

1- *Exactitude de l'information (vérification et comparaison des sources)*

2- *Respect de la vie privée*

3- *Objectivité du traitement*

4- *Subterfuge (le journaliste ne peut en user qu'en cas d'intérêt public)*

5- *Discrimination volontaire (rejeter ou retenir des faits)*

6- *Confidentialité des sources*

7- *Conflits d'intérêt*

(Reporter.org, 2002)

Dans le compte-rendu d'un débat organisé par la Fédération professionnelle des journalistes du Québec en juin 1997, le journaliste Marc-François Bernier souligne :

> Privés d'une connaissance absolue de la réalité, une limite inhérente à leur condition humaine, les journalistes doivent s'approvisionner à plusieurs sources d'information afin de communiquer une description du réel qui soit la plus complète et fidèle que possible puisque eux-mêmes ne possèdent pas toutes les connaissances nécessaires à une appréhension d'abord, mais surtout à une compréhension totale de la réalité sociale, économique, politique, scientifique et culturelle. C'est dans ce contexte que les journalistes ont recours à des sources d'informations, adjuvantes cognitives qu'ils sollicitent, ou par lesquelles ils sont sollicités, afin d'y puiser la connaissance partielle, et toujours partiale, qu'ils ne possèdent pas a priori (Bernier, 1997).

Bernier poursuit plus loin :

> L'information journalistique, ou la nouvelle, est alors considérée comme la transformation d'un événement - parfois tout à fait artificiel comme les conférences de presse ou les mises en scène - en un produit médiatique grâce au travail combiné des journalistes et de leurs sources d'information (Bernier, 1997).

En conclusion, le reporter infléchit fatalement sa représentation historique d'un événement car il l'appuie sur une démarche consistant à retenir et à rejeter des indices. Il devient alors créateur et vecteur de parole mythique au sens de Barthes. Le mythe est une raison, un principe, une persuasion. Le mythe *hacker* n'est pas une fausseté mais une vraisemblance fondée sur une inflexion. Quand

le reporter s'adonne au débat de la preuve du *hack*, il raisonne à partir de signes émanant du phénomène. Est donc *hacker* celui capable d'un *hack*. Or, l'icône *superhacker* est un jugement de valeurs établis à partir d'arguments qui reconnaissent l'aspect hautement exceptionnel du geste fondateur, c'est-à-dire le *superhack*. Le préfixe super signifie formidable, supérieur, surnaturel. Il attribue au mot qui le suit une qualité portée à un très haut niveau. Si le *hack* est une réalisation naturelle et conforme à l'ordre des choses, le *superhack* est une anomalie. Une étrangeté pouvant être interprétée comme le résultat de l'expression d'un pouvoir surnaturel. Le reporter défend ou rejette cette hypothèse en collectant des symptômes et contribue du même coup à alimenter, démolir ou cimenter le mythe. Ce faisant, il aboutit à la construction d'une icône plausible incarnant des pouvoirs mesurés.

Chapitre 3 - Kevin Mitnick : trois iconographies comparées

Les journalistes John Markoff, Jonathan Littman et Jeff Goodell ont chacun proposé une construction (iconographie) du personnage Kevin Mitnick en publiant respectivement les livres *Takedown*, *The Fugitive Game : Online With Kevin Mitnick* et *The Cyberthief and the Samurai*. Ces iconographies ont été tirées parfois à partir de faits reconnus par tous, parfois à partir d'éléments divergents. Dans ce troisième chapitre, j'explique comment chaque journaliste a procédé pour construire son iconographie à travers la sélection et l'abandon d'indices. En comparant ces iconographies, je démontre ensuite que si ces journalistes expriment de profonds désaccords sur les mobiles qui ont motivé Mitnick, ils s'accordent d'emblée pour lui reconnaître une force surnaturelle. Je critique finalement ces iconographies en soulignant leurs forces et leurs faiblesses vis-à-vis d'une conception plus modérée de la puissance *hacktiviste*.

J'ai d'abord retenu les reportages de Markoff, Littman et Goodell pour l'ampleur de leurs couvertures. Ces livres ont été écrits par des journalistes qui avaient déjà consacré de nombreux articles à Kevin Mitnick. Chacun d'eux possédait une vaste connaissance des faits entourant l'évolution et les circonstances de l'affaire. Il faut considérer leurs livres comme l'aboutissement d'un travail de longue haleine qui dura plusieurs années, et ce, souvent à temps plein. Leurs ouvrages sont régulièrement cités dans la presse comme ailleurs. Au cinéma par exemple, les scénaristes des films *Takedown* et *Operation Swordfish* ont puisé abondamment dans ceux-ci avant de soumettre leurs dialogues au découpage technique. Jim Thomas, du *Computer Underground Digest*, salue l'arrivée de ces trois livres : « Il existe relativement peu de livres sur *l'underground* qui fournissent une description aussi riche et une analyse aussi personnalisée tout en entraînant le lecteur avec une prose aussi vive » (Thomas, 1997).

D'autre part, il me fallait choisir des livres plutôt qu'une collection d'articles éparpillés dans le temps. Au fil des événements, il se produit un effet de maturation chez le journaliste. Cet effet entraîne une variation dans son propos. Il peut, par exemple, modifier son analyse à la lumière de faits parvenus jusqu'à lui de manière inattendue. Sa couverture s'en trouve ainsi modifiée suivant l'évolution de ses expériences et de sa connaissance du phénomène observé. D'autant plus que le phénomène évolue lui-même. En revanche, les livres que j'ai retenus ont été écrits à un moment où Mitnick avait été définitivement muselée. De telle sorte que ces journalistes ont aussitôt rassemblé leurs couvertures dans des livres qui se voulaient les bilans d'un phénomène supposé terminé.

Il faut cependant retenir que ces trois journalistes avaient le mandat d'accoucher de jugements de valeurs. Des jugements sur la force de Mitnick ainsi que sur ses mobiles. Appuyés par des couvertures serrées, Markoff, Littman et Goodell rivalisent de détails et d'arguments pour défendre la justesse de leurs iconographies respectives. Le principe d'iconographie prend ici la forme d'un portrait biographique de l'icône. J'ai donc choisi d'examiner comment chacun de ces journalistes avait procédé avant d'arriver à des conclusions définitives. Quels avaient été leurs contextes de recherche et de quelle démarche professionnelle avaient-ils procédé. En bref, étudier la procédure de mise en icône via la sélection et l'abandon de faits. Car nous l'avons vu au chapitre précédent (page 39), le journaliste ne crée pas la nouvelle. Il la choisit.

Rappelons que l'objectif de ce mémoire n'est pas de critiquer la démarche d'enquête propre au métier de reporter. La rigueur du journaliste, qui à travers les témoignages des acteurs, l'observation des symptômes et la collecte des éléments entourant l'événement, demeure une méthode acceptée par des générations de journalistes et internationalement reconnue. Je souhaite plutôt étudier les démarches privilégiées par ces trois journalistes pour ensuite remettre leur travail en contexte. Chacun d'eux a réalisé son enquête sur des mobiles personnels que je nommerai **biais du journaliste**. Ce biais est omniprésent dans tous les aspects de la profession, y compris chez moi-même qui par mon

expérience et mon analyse des faits *hacker* en est venu à développer une représentation modérée de la puissance *hacktiviste*. Il ne s'agit donc pas de critiquer les conclusions apportées par ces trois journalistes mais d'étudier comment ils ont procédé pour les atteindre. Ma critique se situe plutôt au niveau du point de vue que je compte adopter au prochain chapitre par rapport au phénomène du *hack* en lui-même en le dépouillant de son trait surnaturel.

L'iconographie d'un personnage entraîne la collecte **d'indices**, la production **d'une icône** et des propositions **symboliques**. Dans notre cas, les faits *hacker* constituent des indices, c'est-à-dire des traces d'un phénomène ou, plus précisément, d'événements. Comme Peirce le soulignait, l'indice est un symptôme amené comme pièce à conviction et supposé démontrer l'existence d'une chose. Toutefois, il ne constitue pas une preuve infaillible puisqu'il est soumis à l'interprétation. L'icône est un échafaudage d'indices. Il existe même si ses indices sont les symptômes d'un objet qui n'existe pas. L'icône devient ensuite l'inspiration de propositions symboliques exposées par ceux qui interprètent le sens de son existence ou de ses actions s'il y a lieu. En résumé, les journalistes producteurs d'iconographies retiennent ou rejettent des indices (appelés **faits**), dressent des icônes et leurs associent des symboliques.

La proposition symbolique est un jugement de valeurs, c'est-à-dire un énoncé qui incarne une appréciation. Si le jugement de valeurs conduit au débat, il est cependant sensible à tous les égarements vis-à-vis de son sujet. Le philosophe Sylvain Reboul de la Société Angevine de Philosophie rappelle :

> Un jugement de valeurs est toujours l'expression d'un désir subjectif, plus ou moins généralisé et artificiellement produit dans un contexte social donné; or, dès qu'on ne le reconnaît pas comme tel et qu'on croit que la valeur est dans la chose ou l'individu, on est victime d'un artefact, illusion qui attribue à l'objet même un effet produit par les conditions subjectives et objectives de notre regard sur lui. La confusion entre jugement de réalité et jugement de valeurs est, du point de vue épistémologique, la source même de ce qui fait principalement obstacle à la recherche de la vérité: l'illusion (Reboul, 1999).

A cela il faut ajouter les soucis d'éthique. Vautravers tient pour extrêmement graves les fautes professionnelles mêlant la calomnie, la diffamation, les accusations sans preuve, l'altération des documents, la déformation des faits, le plagiat et le mensonge. Il va sans dire qu'à ce stade-ci, ce travail de vérification reste du domaine du plausible. Or il est important de préciser que je réalise l'examen de démarches de journalistes qui n'ont pas la parole ici pour se défendre. De plus, en représentant leurs travaux d'enquête, j'opère moi-même une variation sur ceux-ci. C'est donc dire que seuls les faits et les conclusions explicites peuvent être retenus. En revanche, je profite du recul occasionné par le passage du temps. Depuis la publication de ces livres (1995 à 1997), des éléments nouveaux sont apparus. Leurs superpositions avec les éléments présentés dans ces livres constituent une méthode de comparaison rigoureuse. Les étapes de ma propre démarche :

1- Établir le contexte d'observation : Culture informatique, connaissance du phénomène *hacker*, situation d'observation.

2- Vérifier les antécédents : Le rapport du reporter vis-à-vis du sujet Mitnick.

3- Biais méthodologique : Motivations premières du reporter.

4- Normes et procédures : Stratégies d'enquête vs codes de la profession

5- Liste des faits retenus : Énumération des indices concernant la puissance et les mobiles de Kevin Mitnick et analyse de leur échafaudage.

6- Conclusions : Jugements de valeurs et propositions symboliques.

Les éléments retenus seront chaque fois ceux présentés par le journaliste lui-même et validés par l'enquête d'un tiers. Je retiendrai notamment les journalistes ou experts Scott Rosenberg (indépendant), Mike Brunker (*MSNBC*), James Fallows (indépendant), David Gelernter (*NY Times*), Chris Gulker (*San Jose Mercury News*), Joanna Glasner (*Wired News*), John Christensen (*CNN Interactive*), Keith Stone (*Los Angeles Daily News*), Miles O'Brien (*CNN Interactive*), Richard Peek (indépendant), Kevin Poulsen (*ZDNet News*), M.J. Zuckerman (*USA Today*) et Adam Penenberg (*Forbes*). Je retiendrai aussi un

article commis par Mitnick dans lequel il précise certains des faits rapportés par les trois reporters.

Les formules-choc, les commentaires explicites et les conclusions générales de chaque fin d'ouvrage, une fois replacés dans leurs contextes, constituent le matériel de base de ma propre recherche. L'analyse du contexte est déterminante car la sélection de faits (et de leur échafaudage ensuite) dépend de la situation d'observation du journaliste, de son expérience du sujet, de son mobile d'enquête et de sa stratégie professionnelle. Autant de facteurs qui déterminent le point de vue et qui conduisent à une juste interprétation de l'icône dépeinte par le reporter. J'y parviendrai en rassemblant spécialement leurs affirmations brèves (résumés d'introduction, synopsis, conclusions). Ensuite, en étoffant les bases de ces portraits avec d'autres détails (jugements de valeurs) présents dans le texte et cohérents avec le premier abrégé de l'iconographie. Finalement, en identifiant les propositions symboliques formulées pour chaque icône. En résumé, quels ont été les contextes, les procédures d'enquête et les faits retenus conduisant à la construction d'une iconographie et à la défense de propositions symboliques chez chacun de ces trois journalistes.

1- John Markoff

A) Contexte d'observation

De petits journaux californiens ont consacré quelques colonnes à Kevin Mitnick durant les années 1980. L'actualité locale s'était intéressée à ce jeune homme accusé deux fois de délit informatique d'intrusion, événement plutôt inaccoutumé pour l'époque. Bien sûr, il existait des cas de malveillance informatique en Californie. Mais ceux-ci impliquaient d'ordinaire des employés malhonnêtes qui avaient dérobé des logiciels ou encore des farceurs qui assaillaient les parcs informatiques de virus généralement peu puissants.

Médiatiquement parlant, Mitnick commença à véritablement exister à partir de 1991 après que John Markoff, alors journaliste au *New York Times*, eut publié *Cyberpunk : Outlaws and Hackers on the Computer Frontier*, un livre co-écrit avec son ex-femme Katie Haffner. Comme l'écrira Scott Rosenberg, rédacteur en chef du magazine *Salon* et anciennement collègue de Markoff au *San Francisco Examiner*, il arriva à Mitnick sur une intuition. Il cherchait un cas qui lui permettrait d'illustrer par un fait vécu l'incarnation même du danger *hacker.* Sur la base des quelques colonnes de presse californiennes qu'il put récupérer, il choisit Mitnick et essaya de le rencontrer. Il se buta cependant à un Mitnick très peu intéressé qui demanda derechef que sa collaboration lui soit payée. Selon les dires du *hacker*, cela provoqua la colère de Markoff qui décida de ne plus jamais s'adresser à lui directement (Mitnick, 2000). Quelques mois plus tard paraissait le livre et un long chapitre consacrait le côté obscur du *hacking* à travers la personne même de Mitnick.

En 1994, le *hacker* Shimomura invitait Markoff. Spécialiste en administration des systèmes, Shimomura était le directeur d'un centre de calcul de San Diego récemment victime d'une intrusion commise par Mitnick. Il avait fait de sa capture une affaire personnelle. En échange de l'opportunité offerte à Markoff, c'est-à-dire la possibilité d'assister sur place à la filature, le *hacker* demandait que ce dernier l'aide à écrire un livre si jamais la poursuite aboutissait. Plus encore, que le nom de Markoff y figure comme co-auteur. Marché conclu. Le journaliste débarqua à San Diego quelques jours plus tard et assista à la chasse. Durant les semaines qu'elle dura, il publia plusieurs articles dans le *New York Times*. L'année suivant la capture de Mitnick, il signa *Takedown*, soit le récit complet de ce qui s'était passé chez Shimomura entre décembre 1994 et février 1995. Le livre était officiellement écrit par Shimomura avec l'assistance de Markoff. Mais dans les faits, le journaliste avait durement retravaillé les courts textes du *hacker* pour ensuite charger le livre des siens. Dans les derniers chapitres, il y allait de quelques réflexions personnelles sur la vie et l'œuvre de Mitnick à la lumière des arguments défendus par Shimomura (Rosenberg, 1995).

B) Antécédents et rapports vis-à-vis du sujet Mitnick

Né à Oakland (Californie) en 1949, Markoff décrochait une maîtrise en journaliste en 1976 à la *University of Oregon*. Embauché ensuite par le *San Francisco Examiner*, il est affecté aux affaires technologiques et informatiques de la *Silicon Valley*. Il devient éditeur du magazine *Inforworld* en 1981. En 1984, il passe au *San Jose Mercury* et devient aussi un collaborateur régulier du *Byte Magazine*. Il reçoit en 1988 le *Software Publishers Association's award* pour le meilleur reportage de l'année. Entre-temps, il publie avec Lennie Siegel *The High Cost of High Tech*. Il est aussi le premier journaliste à mettre la main sur Robert Tappan Morris, l'auteur d'un ver qui fait tomber un pan de l'infrastructure Internet cette année-là. Il se joint ensuite au *New York Times* et consacre quelques mois à couvrir le monde des affaires. Avec son ex-femme, Katie Hafner, il publie en 1991 *Cyberpunk: Outlaws and Hackers on the Computer Frontier* dans lequel il consacre le tiers des pages au cas Kevin Mitnick. Il en viendra ensuite au journalisme d'enquête et accorde beaucoup de son temps au *superhacker*. Après la publication de *Takedown* en 1995, il s'attire la hargne des supporters de Mitnick. Une bande de *hackers* ira jusqu'à déflorer le site du *New York Times* en septembre 1998 en guise de vengeance. Markoff a aussi été l'auteur d'une multitude de *scoops*. Il a notamment été le premier à révéler les intentions de l'administration Clinton d'introduire le système d'observation Carnivore (Markoff, 1999).

C) Biais du journaliste

Dans un article intitulé *Cyberspace's most wanted* et paru en juillet 1994, Markoff identifiait Mitnick comme le *hacker* le plus dangereux d'Amérique. Le ton de l'article ne laissait aucun doute :

> Le problème de Kevin est qu'il a été condamné à plusieurs reprises. Peu importe ce que vous pensez de ses crimes, ils ont déclenché des procédures fédérales. Et la justice l'a condamné. Maintenant elle lui court encore après lui pour une autre série de crimes fédéraux (Markoff, 1994).

Il traitait tour à tour Mitnick de « vandale », « d'immature » et de « danger public ». Markoff n'avait pas changé d'avis sur lui depuis *Cyberpunk* en 1991 : il représentait l'extrême côté obscur du *hacking*. Lorsque Shimomura le contacta quelques mois plus tard pour l'accompagner dans sa filature, il récidiva dans un nouvel article qui reprenait les mêmes termes (Markoff, 1995).

Poursuivi par la presse, l'édition et l'industrie du cinéma, Markoff était devenu le grand spécialiste du phénomène Mitnick. Plus encore, son détracteur numéro 1. Il faut retenir qu'à ce jour Markoff était demeuré un journaliste certes bien payé mais à qui on offrait maintenant la possibilité de devenir millionnaire. D'une part, un producteur d'Hollywood lui acheta d'avance sa collaboration pour l'écriture d'un scénario (un contrat de 750,000$). De l'autre, il se vit proposer un contrat de 1,000,000$ pour l'écriture d'un livre à paraître sitôt qu'aboutirait la filature de Shimomura. L'éditeur décida même d'avance quel serait le titre de ce livre. Ce montant fut majoré à 1,400,000$ quelques mois plus tard et partagé en avec Shimomura. Le journaliste Scott Rosenberg rapporte que Markoff s'était aussi entendu pour apporter son soutien à l'industrie du jeu vidéo en échange de droits frisant les 2,000,000$ (Rosenberg, 1995). Tous ses clients attendaient de lui une iconographie détaillée, spectaculaire, fascinante mais surtout résolument criminelle. Ces contrats piégeaient donc Markoff qui devait en arriver à des conclusions négociées d'avance. Le FBI, se découvrant un allié objectif, considéra le travail de Markoff pour stimuler la progression de sa propre enquête.

Entre-temps, Markoff accusa Mitnick dans le *New York Times* de s'être introduit dans sa vie privée et d'avoir divulgué des informations personnelles comme ses numéros de cartes de crédit, ses revenus de placement et les soldes de ses comptes bancaires. C'est dans ce contexte qu'il arriva chez Shimomura. Il découvrait un expert du réseau qui ne dissimulait pas son animosité envers Mitnick, lequel venait de laisser quelques messages moqueurs sur son répondeur téléphonique. Dans l'un d'eux, il agaçait Shimomura en l'appelant par son prénom : « Bonjour, c'est encore moi, Tsutomu, mon fils » (Markoff, 1996). Il lui proposait aussi de lui enseigner le *Kung-Fu*, en référence à ses origines asiatiques. Ulcéré par ces messages, Shimomura fournit les rubans au FBI en

plus de mettre des copies en format numérique sur le net. Son antipathie était sans équivoque.

Quand Mitnick contacta directement Littman, il ne pouvait ignorer que cela aurait pour effet d'enrager Markoff. Il persistait entre eux une rivalité qui datait des années 1980 alors que les deux jeunes loups s'arrachaient les scoops au *San Francisco Examiner*. Mitnick choisit non seulement Littman, mais il le pressa de publier rapidement l'existence de leur relation privilégiée, question sans doute de narguer Markoff à qui il avait refusé entrevue par le passé (Littman, 1994).

Il faut finalement retenir que l'hospitalité de Shimomura était conditionnelle. Il était entendu que Markoff resterait son obligé. Le *hacker* lui exprima même à un certain moment son horreur de l'écriture « mélodramatique ». Il comptait aussi sur sa notoriété acquise via Markoff pour éblouir Julia Menapace, une employée de *l'Electronic Frontier Foundation* dont il était manifestement très épris. Markoff glissa d'ailleurs un mot au sujet de cette histoire dans le livre. Scott Rosenberg confirmera l'existence de ce flirt quelques mois plus tard (Rosenberg, 1995).

D) Normes et procédures professionnelles

Markoff procéda d'une enquête très agressive en usant de nombreux subterfuges qui l'amenèrent à enfreindre la loi. Caché dans un *van* avec Shimomura et un technicien de Sprint, il utilisa un équipement illégal pour écouter et enregistrer les conversations cellulaires de Mitnick, contrevenant au *Electronic Communications Privacy Act*. Plus tard, il publiera certains bouts de ces conversations, se livrant à un grave bris de confidentialité. Eric Corley (alias Emmanuel Goldstein, éditeur du mensuel *hacker 2600*), s'insurgea ainsi que l'une de ses communications avec le *hacker* ait pu être interceptée. Il faut noter que Markoff détient toujours ces bandes et qu'il refuse de les détruire (Rosenberg, 1995). Il alla aussi jusqu'à se présenter sans prévenir chez la grand-mère de Mitnick à Los Angeles, une dame très âgée, pour tenter d'obtenir une

entrevue. Il s'attira ainsi la désapprobation d'autres journalistes dont Littman, Goodell, Rosenberg, Corley et même Poulsen, cet ancien *hacker* converti à l'éditorial (Mitnick, 2000).

Markoff dissimula sa relation de longue date avec Shimomura et il fallut les enquêtes de Littman et Goodell pour la révéler. Il y a donc lieu de s'interroger : avait-il été invité ou s'était-il invité? Markoff prit une part active dans l'aventure et accompagna (physiquement) Shimomura partout durant au moins huit semaines de traque en plus de donner régulièrement son avis sur les techniques d'enquête à prendre pour le retrouver. L'idée du *van* pour écouter les conversations cellulaires de Mitnick était de lui comme il le confirma lui-même dans une entrevue accordée à Chris Gulker : « J'étais dans le camion en tant que reporter du *New York Times* et je m'étais clairement identifié comme tel » (Gulker, 1998). Sal Cinquegrani, porte-parole chez *Sprint Cellular* a pourtant démenti :

> Nous avions reçu un ordre de la cour. On nous avait dit que nous allions rencontrer un expert en informatique. C'est Shimomura qui apparut. Plus tard, quelques agents locaux du FBI arrivèrent à notre centre d'interrupteurs mobile (le *van*). Par le fait même, Mr. Markoff apparut sur la scène. Puisqu'il y avait beaucoup de conversations entre Shimomura et Markoff et les autres aussi, nous avons pensé que tout ce beau monde travaillait ensemble. Ce n'est que plus tard que nous avons appris qu'il était reporter. Nous l'avons appris en même temps que les agents eux-mêmes (Gulker, 1998).

A ce sujet, l'assistant du procureur, John Ken Walker, affirma au journaliste Chris Gulker que Markoff s'était bel et bien introduit dans ce *van* en se présentant comme un expert : « Son rôle dans cette enquête était d'être une source d'informations sur Kevin Mitnick » (Gulker, 1998).

D'autre part, la technique empruntée par Markoff pour évaluer les dommages occasionnés par Mitnick reste discutable. Si par exemple le *hacker* dérobait un logiciel, Markoff s'informait auprès de l'entreprise pour savoir combien il en avait coûté en recherche et développement. Suivant sa logique, un

internaute qui télécharge *Adobe Photoshop 6.0* d'un site de *WAREZ* pourrait donc être accusé d'un méfait évalué à 10,000,000$ alors qu'une copie sous licence de ce logiciel se vend autour de 600$.

Point de vue éthique, le journaliste Chris Gulker s'interroge : « Depuis quand les reporters du *New York Times* font des affaires ($$$) avec leurs sources? N'est-ce pas là un conflit d'intérêt? » (Gulker, 1998) Nancy Nielsen, vice-présidente communications au *New York Times* défend son journaliste : « Comme le stipule notre politique concernant les conflits d'intérêts, John Markoff a suivi la procédure pour recevoir d'abord une permission du *Times* avant de signer son contrat de publication » (Gulker, 1998). Nancy Nielsen refusa cependant de fournir copie de cette politique à la presse, arguant qu'il s'agissant d'un document confidentiel. Elle ajoutera que de toute manière son journaliste n'était pas en conflit d'intérêt puisqu'il avait pris un congé sans solde à partir de mars 1995 (le mois suivant la capture du *hacker*) pour se consacrer exclusivement à la rédaction de *Takedown*. Pour une raison restée inconnue, Markoff mentit ensuite délibérément à la presse en affirmant qu'il avait étroitement collaboré avec Tim Race, son éditeur, durant tout ce temps (de mars à août 1995). Il apparut plutôt que le travail de rédaction avait été vérifié au jour le jour par un employé du *New York Times* lui-même, lequel avait été mandaté par Race, l'éditeur du livre *Takedown*. Cet employé aurait été payé par l'éditeur, parti en vacances à San Francisco, à titre de consultant. Race et Markoff refusèrent ensuite de s'expliquer là-dessus, suscitant l'ire des journalistes Littman, Goodell, Rosenberg, Gulker et Stone (Stone, 1996).

Finalement, Markoff décida de collaborer avec le FBI en divulguant certaines des pièces à conviction. Son travail fut même appelé à la cour et considéré un temps comme un examen d'expert.

E) Énumération des faits retenus : indices de puissance et de mobiles

Markoff s'attarde aux **faits concernant la puissance** de Mitnick pour justifier sa foi en sa puissance *hacker*. Il enchaîne ensuite avec les **faits illustrant les mobiles** qui l'ont vraisemblablement poussé à agir de la sorte.

De la **puissance**, il retient d'abord le film *WarGames*. Le reporter est persuadé que Mitnick a été l'inspiration de ce film tourné en Californie. Il écrit : « Mr. Mitnick a utilisé un ordinateur et un modem pour s'introduire dans le *North American Air Defense Command* en 1982, préfigurant l'histoire du film *WarGames* sorti l'année suivante » (Markoff, 1994). 1982 coïncidait aussi avec la première capture de l'adolescent Mitnick pour une affaire d'intrusion. Des abonnés du téléphone de la région de New York s'étaient plaints de blagues de mauvais goût dont ils étaient victimes. De sa Californie, Mitnick avait pris le plein contrôle de trois centrales téléphoniques new-yorkaises et détournait des appels adressés au service 411. C'était donc lui qui répondait aux usagers. A l'un d'eux qui souhaitait parler à un certain monsieur, il demanda par exemple : « Monsieur est-il blanc ou noir? Voyez-vous, chez AT&T nous possédons deux annuaires téléphoniques : l'un pour les blancs, l'autre pour les noirs » (Markoff, 1991). Il reconnut sa culpabilité et fut condamné à une sentence avec sursis suivie d'une année de probation. Il n'en était pas à ses premiers démêlés avec la justice puisqu'en 1981 déjà il avait été arrêté pour une histoire de vol de manuels électroniques chez Pacific Bell, une compagnie de téléphone locale. De telles frasques avaient fait parler d'elles dans la presse locale. Pour la première fois, la presse s'attardait au cas d'un *hacker* déviant. Markoff considère ces récits comme la genèse de l'icône Mitnick et le point d'ancrage de sa propre iconographie.

Il reprend ensuite son propre compte-rendu de 1991 (*Cyberpunk*) pour dresser l'inventaire des exploits accomplis par Mitnick durant les années 1980. Markoff fut d'ailleurs l'un des rares en 1987 à s'intéresser à la seconde capture de Mitnick pour fraude informatique. Et pour cause, puisque cette courte affaire reste un événement peu documenté encore aujourd'hui comme John

Christensen de *CNN* le rapportait dans un article paru en 1999 (Christensen, 1999). Markoff soutient que Mitnick s'était rendu coupable d'une série d'intrusions dans d'autres stations téléphoniques, plusieurs laboratoires nucléaires et des vols de données dans des ordinateurs du Pentagone. Si Mitnick avait bel et bien plaidé coupable à des accusations sommaires, la cour ne lui imposa aucune peine, faute de preuve, voire de plainte tangible. Aux dires du reporter, ces intrusions avaient été spectaculaires mais n'avaient malheureusement pas capté l'attention de la presse qui ne prenait pas encore ces histoires au sérieux. Markoff croit que le simple fait d'avoir été le premier *hacker* condamné vaut à Mitnick une considération d'exception. Il aurait été le premier « desperado » capable d'inspirer la terreur aux habitants d'un « Far West électronique » (Markoff, 1996). Ce pouvoir terrible, maintenant détenu par des milliers de *script kiddies*, Mitnick aurait donc été le premier à le posséder. Quand Mitnick est capturé une troisième fois en 1989 pour délits graves, l'idée de Markoff est faite : il ne s'est pas trompé sur la personne. Cette fois-ci, il est arrêté pour intrusion dans les ordinateurs de MCI et de *Digital Equipment Computer*, cette puissante institution dont je parlais au premier chapitre (Page 6). Créée en 1957, *DEC* s'était illustrée rapidement pour sa série d'ordinateurs PDP. Elle avait été avalée des décennies plus tard par le géant Compaq. Mitnick est condamné à un an de prison ferme et à trois ans de probation. DEC l'accuse de méfaits évalués à 1,000,000$ et parvient à prouver son point en sortant ses relevés de paie : une masse d'employés avait été contrainte à faire des heures supplémentaires pour reboucher les trous creusés par le *hacker*. Ce casse coûtait véritablement de l'argent. La justice estima que Mitnick représentait une menace pour la société.

Relâché comme convenu l'année suivante, Mitnick s'empressa aussitôt de *hacker* le *State Department of Motor Vehicles* et de retoucher son dossier de conduite. Un système parmi les plus sophistiqués et les mieux protégés au pays. Cette fois c'est du sérieux pense Markoff. Mitnick est déchaîné. Il défonce des systèmes montés par les plus brillants experts, spécialement ceux de Dan Framer et Eric Allman. Il s'introduit dans les bases de données de Netcom Communications et s'empare des numéros de 20,000 cartes de crédit. Il prend

aussi le contrôle d'un essaim d'ordinateurs éparpillés chez Motorola, Sun Microsystems, NEC, Novell et Nokia en plus de pénétrer directement dans l'ordinateur de Shimomura. Le FBI place son nom sur sa liste des *Most Wanted*, faisant de lui l'une des personnes les plus dangereuses de la nation. Markoff y voit un aboutissement naturel : le *superhacker* est devenu l'ennemi public numéro 1. L'étau finit même par se resserrer autour du reporter qui voit sa vie privée violée par Mitnick. Le *superhacker* lit non seulement ses courriels, mais divulgue et partage ses données personnelles sur le net (marges de crédit, placements, soldes bancaires, numéros de carte de crédit, etc.) En dix ans de couverture, Markoff avoue n'avoir jamais vu une créature *hacker* capable de telles choses. Il prétend même avoir reçu la preuve formelle que Mitnick s'est introduit dans l'ordinateur clé du système du *Department of Defense* (DoD), un ordinateur théoriquement capable de commander la mise à feu de missiles intercontinentaux.

Markoff est persuadé qu'aucun système ne peut résister à l'acharnement de Mitnick. Il est aussi persuadé que seule la trahison peut conduire à l'arrestation du *superhacker*. Pour cause, ses trois précédentes arrestations avaient été rendues possibles grâce à la délation d'amis proches. La première fois en 1981 quand une certaine Susan Thunder le dénonça lui et son groupe d'amis *phreakers*. Après avoir été larguée par Roscoe, chef de la bande, elle se vengea en appelant la police. La seconde fois en 1987 quand d'autres potes *hackers* le lâchèrent. Puis en 1988 quand son meilleur ami d'alors, Lenny DiCicco, lui tendis un guet-apens dans un stationnement après avoir mal apprécié une plaisanterie. Large sourire, il s'adressa à lui : « Dis Kevin, tu connais cette sensation au creux de l'estomac lorsqu'on sait qu'on va se faire ramasser par les flics? » (Littman, 1996)

Mais cette fois Mitnick semble à l'abri. Sa fougue et son effronterie le confirment : le *superhacker* pousse l'audace jusqu'à téléphoner à ses victimes pour les narguer. On ne lui connaît aucun ami, aucun partenaire. C'est lui contre le monde entier et il s'en vante. Le reporter soutiendra plus tard que seule une stratégie impliquant à la fois un esprit « hautement supérieur » comme celui de

Shimomura et des méthodes à la limite de la loi pouvait conduire à la capture du *superhacker* (Markoff, 1996).

Markoff considère aussi l'ampleur des plaintes adressées à Mitnick comme des indices révélateurs de sa toute puissance. Il vérifie les savants calculs auxquels se sont adonnées les victimes et valide leurs sommes : les réclamations consolidées atteignent bel et bien les 80 millions de dollars. Malgré une jurisprudence encore pauvre en cas de *hacking* criminel, Mitnick s'expose à des chefs d'accusation pouvant le condamner à une peine de 460 ans de prison. Des meurtriers auraient connu moins pire. Le reporter, s'appuyant sur sa longue expérience du phénomène *hacker*, dira après la capture du *superhacker* :

> A mon avis, il a été une menace publique qui aura davantage endommagé le principe même de la confidentialité à l'âge de l'information que tout ce que j'avais pu imaginer comme possible et faisable par le passé (Gulker, 1998).

Du **mobile**, Markoff retient tous les faits qui témoignent du côté récidiviste de Mitnick. D'abord, il s'étonne qu'après trois arrestations, douze mois passés en prison et aussi quinze ans de maturation, Mitnick n'ait jamais cessé de s'introduire dans les systèmes. Il retient aussi ce bris de conditions commis par Mitnick en 1992 lorsque celui-ci cessa de se rapporter à son agent de probation alors qu'il aurait eu tout intérêt à le faire. En effet, Markoff considère que Mitnick aurait logiquement pu profiter de ce support pour se bâtir une honnête vie, et à terme, louer son pouvoir à des entreprises légitimes. Mais il semblerait que le *superhacker* soit détaché des préoccupations humaines. L'argent par exemple. De ses premières frasques en 1980 jusqu'à sa capture finale en 1995, jamais le *superhacker* n'a profité de son pouvoir de commander les machines du réseau pour gagner quelque argent que ce soit. L'enquête de Markoff démontre que le *superhacker* n'a jamais été soupçonné d'avoir revendu un seul logiciel, ni utilisé frauduleusement les numéros des 20,000 cartes crédits retrouvés sur l'un de ses disques durs, ni commis de détournement de fonds. Son seul profit aurait été d'utiliser les services du téléphone sans jamais les payer. Le reporter remarque que la pauvreté a toujours été une constante dans la vie de Mitnick et qu'il n'a

jamais rien fait pour s'en sortir. Le plus puissant des *hackers* n'avait même pas les moyens de se payer un simple entretien avec un avocat au lendemain de sa capture.

Le reporter insiste ensuite sur ce qu'il nomme la « perturbation de Mitnick par rapport au monde extérieur ». Selon l'ensemble des témoignages recueillis auprès des parents et des anciens amis, Mitnick aurait toujours été un solitaire aux allures d'autiste. Son usage du pseudonyme *Condor* serait d'ailleurs révélateur de sa schizophrénie. Markoff croit que ce choix n'a pas été fait à la légère. Le fait est que *El Condor* proviendrait d'un film avec Robert Redford sorti en 1975 : *Three Days of the Condor*. Un film apprécié de Mitnick et qui racontait l'histoire d'un homme persécuté par la CIA. Le personnage principal, joué par Redford, se tirait d'impasse en utilisant son expérience militaire des télécoms. Markoff s'appuie aussi sur une photo qui, avance-t-il, réunit tous les traits de personnalité du *superhacker*. La photo montre un Mitnick gras, mal rasé et caché derrière d'épaisses lunettes rectangulaires. Le journaliste Scott Rosenberg contemplera cette photo spécialement choisie par le reporter : « Verres épais, double menton, lèvres serrées, sourcils et regard fixes et amers : cette photo de Mitnick suggère plutôt le visage d'une gargouille *hacker* » (Rosenberg, 1995). Markoff la commente en faisant ressortir l'aspect « renfrogné », les chairs « bouffies » et le regard « absent » du *superhacker*. Sa conclusion : « le portrait d'une tronche qui a mal tourné » (Markoff, 1994).

Mal tourné en effet. Markoff retient qu'en 1989 le *superhacker* avait été obligé par la cour de réussir une thérapie pour « pratique obsessionnelle » de l'informatique. Lors de cette troisième condamnation, l'avocat de Mitnick lui-même avait plaidé la cause de la dépendance et du désordre mental. Markoff brandit un rapport dans lequel un psychologue déclare que Mitnick est malade. Qu'il est un « obsessionnel ». Un « monomaniaque ». Il brandit aussi le verdict de 1989 dans lequel le juge compare la relation du condamné avec l'informatique à celle du toxicomane pour la drogue dure. Markoff souligne d'ailleurs que c'est bel et bien au milieu d'une bande de trafiquants que Mitnick purgea cette peine-là (Markoff, 1996).

Le reporter enchaîne avec d'autres faits qui tendent à démontrer le dérangement mental de Mitnick. Par exemple, l'aberrance de ces nombreux messages que le *superhacker* lui a directement adressés par téléphone et messagerie électronique. Un *Most Wanted* gaspille son temps pour narguer un simple reporter alors qu'il a toute la nation aux trousses. Il note aussi ces nombreuses insolences adressées à Shimomura dans un contexte à la limite du danger alors qu'une capture lui garantira une lourde de peine. Le génie de Shimomura s'appuierait justement sur une série de faits indiscutables. Markoff qualifie de « brillant », de « supérieur intellectuellement » et de « génial » celui qui décrocha un doctorat de *Los Alamos University* à l'âge de dix-neuf ans, cela en sautant une partie du lycée. Les faits tendent à démontrer que Shimomura mène une vie exemplaire et qu'il possède une éthique de travail absolument irréprochable. Extrêmement respecté par ses collègues, dont plusieurs témoignent à Markoff de leur plus profond respect, le *hacker* "blanc" (qui signifie honnête) s'est rapidement vu confier un poste de direction dans un réputé centre de calculs de San Diego. D'autres témoignages d'institutions et de personnalités politiques certifient qu'ils ont pleinement confiance aux immenses compétences du Japonais Shimomura, lequel est déjà considéré à trente ans comme « l'un des plus grands spécialistes mondiaux en sécurité informatique ». « Austère », « dévoué », « performant », « ingénu », « efficace », « honnête », Shimomura serait bien l'homme de la situation. Pourtant Mitnick parvient à lui infliger une humiliante défaite en s'annonçant puis en s'introduisant dans son propre ordinateur la veille de Noël 1994. Une intrusion « surnaturelle » commise au nez et à la barbe d'agents du FBI équipés d'un « matériel de détection ultra-sophistiqué » qui attendaient justement la passe (Markoff, 1995).

Markoff rejette l'hypothèse de la farce. Mitnick serait plutôt un être « malicieux » et il présente ses faits. D'abord, les propos tenus par le *superhacker* sont ceux d'un vengeur. Cette hargne manifeste, cette moquerie de tous les instants, cette méchanceté sans fondement. Il s'agit d'une tentative d'écœurement visant à rabaisser l'estime de ses victimes. Ensuite, toute sa vie Mitnick démontra combien il était un être fort peu scrupuleux. La manière ingrate avec laquelle il traita ses quelques amoureuses, sa famille, ses amis puis sa

conduite à l'école comme au travail, son non-respect des lois et des conventions sociales les plus élémentaires, son désengagement aussi pour quelque cause que ce soit, tout cela démontre qu'il est tout « sauf un bon garçon » (Markoff, 1996).

Finalement piégé par Shimomura qui s'était rendu lui-même sur place en Caroline du Sud avec les policiers partis l'arrêter, Mitnick le regardera dans les yeux et lui dira : « Je respecte tes talents » (Markoff, 1996). Pour Markoff il s'agit d'un fait démontrant à la fois l'immense compétence de Shimomura mais aussi la vulnérabilité mentale de Mitnick. Car somme toute, ce seront les aptitudes mentales du Japonais, sa retenue et son pragmatisme qui auront rendu possible la capture du *superhacker* mentalement dérangé. Si Mitnick avait su être plus raisonnable, plus réfléchi aussi, jamais un être doté d'un tel pouvoir n'aurait pu être capturé de la sorte. La haine, le principal mobile de Mitnick, aurait aveuglé le *superhacker* au point de lui faire perdre le contrôle de lui-même et de sa destinée.

F) Jugements de valeurs et propositions symboliques

L'iconographie de Markoff aboutit à un Mitnick certes puissant mais atteint d'un grave désordre mental. Le jeune homme serait détraqué. Dangereux car irréfléchi, déraisonnable et impulsif. Un être emporté qui foudroie le parc informatique mondial de ses pouvoirs *hacker*. Une première thérapie échoua à le soigner, il faudrait cette fois-ci lui administrer un châtiment punitif exemplaire. Du moins l'enfermer tant et aussi longtemps qu'il représentera l'une des pires menaces publiques jamais enfantées par le médium Internet. Le garder enfermé aussi tant qu'il restera une créature *hacker* détachée des préoccupations humaines. Une créature incapable de reconnaître les conséquences de ses actes. En bref une icône populaire abjecte et malveillante.

Markoff retient de Mitnick le symbole d'un échec. Ce *superhacker* serait un raté tandis que Shimomura incarnerait la quintessence de ce que « devrait

être un *hacker* » (Markoff, 1996). Il compare la personnalité chevaleresque du Japonais au tempérament malicieux de Mitnick. Sa figure personnifierait les fantasmes de *hackers* noirs (malhonnêtes) décidés à imposer leurs sinistres pouvoirs aux autres usagers de l'Internet. Mitnick serait devenu en quelque sorte leur héros terroriste. Une inspiration au désordre électronique comparable à une première cellule cancéreuse qui menace l'organisme. Pour le reporter, Mitnick symbolise cette première fragilité de l'Internet.

2- Jonathan Littman

A) Contexte d'observation

Jonathan Littman, journaliste indépendant, eut la chance de suivre Mitnick durant les neufs derniers mois de sa cavale. Quelques mois après la parution d'un récit sur Kevin Poulsen (en juin 1994), Kevin Mitnick lui téléphona. Il proposa de lui raconter son histoire. A condition que cela se fasse à distance. D'aucune façon Littman ne devait tenter de le retracer. C'est qu'à ce moment-là, Mitnick semblait particulièrement nerveux aux dires de Littman. Le FBI venait de mettre son nom sur sa liste des *Most Wanted*, fait sans précédent pour une affaire de hacker. Littman devint donc le confident de Mitnick qui lui téléphona plusieurs douzaines de fois entre juin 1994 et février 1995. Non seulement il lui racontait des détails intimes sur sa vie, mais il le tenait aussi au courant de ses intrusions les plus fraîches. Littman était mis au parfum d'intrusions la plupart du temps encore ignorées par les victimes elles-mêmes. Les scoops étaient précis et malgré son acharnement à les vérifier systématiquement, Littman ne parvint jamais à soupçonner le moindre mensonge. Cela conforta sa confiance en Mitnick comme il l'avouera plus tard (Littman, 1996).

Les révélations du *superhacker* fournirent à Littman des occasions d'enquête inespérées. Des pistes le conduirent jusqu'à rencontrer directement des victimes pas encore au fait de l'agression. Il récupéra ainsi quelques

témoignages à chaud. Il put ensuite les discuter avec Mitnick qui précisait ou rejetait certains points d'interrogations.

Mitnick déclara éprouver beaucoup de respect pour ce reporter. Il le lui dit en juin 1994, date de leur premier contact. Il admirait sa rigueur et sa capacité de recul vis-à-vis des événements, particulièrement les événements *hacker*. Il se sentait suffisamment en confiance pour s'ouvrir à lui (Fallows, 1996).

B) Antécédents et rapports vis-à-vis du sujet Mitnick

Journaliste d'excellente réputation (nominé au *Pulitzer* en 1991 pour un travail d'investigation dans une communauté amérindienne aux prises avec des problèmes de jeux compulsif), Littman publiait en 1994 un livre intitulé *The Last Hacker*, soit le récit et l'iconographie de Kevin Poulsen. Il avait commencé à couvrir l'actualité informatique au début des années 1980 pour le compte du *San Francisco Examiner* après avoir décroché un diplôme en rhétorique à l'Université de Berkeley. Il suivit également quelques cours de programmation et publia même un manuel technique en 1983. Il devint ensuite collaborateur régulier de nombreuses publications à partir de 1984 : *PC Magazine*, *Forbes*, *PC Week*, *Mac Week*, *The Village Voice*, *Upside* et continua par intermittence au *San Francisco Examiner.* Littman est aussi réputé pour ses habiletés interpersonnelles et sa facilité à établir des contacts humains. Il parle d'ailleurs quatre langues : anglais, espagnol, italien et portugais. Sa personnalité attachante lui aurait valu de nombreuses opportunités de carrière. Peu orgueilleux, il rigole volontiers de lui-même et de sa notoriété. Sa véritablement passion, écrit-il, c'est de faire pousser des tomates (Littman, 1997).

Il acquit sa notoriété en publiant *Shockwave Rider, the saga of Robert Morris* en 1989. Morris, rappelons-le, était le fils d'un informaticien devenu célèbre pour avoir crashé une partie du réseau Internet en 1988 en y lâchant un ver. Son reportage lui valut le *Computer Press Award* et il continue d'être publié à chaque année. En 1990, il publia *Once Upon A Time In Computer Land*, un

reportage salué par la presse qui racontait l'élévation et la chute du milliardaire Bill Millard, grand fabricant d'ordinateurs personnels. Il consacra ensuite de nombreux articles sur le phénomène *hacker*, dont un important à l'automne 1993 sur *Phiber Optik* (Mark Abene) et son gang les *Masters of Deception*.

En juin 1995, c'est cependant l'appel de Mitnick qui le décida à s'occuper plus précisément de cette affaire.

C) Biais du journaliste

La rivalité qui liait Littman et Markoff depuis leurs années au *San Francisco Examiner* se poursuivait en 1995. Deux journalistes très en vue qui s'attardaient souvent aux mêmes sujets. Quand Mitnick appelle Littman pour lui offrir un accès privilégié, le reporter a tout intérêt à ne pas brûler son contact. Il a, affirme-t-il, une chance inouïe. Il a surtout la chance de devancer Markoff (Littman, 1996).

Le journaliste James Fallows remarque que Littman y est allé tout en douceur. Les questions adressées au *superhacker* étaient empreintes de tact. Il conservera ensuite mystérieusement le secret sur l'ensemble de leurs conversations. Ce qui laisse croire, affirme Fallows, qu'il y ait eu un accord pour couper certaines déclarations *off the record*. Bien sûr *The Fugitive Game* est plein de retranscriptions mais jamais Littman n'accepta de partager le reste avec la presse (Fallows, 1996).

Depuis le ver de Morris en 1988, Littman s'était toujours fait connaître pour ses prises de position contre l'instrumentalisation politique et économique du phénomène *hacker*. Bien sûr, il reconnaît que l'activité *hacker* occasionne des coûts mais il soutient qu'ils sont habituellement exagérés. Avec Mitnick, il obtenait son meilleur argument. Des sommes colossales lui étaient imputées. Des sommes défendues par Markoff lui-même. Il aborde donc l'affaire en

critiquant ouvertement chacune de ces sommes et en vient à banaliser les frasques du *superhacker* (Littman, 1996).

Enfin, Littman tenta une incursion à Hollywood pour y vendre les droits de son livre. Ce qui lui vaudra la condamnation de plusieurs journalistes. Richard Peek et David Gelernter découvriront plus tard que Littman avait conclu une entente avec un producteur de Broadway pour un montant indéterminé. Gelernter dira qu'il ne valait donc pas mieux que l'autre (Markoff) : « Littman est jaloux des pactes de Shimomura et Markoff avec l'industrie du cinéma (...). Mais qui aurait pu le blâmer ? » (Gelernter, 1996)

D) Normes et procédures professionnelles

Une enquête tatillonne, un respect évident pour son sujet, un esprit critique omniprésent, tout porte à croire que Littman a dûment respecté les normes de la profession. Comme le souligne Gelernter, le reportage de Littman ressemble à un « *scrapbook* » d'articles de presse et de retranscriptions choisies parmi les conversations les plus intéressantes avec le *superhacker*. Il s'agit d'un travail « diffus » tandis que celui de Markoff était « focalisé » (Gelernter, 1996). En fait, comme l'écrira Littman, une tentative pour encadrer le phénomène Mitnick de la manière la plus large possible. Le reporter souhaitait faire comprendre à son lecteur qu'il existait certainement d'autres Mitnick et que ce dernier était une création politique. Une incarnation symbolique de quelque chose de plus vaste. Il vérifia ainsi systématiquement chaque cas d'intrusion (*hack*) dont Mitnick se vantait d'être l'auteur. Il en vint à la conclusion qu'il n'existait pas de preuve inébranlable pouvant prouver qu'il en était l'auteur. Du moins le reporter conviendra que si Mitnick n'était pas l'auteur direct de ces intrusions, qu'il était manifestement très proche de son artisan (Littman, 1996).

Si certains symptômes lui parurent frappants, Littman tenta pourtant de les démonter par tous les moyens. Il confronta même Mitnick à plusieurs occasions, réclamant des explications sur l'aspect magique de ses gestes. Il condamna les

réponses évasives du *superhacker* et douta certains instants de sa réelle compétence. Du moins, il suscita le doute chez le lecteur lui-même. Littman resta donc sceptique tout au long de son travail.

Littman garda aussi la vie privée de Mitnick en dehors du débat. Les seuls points qu'il rapporta furent ceux qui obtinrent l'approbation de Mitnick lui-même. Pour le reste, il considéra sa vie privée comme un élément secondaire. Malgré le privilège qui lui était accordé, Littman n'usa pas de quelque subterfuge que ce soit pour s'approcher davantage du *superhacker*. Il respecta sa parole et ne tenta jamais de le retracer, allant même jusqu'à accepter de brouiller sa propre ligne selon le vœu du *hacker* (Littman, 1996). Il se concentra plutôt à contacter les victimes de ses intrusions et à rapporter leurs témoignages.

Chez Littman, l'effort est indiscutable : Mitnick était un sujet comme un autre. Il s'en tint à des conversations directes et n'accorda jamais ni admiration, ni désapprobation aux propos de Mitnick. Il s'agissait pour lui d'un exemple *hacker* tout puissant qu'il pouvait interviewer à son aise. Son livre aboutit à un questionnement plutôt qu'à un éloge de l'icône.

Sollicité plus tard par la justice qui lui demanda de fournir copie de ses conversations, le reporter refusa de collaborer. Ses documents resteraient dans ses archives personnelles et n'en sortiraient qu'après un accord avec Mitnick.

Soucieux de ne pas être accusé d'entorse à l'éthique, Littman rompit toute relation avec Mitnick après sa capture. Il rédigea ensuite son livre et attendit sa publication avant de contacter l'industrie du cinéma.

Littman reconnut qu'il n'était pas assez grand spécialiste ni assez proche encore pour juger des prouesses de Mitnick. Il se méfia aussi des témoignages des victimes qui consacraient l'aspect surnaturel des pouvoirs du *superhacker*. Il les citait mais toujours en les considérant comme des faits modérés et discutables. Richard Peek saluera sa démarche et la qualifiera de « sérieuse » et

ses conclusions comme « bien documentées », « compréhensibles » et « divertissantes » (Fallows, 1996).

E) Énumération des faits retenus : indices de puissance et de mobiles

A priori, Littman possède assez d'expérience de la programmation pour ne pas croire en la compétence de Mitnick à ce niveau. Il le croit cependant très habile pour utiliser les programmes des autres et l'illustre à travers **plusieurs faits de puissance**. Spécialement l'originalité avec laquelle il parvient à les dépraver pour en faire une toute autre utilisation. Un logiciel *Netbus* par exemple. Un utilitaire d'administrateur réseau capable de commander à distance (dit *remote control* en anglais) d'autres machines éparpillées à l'intérieur d'un réseau privé. Après une retouche astucieuse, *Netbus* devient non seulement une porte d'entrée mais aussi un mécanisme de surveillance qui accompagne la machine infectée dans ses moindres connexions. Un habile *script kiddie* peut aisément retoucher le code source d'un tel logiciel pour ensuite s'en servir comme une arme. Bien sûr nulle magie, seul le mérite d'avoir eu la bonne idée. A ce jeu, Mitnick serait l'un des meilleurs. Justin Petersen, *hacker* et ami virtuel de Mitnick, affirmera au reporter que son compagnon d'infortune n'avait pas son pareil. Littman prend ce Peterson au sérieux. Capturé et condamné à servir 41 mois dans un établissement pénitencier après l'étalage d'une preuve accablante (fraudes à des concours radiophoniques, importants détournements de fonds bancaires, brigandage électronique, etc.), véritable programmeur aux antécédents reconnus et incorrigible casseur de sécurité, Petersen est sans contredit l'un des plus dangereux *hackers* au pays. Pourtant, Mitnick lui serait supérieur lorsqu'il s'agit de pervertir un logiciel. Mais le reporter note qu'il s'agit là d'un aspect « technique » de la créature et que son interprétation est sujette à « hyperbole ». David Schindler, procureur fédéral en chef à Los Angeles, minimise curieusement l'excellence du code de Mitnick (rappelons que dans le jargon informatique le programmeur développe le logiciel et que le codeur le remanie). : « Quand vous ne comprenez pas très bien le monde de l'ordinateur, vous êtes susceptibles de croire aux exagérations de personnes comme Markoff

et Shimomura. Des gars qui font finalement la promotion d'un livre » (Stone, 1996).

Exagération sur les dégâts d'abord. En effet, Littman refuse de s'émouvoir devant le nombre et la gravité des dégâts imputés au *superhacker* qu'il considère de l'ordre du « délire ». Comme si Mitnick volait un stylo Bic dans un supermarché et qu'on l'accusait d'avoir commis un vol de plusieurs millions de dollars en se basant sur les coûts de recherche et développement. Son analogie est partagée par le journaliste James Fallows qui explique pourquoi Littman n'a pas réussi à évaluer lui-même les dégâts. Puisque les déclarations des victimes et de Markoff étaient grossièrement exagérées, il ne restait plus de matériel à analyser. Du moins l'exercice devenait très pénible. Littman décida donc de laisser tomber (Fallows, 1996).

Exagération ensuite sur les prouesses passées du *superhacker*. Littman démonte certains faits rapportés par le *Takedown* de Markoff publié en 1991. Il rejette cette genèse en bloc quand il découvre que son fait le plus marquant est vraisemblablement tiré de l'imagination de son auteur. Non, Mitnick ne se serait pas introduit dans les ordinateurs du *North American Air Defense Command* en 1982. Il s'agirait d'une affirmation fantaisiste. Le reporter contacte ensuite les producteurs du film *WarGames*. Surprise : ceux-ci ignoraient jusqu'à l'existence du jeune Mitnick quand ils sortirent leur film en 1983. Durant ses conversations téléphoniques avec le fugitif (cinquante heures de ruban), Littman tente d'éclairer certains autres faits mais Mitnick n'en a conservé aucun souvenir. Sinon il nie. Il s'agit pourtant de vieilles histoires pour lesquelles le *superhacker* ne risque plus rien, qu'il les révèle ou non (Littman, 1996).

En revanche, Littman s'intéresse beaucoup à ses pouvoirs *phreaker*. Il y a quelque chose d'étonnant, pense-t-il. Ou du moins, d'inexpliqué. La téléphonie serait le véritable terrain où les pouvoirs de Mitnick se manifesteraient. Littman explique que l'ordinateur et son modem représentent simplement des périphériques dans le phénomène Mitnick. Enfant du *phreaking*, il aurait découvert les possibilités du téléphone bien avant celles de l'ordinateur. Le

reporter découvre qu'avec un seul téléphone cellulaire, Mitnick parvient, par exemple, à bloquer la voix de la caissière d'un *fast-food* pour répondre lui-même aux clients de la commande à l'auto. Littman s'informe auprès d'experts et obtient des explications floues au sujet de cette prouesse dont Mitnick est manifestement le seul à détenir le secret. De celle-là et de bien d'autres. Littman remonte jusqu'à *Teltec Investigations* par exemple. Une entreprise d'enquêtes californienne au service des corporations désireuses d'obtenir des renseignements confidentiels sur leurs employés, clients, postulants, etc. En 1992, *Teltec* embauche Mitnick qui dissimule sa véritable identité derrière un faux nom. Son patron témoigne à Littman de son abasourdissement. Ce garçon était un prodige. Il pouvait obtenir n'importe quelle information. Avec son modem, il se branchait à distance sur toutes sortes de terminaux téléphoniques et déjouait vraisemblablement des systèmes de confidentialité à la chaîne. Son employeur, content des résultats, avait fermé les yeux pour laisser Mitnick s'adonner à son mystère, pourvu que ça rapporte. Quand *Teltec* fut mise sous enquête par le FBI pour pratiques douteuses, Mitnick s'évapora. Autre fait considéré par le reporter : Mitnick savait découvrir systématiquement les trajectoires téléphoniques sous écoute. D'instinct. Il possédait une *hot list* de quinze numéros de téléphone cellulaire appartenant à des agents du FBI et à des techniciens de Pac Bell. Des lignes qu'il utilisait lui-même malgré le fait qu'il les savait sur écoute. En effet, le FBI connaissait les utilisations faites par Mitnick et espérait le surprendre, ensuite le localiser. Malheureusement, elles ne pouvaient être mises sous balayage continuel (localisation) puisqu'il fallait permettre à leurs véritables usagers de les utiliser, leurrant ainsi Mitnick. Entre l'activation et la désactivation du balayage, le fugitif parvenait pourtant à les utiliser sans s'inquiéter. Il relâchait aussitôt qu'il sentait que sa trajectoire était remise sous écoute. Littman rapporte que jamais, malgré sa fréquente utilisation de ces quinze lignes, Mitnick ne fut repéré. Le journaliste Timothy Gallwey validera son enquête trois ans plus tard. Non seulement Mitnick n'a jamais été intercepté, mais il semblerait que le bidule se soit retourné contre le FBI lui-même. Comme par magie. Gallway écrit : « C'était comme si ces agents portaient un collier de chien » (Gallwey, 1998). D'autres lignes étaient d'ailleurs mises sous écoute aux États-Unis. Écoutes qui n'étaient pas destinées à Mitnick.

Pourtant, Littman découvre que des techniciens ont été contactés par le fugitif qui les informait tout sourire qu'il savait qu'ils écoutaient malhonnêtement quelqu'un. Comme s'il possédait un sixième sens pour percevoir la mise sous écoute.

Littman s'aperçoit plus tard que si Mitnick parvient si facilement à dérober des logiciels et de l'information avant de brouiller la piste, c'est justement à cause de cette étonnante sorcellerie qu'il exerce sur le téléphone. Le jeune homme parviendra à dérober deux puissants logiciels en s'introduisant dans des systèmes inviolables. Bien sûr il démontrera des aptitudes certaines pour coder. Mais la vraie force du fugitif, celle qu'il faut redouter, c'est sa capacité à commander la téléphonie selon Littman.

Mitnick aurait vraisemblablement réussi quelques *hacks* d'intrusion à première vue « extraordinaires ». L'intrusion du 24 décembre 1994 dans l'ordinateur de l'expert Shimomura (pourtant prévenu) est un fait. Toutefois, Littman croit qu'il s'agissait d'un piège. Que Shimomura aurait laissé la porte ouverte, histoire d'incriminer l'intrusion de Mitnick en l'enregistrant dans des circonstances idéales. Se servir ensuite de cet enregistrement pour le retracer. Si le Japonais eut l'air aussi étonné au lendemain de l'intrusion, c'est qu'il ne savait pas Mitnick capable d'entrer de la manière qu'il l'a faite. Non plus de repartir aussi effrontément sans laisser quelque piste que ce soit. Comment? Encore une fois, le réseau téléphonique couvrait sa retraite (Littman, 1996).

Littman explique la technique utilisée. En fait, c'est John Gilmore, *hacker* blanc de *l'Electronic Frontier Foundation*, qui la lui explique. Le *ip spoofing* consiste à construire un canular d'identification sur la machine hôte en inventant une position farfelue. L'adresse réseau (adresse *ip*) étant un indice numéroté et affiché obligatoirement par toutes machines connectées au net. La technique traditionnelle utilisée par les *hackers* consiste à cacher le *ip* en effectuant un ou des bonds chez d'autres serveurs avant d'atteindre leur cible. De telle sorte que la cible enregistre seulement l'adresse *ip* du dernier bond réalisé et non celle du *hacker*. Malheureusement, une collaboration des propriétaires de serveurs visités

durant ces bonds permet généralement aux enquêteurs de remonter jusqu'au premier signal. Par contre, le *ip spoofing* est né durant une expérience aux États-Unis au début des années 1990. Cette technique permettait à l'usager d'arriver sur sa cible et de lui faire gober une adresse *ip* fantaisiste en jouant sur le *ip* de la cible elle-même. Faute d'indice de comparaison valable, le serveur visité (la machine) n'avait d'autre choix que d'accepter l'identification. Mais comme le rapporte Littman, personne n'avait jamais réussi ailleurs que dans les conditions idéales d'un laboratoire. L'exécuter à distance et en traversant un système téléphonique instable, chaotique, capricieux et où les standards s'affrontent (compétition des centrales téléphoniques), cela relevait du mystère. Mitnick l'a pourtant fait. Comment? L'énigme restait entière au terme de l'enquête de Littman (Gulker, 1998).

Le reporter retient donc, comme principal fait de puissance, cette domination totale du territoire téléphonique exercée par Mitnick. D'ailleurs, il remarque qu'il faudra une astuce humaine pour finalement le retracer. En décembre 1994, Kathleen Carlson, psychologue et agente du FBI, s'interroge sur les fantasmes de Mitnick. S'il utilise un pseudonyme (*El Condor*) inspiré d'un vieux film de Robert Redford, peut-être a-t-il aussi aimé *Sneakers*, encore un film d'espionnage où Redford tient le rôle principal. *Marty* est le prénom du personnage. Elle suggère à Shimomura de vérifier si le nom d'usager (*login name*) *marty* apparaît dans les logs de chez Well, dernier serveur victime d'une intrusion de Mitnick. En effet, il existe un marty. Ils commencent alors à surveiller tous les pseudonymes *marty* qui se contactent au réseau de Netcom. Après une enquête chanceuse, le FBI remonte jusqu'à Raleigh en Caroline du Sud. Leur homme est probablement là. Ils termineront le boulot avec un *scanner* mobile (Cooke, 2001). Sans la clairvoyance de Carlson, pense Littman, Mitnick continuerait peut-être de courir.

Le reporter s'attarde ensuite aux **faits concernant les mobiles** de la créature. cinquante heures de conversation avec Mitnick l'amènent à penser qu'il s'agit d'un gamin : « Il s'exprime comme un homme qui aurait dix ans de moins que ses trente ans » (Littman, 1996). Le reporter repère deux pôles. Le premier

pôle : Mitnick vole du *software* parce qu'il n'a pas d'argent pour se le payer. Il expose une série de faits confirmant sa pauvreté de toujours, sa condition de vie, son peu d'intérêt pour le travail. Par contre, il est pris de désirs intenables pour tout ce qui concerne le *software*. Et pas n'importe lequel. Il aime mettre la main sur le dernier cri. Celui qui n'est pas encore tout à fait terminé ni commercialisé. Son nombre incalculable d'intrusions correspondrait à ce désir de ne pas attendre ni d'acheter. Le second pôle : la farce. Il déclare au journaliste :

> Je ressemble aux meilleurs perceurs de coffres-forts. Je lirai votre journal intime, je ne prendrai pas l'argent et refermerai le coffre sans que vous sachiez que je suis passé par là. Je le ferai parce que c'est super, parce que c'est un défi! (Littman, 1996)

Mais Littman n'y croit pas. Mitnick collectionne les blagues puériles depuis le début des années 1980. Il aime particulièrement les blagues qui auront lieu d'enrager les victimes. Il titille le FBI en s'adressant directement à eux. Il laisse des messages à ses poursuivants. Appelle des techniciens (comme chez Pac Bell) pour les informer qu'ils ont oublié quelques travaux de maintenance importants. Il lit les courriels de Markoff et l'en informe. Toujours faire enrager. Peu importe qu'il soit le seul à rire, il continue depuis toujours. Il s'empare d'un service 411 et répond lui-même aux abonnés, se faisant passer pour un agent du service à la clientèle. Il invente toutes sortes de tours pendables et tient à assister à la colère de ses victimes. Il reprogramme par exemple à distance une boîte téléphonique pour que la voix automatisée demande à l'usager d'introduire sa monnaie. Lorsque celui-ci s'exécute, la même voix lui en redemande. Encore et encore. Pendant ce temps, Mitnick écoute sa victime haleter, jurer, cogner. Il se marre de cette bonne blague et la fait entendre à ses amis. Comme s'il s'agissait d'un jeu d'enfant destiné à provoquer la colère des grands.

Littman reconnaît dans le comportement de Mitnick les mêmes symptômes que celui du joueur compulsif (*gambler*). Malgré plusieurs démêlés graves avec la justice et des peines d'emprisonnement, malgré aussi les risques qu'il court à se faire reprendre, il continue de commettre ses blagues sans

pouvoir s'arrêter. Arrivé à trente ans, considère Littman, il continue de s'adonner aux mêmes jeux adolescents qu'il avait quinze ans plus tôt.

F) Jugements de valeurs et propositions symboliques

L'iconographie de Littman aboutit à un Mitnick capable d'exercer des pouvoirs étonnants sur n'importe quel système téléphonique. C'est bel et bien le modem et le téléphone qu'il faut lui confisquer car ainsi armé, il devient dangereux. S'il démontre un fort niveau de compétence informatique, il demeure cependant un *hacker* intermédiaire plus intéressé par la blague que par la prouesse. Le reporter écrit : « Si Mitnick est dangereux, c'est parce qu'il ne semble pas motivé par l'appât du gain » (Littman, 1996). Il agit par pur plaisir et il est bien incapable de se contrôler. Richard Peek explique la conclusion de Littman :

> En réalité, Littman prétend que Mitnick était un *hacker* dépendant qui aurait certainement quitté sa femme, loué une chambre de motel et commencé à pirater des systèmes toute la journée de la même manière que d'autres gens partent en beuverie ou cèdent à la tentation du jeu (Peek, 1997).

Il serait finalement une sorte de bouffon qui se moque d'un auditoire électronique pour un public constitué de *hackers* noirs en devenir. Littman pense qu'il n'est pas un homme foncièrement menaçant. Il déclare à Keith Stone : « Kevin Mitnick a été tourné en icône, une icône représentant ce qu'on devrait craindre » (Stone, 1996). Ses blagues lui ont attiré des coups et des bosses.

Son visage aurait été instrumentalisé par les accidentés de la malveillance informatique. Littman soutient que le jeune homme a finalement été victime des circonstances. Les mondes électroniques, politiques et judiciaires se cherchaient un exemple et un ensemble de circonstances médiatiques, notamment l'apport du travail de Markoff depuis 1991, ont fait en sorte que le hasard tombe sur lui. Il est devenu l'incarnation même du *hacker* à punir. Ses actes ont aussi pavé la

voie à une jurisprudence qui se cherchait des causes. En bref, Littman suggère que Mitnick soit le symbole même de la fragilité du médium Internet et de l'insécurité de l'information à l'ère du réseau informatisé.

3- Jeff Goodell

A) Contexte d'observation

L'aventure commence en janvier 1995, quelques semaines avant la capture de Mitnick. Le magazine *Rolling Stone* demande à Goodell, collaborateur occasionnel, d'écrire un reportage de 3500 mots sur la saga Kevin Mitnick. Le journaliste se souvient :

> Cela est arrivé à un moment où l'anxiété à propos de la technologie était incroyablement élevée. Le monde changeait rapidement à cause de l'avènement de cette chose appelée Internet. Peu de gens savaient vraiment de quoi il s'agissait. Internet déstabilisait l'emploi par exemple. Il y avait un véritable désir de contenir les débordements. Je pense qu'une partie de cette anxiété était alors canalisée sur Kevin Mitnick (Gulker, 1996).

Malheureusement, Goodell ne parvient pas à contacter Mitnick. D'ailleurs, c'est bien la première fois qu'il s'intéresse à lui. Au phénomène *hacker* aussi. Il décide alors de concentrer son énergie sur les gens qui l'ont personnellement connu. Il réalise donc une enquête sans attirer l'attention puisque les projecteurs sont tournés vers Markoff et Littman qui publient déjà des articles sur l'affaire. Il rencontre tour à tour la famille, des enquêteurs, des policiers, des experts en sécurité informatique, des psychologues, des anciens amis, etc. Il va même jusqu'à rencontrer un brocanteur qui a déjà loué une voiture à Mitnick. Conscient de son inexpérience vis-à-vis du sujet Mitnick, Goodell se tourne résolument vers le *human interest*. Il s'intéresse au côté humain de la créature Mitnick.

L'article paraît dans le *Rolling Stone* au printemps 1995. Il est remarqué à ce point qu'un éditeur (Dell) contacte Goodell et lui offre d'écrire un livre sur la base de ce seul article. Goodell a recueilli tellement de témoignages qu'il se sent à l'aise avec l'idée. Il a le matériel pour un livre de 328 pages. Ce sera *The Cyberthief and the Samurai* publié à l'automne 1995.

B) Antécédents et rapports vis-à-vis du sujet Mitnick

Jeff Goodell est un enfant de la *Silicon Valley.* Fils d'un père entrepreneur et d'une mère employée de la première heure chez Apple, frère d'une sœur propriétaire de *start up* et petits-fils d'un vieil ingénieur excentrique hautement respecté dans le domaine de la robotique, Goodell a toujours manifesté un amour profond pour sa vallée, pour ses gens, pour ses réalisations, pour sa culture si particulière. Goodell est aussi doté d'un incontestable sens de l'humour qu'il exhibe tant dans ses agissements au quotidien que dans ses écrits. Il commença sa vie d'adulte en tant que stagiaire chez Apple mais quitta rapidement en déclarant à ses patrons : « Apple, je pense, c'est comme IBM mais avec des cheveux longs » (Williams, 1997). Il s'exila ensuite à New York le temps de compléter un diplôme en sciences informatiques à la *Columbia University*. Il revint rapidement et annonça à toute famille qu'il gagnerait désormais sa vie sur le net en devenant un journaliste électronique de la première heure (Nous sommes en 1989). Auteur de nombreux articles au *Rolling Stone Magazine*, *New Republic*, *New York Times* et *Wired*, Goodell se révèle comme un investigateur hors pair qui possède de nombreuses connexions (Williams, 1997).

Goodell possède peu d'expérience du phénomène *hacker.* Il sait simplement que Mitnick est considéré par la presse, Markoff en tête, comme un « démon », un « *hacker* noir » et une « menace sociale ». C'est son point de départ (Goodell, 1997).

C) Biais du journaliste

Goodell confie à Chris Gulker qu'il avait, dès le départ, le pressentiment que cette saga Mitnick avait atteint une démesure médiatique et que seule une humanisation du personnage pouvait modérer cette hystérie collective. Il ne se sentait pas à l'aise avec l'idée de démonter le fait technique validant la puissance du *superhacker*. Il reconnaissait que d'autres étaient mieux situés que lui pour interpréter ces faits. En revanche, il espérait découvrir un pauvre bougre. A son avis, ça ne pouvait être que ça. Il adopta alors une stratégie d'enquête visant à révéler le côté « multidimensionnel » du personnage. Toutefois, Chris Gulker le défend d'avoir voulu biaiser le portrait : « (...) son meilleur argument résidait dans le fait qu'il n'entretenait aucune relation émotionnelle ou financière avec Mitnick ou n'importe quelle autre personnalité impliquée dans l'affaire » (Gulker, 1996).

En publiant son reportage dans le *Rolling Stone*, Goodell ne pouvait savoir que cela déboucherait sur un généreux contrat d'édition. Un reportage paru dans ce magazine avait tout pour passer inaperçu. Il avait simplement reçu le mandat d'accoucher d'une brève iconographie. C'est Dell qui saisit l'occasion et contacta Goodell pour essayer de le convaincre d'étirer le texte et d'en faire un livre. Goodell n'accepta pas immédiatement. Chris Gulker soutient que c'est cette mauvaise publicité entourant le travail de Markoff et Littman qui permit à Goodell de s'imposer comme une tierce analyse (Gulker, 1996).

D'autre part, Goodell semble avoir été profondément choqué par cette photo de Mitnick publiée par Markoff dans le *New York Times*. Une photo, rappelons-le, qui montrait un Mitnick gras, le regard vide et le visage mal rasé. Goodell est choqué parce qu'il soupçonne un sale coup de Markoff. Il rassemble lui-même de nombreuses photos connues et datant de 1980. Des photos que Markoff possède assurément lui-même. Parmi toutes, celle choisie par Markoff présente le pire jour du *superhacker*. Pis encore, son visage est quasiment méconnaissable. A croire qu'il s'agit de quelqu'un d'autre, pense Goodell. Le journaliste croit en la diabolisation organisée. Il part donc à contre-pied de

Markoff et oriente son enquête de manière à ce qu'elle puisse humaniser Mitnick. Lui trouver des qualités, des passions, des charmes, etc.

D) Normes et procédures professionnelles

En 1994, Goodell suivit les articles de Markoff et Littman avec beaucoup d'intérêt. Difficile de déterminer si c'est le *Rolling Stone* qui appela Goodell ou l'inverse. Toujours est-il que le journaliste arriva au magazine en possession d'un plan d'attaque. Il lui fallait rejoindre Mitnick d'abord, Shimomura ensuite. Il ne parvint pas à rejoindre le premier. Il décida de mener une véritable traque à Shimomura. Celui-là, personnalité publique, ne pourrait pas se cacher. En effet, ce *hacker* blanc était largement médiatisé par la presse.

Il le contacte d'abord simplement. A son grand étonnement, Shimomura refuse. Il semble même le fuir. Comme s'il était fidèle à Markoff. Le journaliste fouille et découvre que ces deux-là viennent de signer une entente avec Hollywood pour la cession des droits de leur histoire. Le contrat comprend une entente de non-collaboration avec la presse. Une forte somme d'argent leur a déjà été versée. En décembre 1994, Goodell est vraisemblablement le seul journaliste au courant de la situation (Gulker, 1996).

Ses recherches l'amènent pourtant jusqu'à une pente de ski de l'État de Washington où Shimomura donne des leçons. Il appert que la véritable passion de celui-ci soit justement le ski et qu'il tienne à la garder secrète. Goodell décide donc de se hasarder sur les pistes et de pourchasser le *hacker* jusqu'à ce que celui-ci décide enfin de lui accorder une entrevue. Choqué, il refuse puis change d'idée après que Goodell eut réalisé une chute mémorable. L'entretien est à la fois trop court et trop sec pour éclairer le journaliste qui décide finalement d'orienter son travail d'enquête vers d'autres acteurs. Il parvint ainsi à rassembler des dizaines de témoignages de gens qui avaient connu Mitnick de près ou de loin. Il n'obtint aucun refus. Il voyagea donc de San Diego à New York, s'arrêtant aussi à Los Angeles, San Francisco et plusieurs autres villes pour finalement

aboutir à Raleigh les jours suivant la capture du fugitif. Il parle de ses voyages à Gulker avec un certain enthousiasme, ce qui laisse supposer que tout s'était fort bien déroulé (Gulker, 1996).

Goodell reconnaît cependant qu'il était chaque fois précédé par l'image positive du *Rolling Stone* qui l'auréolait de son énergie sympathique. Il y a aussi fort à parier que le sens de l'humour et l'agréable personnalité du journaliste aient joué sur son efficacité à convaincre les gens de lui accorder entrevue. D'ailleurs, aucun d'entre eux ne l'accusa d'avoir publié des déclarations *off the record*. En bref, comme le souligne James Fallows, Goodell a réalisé un travail sans bavure et dans la limite de ses capacités (Fallows, 1996).

E) Énumération des faits retenus : indices de puissance et de mobiles

Goodell passe rapidement sur les **faits de puissance**. Il n'espère pas convaincre son lecteur de la puissance de Mitnick. Il la considère comme acquise. Il dresse simplement un bref inventaire des faits récupérés parmi les plus marquants. D'abord cette histoire de *ip spoofing*, cette technique pourtant jamais réussie à l'extérieur des conditions idéales d'un laboratoire, dont Shimomura aurait été la victime ce 24 décembre 1994. Justement, Goodell préfère dresser la liste des victimes que de faire l'apologie des *hacks*. *Toad.com* (serveur puissamment protégé), appolo.it.luc.edu (serveur situé à la *Loyola University*), Well (le réseau d'information), Netcom (important fournisseur d'accès Internet), et ça continue. Ensuite, il cite les experts Bruce Koball et Mark Lotor pour qui la puissance de Mitnick ne fait aucun doute. Il reconnaît aussi des dégâts. Même si ses estimations se situent bien au-dessous de celles de Markoff, elles atteignent pourtant plusieurs millions de dollars. Mais Goodell précise : « Il n'y a pas de preuve démontrant que Mitnick ait vendu de l'information ou utilisé des données pour causer des dommages commerciaux » (Goodell, 1996). Goodell concède simplement que ses frasques ont coûté quelques centaines de milliers de dollars en réparation, probablement même quelques millions. Il rappelle aussi à quel point les activités de Mitnick peuvent

inquiéter les autorités. Surtout que cela dure depuis fort longtemps, comme le démontre son intrusion dans le *North American Air Defense Command* en 1982.

Goodell reconnaît donc des pouvoirs à Mitnick mais questionne certaines des autres preuves appelées, particulièrement les contenus de ses disques durs au lendemain de sa capture finale en février 1995. Ces 20,000 numéros de carte de crédit retrouvés, avance-t-il, auraient certainement pu être volées par quelqu'un d'autres qui aurait ensuite diffusé la liste sur le net. Goodell accuse Markoff d'avoir bâclé son enquête et d'avoir considéré des preuves qui auraient mérité d'être éclaircies. Mais il n'insiste pas, conscient de sa propre incapacité à démontrer le contraire.

L'informaticien et journaliste David Gelernter souligne que le livre de Goodell manque cruellement de détails techniques (Gelernter, 1996). En effet, l'auteur oriente sa recherche sur les **faits expliquant les mobiles** du *superhacker.* Premièrement, Mitnick serait davantage un comédien qu'une véritable créature des ténèbres. Sa passion pour l'ingénierie sociale le confirmerait. Il aime jouer des rôles crédibles et il y parvient plutôt bien. Deuxièmement, il ne s'est jamais senti très bien dans sa peau. Toutes les personnes ayant bien connu Mitnick l'affirment. A l'adolescence, il aurait découvert que le *phreaking* lui permettait de se fabriquer des avatars et de se faire connaître sur les *party lines.* Il se fabriquait un personnage avec lequel il se sentait bien. Il aimait aussi montrer à ses amis à quel point il était doué pour s'amuser aux dépends des réseaux téléphoniques. C'est d'ailleurs au téléphone qu'il parvint à rencontrer certaines de ses amies de cœur. Il appréciait par-dessus qu'on le félicite pour ses talents.

Par ailleurs, Mitnick aurait grandi dans un milieu dysfonctionnel. Parents divorcés, une enfance instable avec des déménagements fréquents, des demi-frères et demi-sœurs changeants... Goodell apprend même que le jeune Mitnick aurait été la victime de certains abus de la part de beaux-pères criminels. Il atteint sa majorité sans diplôme ni travail et n'a pour seuls amis qu'une bande de voyous *phreakers* dont il était en quelque sorte le meneur spirituel. Ensemble, ils

commettent toutes sortes d'actes bientôt considérés criminels. Une membre de ce gang (Susan) s'adonne à la prostitution et ramène l'argent pour financer les activités. Mais en 1980, ils s'attaquent à un ordinateur de *time-sharing* basé à San Francisco et provoquent une grave destruction de données. L'année suivante, la jeune prostituée décide d'appeler la police et de vendre le gang après que l'un de ses membres (Roscoe) ait rompu sa relation amoureuse avec elle. Mitnick est donc arrêté et se retrouve trois mois dans une maison pour jeunes contrevenants. Goodell pense que cette Susan aurait elle-même détruit les données de ce serveur pour ensuite en accuser le gang. D'autant plus que Mitnick s'était toujours défendu d'avoir commis ce geste (Goodell, 1996).

La vie de Mitnick serait une succession d'incompréhensions et d'injustices. Excédé de toujours rater ce qu'il entreprend, le garçon décide de s'organiser par lui-même. Il accumule ainsi les méfaits. En 1986, il est arrêté par la police pour avoir contrefait une autorisation de crédit lui permettant d'obtenir un prêt pour acheter un ordinateur personnel. Si l'histoire que découvre Goodell a été oubliée par la presse (dont l'enquête de Markoff), c'est que la police l'avait relâché le jour même. La preuve informatique du délit avait mystérieusement disparu le jour même.

Ses amours aussi tournent mal en général. En 1987, il remarque une fille de son âge sur un canal de discussion (*chat line*). Ils se rencontrent, se fréquentent et décident de se marier. Le couple s'inscrit même à un programme d'informatique et Mitnick semble disposé à se prendre en main. Mais la police débarque chez lui et l'arrête pour utilisation frauduleuse de fausses cartes de crédit. Fauché, Mitnick aurait été contraint d'utiliser de faux numéros pour payer ses factures de téléphone. Sur ses disques durs, la police découvre aussi de petits logiciels volés récemment à une compagnie de Santa Cruz et l'accuse. Ce double méfait lui vaut un traitement discutable de la part des policiers. En effet, Mitnick reçoit une baffe supposée accidentelle et contre laquelle il n'obtint aucun recours faute de pouvoir se payer un avocat acceptable. Goodell parle de la détresse de Mitnick comme d'un fait qui allait bientôt le conduire à la rébellion sociale.

En 1989, il sera trahi par son meilleur ami (Lenny DiCicco) qui le vend aux policiers en échange de sa non-accusation. Complice de Mitnick, DiCicco s'était rendu coupable de méfaits importants à l'endroit de *Digital Equipment's Palo Alto Research Laboratory*. Les deux comparses s'étaient adonnés à une compétition de plusieurs mois avec les techniciens. Sentant la soupe chaude, DiCicco vendit son ami. Il se défendit à Markoff d'avoir simplement agit par vengeance après que Mitnick lui ait fait une blague douteuse. Goodell considère comme déterminante cette sentence prononcée contre lui en 1989. Le juge compara la passion de Mitnick à celle du toxicomane pour la drogue dure et l'obligea à purger sa peine parmi des trafiquants. Il traverse une pénible thérapie d'un an durant laquelle il se fait répéter à tous les jours qu'il est affecté d'un grave « désordre mental », qu'il est « obsessionnel » et qu'il doit être soigné. Il accepte de prendre une part active dans sa thérapie (Goodell, 1996).

Quand il est libéré en 1990, Mitnick n'arrive pas à trouver de boulot. Goodell découvre que son agent de probation appelait systématiquement tous les employeurs chez qui il postulait un emploi pour les informer du danger. Écœuré, Mitnick parvient quand même à se trouver du travail dans une entreprise de diffusion électronique située à Las Vegas. Goodell enquête fort dans cette direction et établit que Mitnick ne s'était rendu coupable d'aucune incartade durant l'année qu'il resta à l'embauche de ces gens.

Nouvelle cassure dans la vie de Mitnick : un demi-frère, avec lequel il entretenait des relations affectives très étroites, se tue en voiture après une présumée surdose d'héroïne. Sa femme, de laquelle il est séparé depuis sa détention, lui annonce qu'elle réclame le divorce. Trop, pense Goodell. Cette fois Mitnick se cherche un exutoire. Il part travailler chez *Teltec*, cette entreprise d'investigation, et se livre à tous les méfaits imaginables. Le fait est qu'il récidive pour la première fois depuis qu'il a été relâché. A partir de cette date, il s'en prend au monde entier, n'a plus d'amis et ne fait confiance à personne. Il accepte de porter le chapeau criminel qu'on veut lui faire porter.

Goodell s'attarde aux messages qu'il laisse à ses victimes. Ils expriment un profond dédain pour l'institution, la loi, les techniciens informatiques aussi. Quand Mitnick commence à entendre parler de lui dans la presse, il le prend pour un compliment. Ça l'excite et le valorise. Le journaliste considère que c'est la raison pour laquelle Mitnick contacta directement Littman en 1994. Il voulait s'attirer la gloire et le mérite. Considéré comme un raté par sa famille (son père en avait honte), pauvre, sans diplôme et rejeté par la société, voilà autant de faits qui inspirent à Mitnick une quête débridée pour la reconnaissance de son seul talent : le *hacking*. Et à n'importe quel prix, soutient Goodell. Pour preuve : quand Mitnick s'annonce puis s'en prend au réputé Shimomura, il espère commettre le bouquet final. Geste de folie selon Markoff, geste logique selon Goodell. Il lui fallait prouver une fois pour toute combien il était doué. Parce que, fait ultime validant son mobile, Mitnick sait qu'il ne lui reste plus beaucoup de temps. Avec ou sans l'attaque adressée à Shimomura.

F) Jugements de valeurs et propositions symboliques

Goodell dresse l'iconographie d'un Mitnick détruit par la vie. Au-delà des crimes et de la manifestation de pouvoirs surnaturels, il y aurait un homme qui souffre. Un homme qui aurait trouvé dans le *hacking* sa seule gratification. Démuni, trahi, rejeté, son seul plaisir consistait à défier la compétence informatique d'autrui. Ainsi, il s'assurait la reconnaissance et certainement même la célébrité. Mais pour Goodell, Mitnick c'est davantage la tragédie d'un pauvre type que l'histoire d'un *superhacker* solide aux pouvoirs étonnants. Il souhaite que son iconographie soit diffusée dans la presse et qu'elle inspire un peu plus de compassion. Quelle lui permette aussi de se questionner sur son traitement du phénomène *hacker*. Le *superhacker* n'aurait peut-être pas poussé le bouchon aussi loin s'il ne s'était pas aperçu un jour que tout le pays parlait de lui, pense Goodell. Et en dépit des conséquences qu'il connaissait d'avance, il a choisi ce moment-là pour vivre son quart d'heure de gloire.

Kevin Mitnick serait un symbole vénéré par les jeunes déshérités de la société qui ont trouvé dans l'informatique un instrument de révolte sociale. Par

leur *hacking*, ils exerceraient une pression sur la société branchée en réseau sans but cohérent. Timide, incompris, trompé, tabassé, trop sévèrement puni, Mitnick serait devenu celui qui incarnerait parfaitement leur idée d'un allez vous faire foutre (*fuck and destroy*) électronique capable de faire trembler cette société qui les écœure. Cela expliquerait donc pourquoi tous les marginaux ou autres possédés du médium Internet auraient pris spontanément position pour défendre Mitnick (Goodell, 2000).

4- Les trois iconographies comparées

A) Points communs entre les icônes

Premier point commun. Ces trois icônes sont associées à une puissance basée sur la plausibilité des faits techniques. Au précédent chapitre, j'expliquais pourquoi il était impossible pour le journaliste de décider de la valeur d'un *hack* (Pages 40-41-42-43). Markoff, Littman et Goodell ont donc été contraints de fonder la puissance de leurs icônes en ne considérant que des symptômes. C'est-à-dire des témoignages clé et des évaluations de dégâts résultant de l'expression dudit pouvoir. Cela les a conduit à des icônes aux pouvoirs vraisemblables mais improuvables. Markoff croit Mitnick possédé d'un incontrôlable pouvoir *hacker*, Littman d'une magie capable d'envoûter les systèmes téléphoniques et Goodell d'un don du ciel pour s'introduire dans n'importe quel système. Autant de représentations qui s'accordent sur le caractère surnaturel des aptitudes de Mitnick. Le journaliste Richard Peek est cependant rationnel et rappelle qu'il s'agit toujours ici d'une affaire de probabilité. Il écrit à propos du travail de Littman à ce sujet : « Le reportage de Littman est minutieux, bien documenté, compréhensible, et divertissant. Si j'avais à parier à savoir si les conclusions de Littman étaient exactes ou non, je parierais que si » (Peek, 1997).

Deuxième point commun. Ces trois icônes proposent un portrait inquiétant de Mitnick. A des degrés différents, elles se ressemblent au point de vue du

danger. Mitnick serait une créature menaçante pour ses ennemis. Aussi, une créature capable de mettre ses menaces à exécution. Les icônes dépeintes par Markoff, Littman et Goodell sont redoutables.

Troisième point commun. Aucune intelligence n'est accordée aux propos tenus par l'icône. Bien sûr, Littman citera Mitnick abondamment mais il n'utilisera ce matériel que dans la mesure où cela pourra l'aider à mieux comprendre la situation mentale du fugitif et à collecter des faits techniques. Il censurera tout le reste. Markoff retiendra les insultes qui ont été adressés à lui-même comme à Shimomura tandis que Goodell ne citera tout simplement jamais Mitnick, faute de pouvoir communiquer avec lui. Il laissera aussi tomber les autres déclarations commises par le fugitif. Par conséquent, les trois icônes ne sont pas associées à un discours pouvant être interprété comme une parole d'évangile, un enseignement ou une tentative pour légitimer une cause.

Quatrième point commun. Il s'agit dans les trois cas d'icônes dépeignant un *outsider*, c'est-à-dire un marginal exclus de la société pour qui il n'existerait pas de véritable pendant. Mitnick serait unique en son genre et ce serait pourquoi il valait la peine qu'on y accorde un livre.

B) Différences entre les icônes

Première différence. Chacune des ces trois icônes agirait suivant des mobiles différents. L'icône de Markoff est détraquée. Elle représente un homme fou dangereux emporté par sa maladie mentale. Une icône déraisonnable. Celle de Littman dépeint un farceur compulsif pour qui la blague représente la quintessence du divertissement. Il s'adonne ainsi au *hack* d'intrusion parce que cela l'amuse terriblement. Chez Goodell, l'icône Mitnick représente un cas d'échec. Déshéritée et désabusée de sa vie réelle, l'icône aurait choisi de mener une autre vie (double vie), virtuelle celle-là. L'icône de Mitnick dépeint alors une sorte de super-héros masqué dont le mobile principal consiste à s'attirer la reconnaissance et la gloire en dominant ses ennemis en ligne.

Deuxième différence. Bien qu'elles s'accordent sur l'aspect inquiétant de la créature, les trois icônes s'opposent au niveau de la malveillance dont il faudrait l'accuser d'emblée. L'icône échafaudée par Markoff est cynique et se moque éperdument du genre humain. Elle cherche à causer des torts qui affecteront les gens. C'est là que résiderait toute sa motivation. L'icône de Littman est moins sinistre. Elle représente un farceur compulsif qui manque de maturité et dont l'intention première est de s'adonner à des blagues d'adolescent. Son intention serait bel et bien de se moquer des gens et non de leur causer des torts. Enfin, l'icône de Goodell cherche à attirer l'attention. Son dessein est foncièrement pathétique.

C) Forces de ces iconographies

La première force. Chacune de ces icônes trouve son fondement principal dans le *hack hacktiviste* (*hack* d'intrusion). Les auteurs ont pris le *hack* très au sérieux puisqu'ils le considèrent unanimement comme une condition *sine qua none* à l'existence même de l'icône. Sans le *hack*, pas d'icône *hacker*. C'est donc dire qu'ils ont tous les trois reconnu ce passage obligé. Chacune de ces icônes a été associée à un discours cohérent supposé confirmer la capacité de Mitnick à réaliser des *hacks*. Il s'est agit de témoignages et de faits techniques échafaudés en un même argument (y compris chez Goodell) puis présenté au lectorat. Mais nous l'avons vu au premier chapitre : ces couvertures (lire mesures) du *hack* sont indécidables. C'était vrai pour les *hackers* des sixties, ce l'est encore pour ceux d'aujourd'hui.

La deuxième force. La combinaison de ces trois icônes permet une représentation tridimensionnelle de Mitnick. Évidemment, les icônes s'opposent sur les mobiles du *hacker* et sur la gravité de ses gestes. Cela est dû à un ensemble de **circonstances** impliquant le contexte d'observation, les antécédents de l'auteur par rapport au sujet, son biais de recherche et ses normes (stratégies) professionnelles. Mais un recoupage simultané fournit un

aperçu détaillé et complémentaire de la créature. La circonstance de Markoff l'a conduit à dépeindre Mitnick en adoptant le point de vue de **l'ennemi**. Il a donc rassemblé des faits et des témoignages récupérés chez Shimomura, au FBI, etc. Littman a abouti à une icône en adoptant le point de vue des **commentateurs**. Des gens plus ou moins concernés mais qui avaient une connaissance de Mitnick et de ses agissements. Quant à Goodell, il a adopté le point de vue de **l'entourage sympathique**. La famille et les amis par exemple. C'est ainsi que les trois journalistes sont parvenus à mesurer le *hack* et à lui trouver des intentions. Leurs conclusions seules s'opposent tandis que leurs démarches sont semblables. Il est donc maintenant possible de considérer les faits et les témoignages collectés durant ces trois reportages et de les replacer dans le cadre d'une même couverture. En clair, échafauder de nouvelles hypothèses en procédant d'une construction déterminée par une nouvelle circonstance de recherche.

D) Faiblesses de ces iconographies

La première faiblesse. Chacune de ces trois icônes possède un indice de puissance qui admet la cause surnaturelle. Elles reposent sur un récit de miracles. Le miracle (symptôme) devient l'histoire tandis que le geste précurseur (cause) devient une évidence. L'icône n'admet aucun questionnement sur la nature de cette cause. S'agit-il de pure magie ou de prestidigitation? Impossible de le déterminer sur la base d'un récit de miracles imposé avec faits et témoignages fiables à l'appui. Barthes appelait ça « la déperdition de la qualité historique des choses » (Barthes, 1957). Le mythe fondateur est une inflexion. Une manière de voir les choses. Une conclusion. C'est pourquoi toutes ces icônes aboutissent à une créature *superhacker* dont Markoff, Littman et Goodell se sont faits les chroniqueurs. Le premier la diabolisa, le second la vanta et le troisième l'excusa. Mais toujours, ils respectèrent sa puissance surnaturelle. Bien sûr, les causes restent indécidables au reporter. Pourtant, l'extrême gravité du miracle ne constitue pas une preuve formelle démontrant l'extrême gravité de la cause. Il s'agit ici d'un cas de foi, de conviction, même d'espoir. Le sceptique n'est pas obligé de croire aux seules hypothèses connues pouvant expliquer un

phénomène paranormal. Citons par exemple ces *crop circles* tant répandus au Royaume-Uni et pour lesquels la science ne possède aucune explication (Herbe brûlée, présence d'un taux anormal de chlorophylle, tracé parfaitement circulaire, etc.). L'ufologue suggère l'atterrissage de soucoupes volantes. Faut-il y croire? Par analogie, les trois icônes de Mitnick supposent pourtant que si. Néanmoins, le récit des miracles (celui qui prête foi et/ou argument à des causes surnaturelles) est parfaitement récupérable pour éclairer les mobiles de l'icône.

La deuxième faiblesse. Ces icônes n'admettent pas la **peur**. Mitnick serait un détraqué chez Markoff, un farceur compulsif chez Littman et une victime de la société chez Goodell. Si Mitnick a peur, il le cache très bien. L'icône est infaillible. Ses agissements ne seraient jamais motivés par ce sentiment. Pourtant, Littman cite souvent sa peur sans la remarquer. Mitnick lui déclare que s'il n'a plus le choix de lire les courriels de Markoff en pénétrant le serveur du *New York Times*, c'est parce qu'il espère ainsi en savoir davantage sur l'avancement de sa filature. Chez Markoff, ce sentiment est inexistant. Il s'agit pour lui d'une créature « malicieuse » qui causera le mal sans état d'âme. Chez Goodell, Mitnick est motivé par un désir d'autodestruction. Étrangement, ces trois icônes oublient presque de signaler que Mitnick est fugitif et activement recherché depuis trois ans.

La troisième faiblesse. Les propos de Mitnick sont considérés comme de pures élucubrations. Comme si son discours était un détail secondaire à l'événement. Markoff se contente de rapporter les mots de haine que Mitnick adresse à ses ennemis. Littman le cite abondamment dans le but de dresser son profil psychologique plutôt que pour en tirer un discours cohérent capable d'expliquer ses agissements. Goodell n'a pas confiance aux vieilles citations qu'il glane dans la presse. Il affirme avoir de mal à les contextualiser. En bref, ces trois icônes ont un point en commun : elles sont dépourvues d'un quelconque discours légitimant.

E) Vers une contre-icône

D'une part, chacune de ces icônes est fondée sur un ensemble de faits de puissance qui défendent l'hypothèse d'un pouvoir surnaturel. De l'autre, un échafaudage de faits concernant les mobiles suggère les intentions qui se cachaient vraisemblablement derrière les agissements de l'icône Mitnick. Nulle critique possible au niveau de la démarche car le *hack* relève du domaine du plausible et le mobile du domaine du débat. Impossible de distinguer le vrai du faux, le fait du contrefait, la vérité de l'erreur. Mais, comme le pensent plusieurs *hackers* (Brian Martin par exemple), le *hack* d'intrusion est un événement fortuit et non l'expression d'une force surnaturelle pouvant être systématisée (Martin, 2000). Il s'agit-là d'un biais de recherche qui n'a pas été essayé par nos trois reporters et qui correspondrait pourtant mieux à l'idée que se font les *hackers* de la véritable pratique du *hacking* d'intrusion. Car le biais des Markoff, Littman et Goodell induit l'idée de **facilité** dans le *hack*. Cette idée élimine des mobiles. Par exemple, celui de la quête du danger. Un *superhacker* en plein contrôle craindrait-il de se voir piégé sur le terrain de sa magie? C'est pourquoi la scène *hacker* (appellation courante de la communauté) a si durement critiqué leurs conclusions qu'elle jugeait farfelues. Pourtant, ces reporters ont procédé d'enquêtes rigoureuses qui ont permis de rassembler une incomparable somme de faits. Des faits authentifiés par d'autres enquêtes menées ultérieurement par des reporters comme Rosenberg, Peek, Gulker, etc.

Chaque conclusion a été l'aboutissement d'une série d'étapes. Nous avons vu que la conclusion dépendait du contexte, de l'antécédent vis-à-vis du sujet, de la norme professionnelle et surtout du biais de recherche. Le prochain chapitre consistera donc à parcourir le même chemin pour aboutir à un article de 3500 mots mais en adoptant un biais résolument différent. D'emblée, le biais conducteur considérera que le *hack hacktiviste* (d'intrusion) n'est pas le résultat de l'expression d'une magie mais l'aboutissement d'un ensemble de connaissances, d'audace, de chance, d'opportunités et de ruses. Que le *hack* n'a

rien de facile et qu'il reste un événement rare aux conséquences incertaines. Ce seul biais conduira inévitablement à de nouvelles conclusions au sujet des mobiles de Mitnick, celles-là plus recevables pour la scène *hacker*. Et si ce portrait était réellement diffusé, il fournirait à la presse une quatrième vue (dimension) de Kevin Mitnick, celle-là plus refroidie vis-à-vis de la véritable puissance *hacker* de l'icône.

Chapitre 4 - Kevin Mitnick : contre-iconographie d'un *superhacker*

Après l'icône détraquée de Markoff, l'icône compulsive de Littman et l'icône victime de Goodell, maintenant l'icône extrême. Une icône excessive qui carbure à la peur en poussant jusqu'à la limite du danger sa recherche d'adrénaline. Mitnick n'était pas un magicien possédé par des pouvoirs surnaturels et il le savait. Mais Markoff, Littman et Goodell, obnubilés par leur foi pour le surnaturel, n'ont rien vu. Leur biais de recherche ne leur permettait pas de remarquer combien Mitnick était avide de sensations fortes et combien il était prêt à risquer pour elles. Les trois l'ont cependant prétendu présomptueux et sûr de son pouvoir. Un tel portrait ne pouvait s'accorder avec l'idée d'un Mitnick excité par le danger. J'arrive à cette conclusion en reprenant les faits rapportés par les enquêtes de ces trois reporters et en les combinant avec d'autres faits apparus depuis. Voici un article de 3500 mots.

Les émotions fortes de Kevin Mitnick le « *superhacker* »

Par Jean-Sébastien Coutu
Avril 2002

Relâché en janvier 2000 après 54 mois d'incarcération, le hacker Kevin Mitnick continue de susciter la peur. Étroitement surveillé depuis, la justice lui refuse jusqu'à occuper un boulot de caissier dans un fast-food. Portrait d'une créature aux pouvoirs supposés extraordinaires.

Chaque fois que le matricule 89950-012 quittait sa cellule pour se saisir du téléphone, les gardiens étaient sur le qui-vive. De sa prison à sécurité maximale de Los Angeles, ce petit homme aux manières délicates était présumé capable de déclencher la mise à feu d'un missile intercontinental en sifflant trois fois dans

le combiné. Quinze minutes par jour ouvrable. C'est tout ce que la cour lui avait accordé. Et encore, ses appels étaient sous écoute.

Les poches vidées, les chevilles menottées jusqu'aux douches, on défendit finalement à Kevin Mitnick de posséder quoi ce soit. Le mélomane dût se priver de son walkman. Il fut même envoyé au trou après été surpris en train de collectionner des boîtes de thon (64 boîtes). Plus tard, on l'y renvoya pour avoir osé utiliser la télécommande pour changer la télévision de chaîne au salon des détenus. Explications du directeur de la prison : « Mitnick est tellement dangereux qu'il serait bien capable d'abîmer notre système d'intercom. » Enfermé dans une prison réservée aux pires criminels de l'état (accusés de meurtre, viols, kidnapping, hold-up, attentats piégés, etc.), Mitnick commente sa vie quotidienne au milieu de ses compagnons : « Tout le monde ici passe ses journées à regarder la télévision, jouer aux dominos, s'affronter au poker. Moi je travaille sur ma défense quatorze heures par jour. » Mais mal lui en prit le jour où il réclama qu'on lui fournisse un bloc-notes (laptop) pour préparer cette défense. Le juge choisit plutôt d'imprimer l'ensemble des documents de cour (deux millions de pages pour commencer) et de les charger sur des chariots pour ensuite les rouler jusqu'à sa cellule. Malgré tous les efforts du personnel, il fut impossible d'entrer toute cette paperasse dans une même cellule. Ni même dans trois. Le juge lui accorda donc la permission d'utiliser un bloc-notes par intermittences, à condition que celui-ci soit inspecté après chaque utilisation. C'est donc ainsi que Mitnick vécut sa détention (sa sixième). Celle-ci dura 54 mois.

Un beau matin de septembre 1998, il apprend qu'une bande *hackers* vient de déflorer le portail du *New York Times*. Consternation. Le populaire quotidien américain affiche un écran noir au centre duquel trônent des femmes nues et quelques slogans orduriers. Des milliers de lecteurs ont le temps de lire la revendication : « Libérez Kevin ». Un message haineux est spécialement adressé à John Markoff. Celui-là est journaliste d'investigation et auteur d'un best-seller (*Takedown*) racontant les plus noires péripéties qui ont conduit le *superhacker* en prison. C'est le journaliste Doug Thomas (*Wired*) qui annonce la

nouvelle au téléphone à un Mitnick qui s'écrie : « Mon Dieu, comme si j'avais besoin de ça! ».

Des *hackers* du monde entier se mobilisent pour défendre la liberté en ligne et font de Mitnick un symbole. Un site vend des milliers de t-shirts barrés d'un *Free Kevin* jaune. Un autre fabrique des bannières. Ou des casquettes. « Le gouvernement américain veut faire de Mitnick un exemple: il est un bouc émissaire », déclare Brian Martin (*Jericho*), un *hacktiviste* bien connu. Il poursuit : « Avec cette affaire, le gouvernement a voulu envoyer un message à tous les *hackers*, mais elle a surtout contribué à nous diaboliser tous. » En effet, le gouvernement américain redoute ce que le sénateur Sam Nunn appelle « le prochain *Pearl Harbor électronique* » dans un discours enragé. Le *hacker*, cet ennemi de nulle part et de partout à la fois, menace le pays.

Relâché en janvier 2000, Mitnick s'est immédiatement retrouvé sans le sou. Son passé de *hacktiviste* et les conditions de sa libération ne lui permettent pas de travailler dans un endroit où il existe un accès à un quelconque dispositif informatisé. Comprendre ici une caisse enregistreuse, le panneau d'un système d'alarme, un intercom mobile (*head set*) ou même un téléphone. Dans de telles conditions, impossible de trouver du boulot. Pis encore, une loi américaine interdit maintenant aux criminels de profiter financièrement du récit de leurs actes. Le *superhacker* a donc été contraint à vivre de l'aumône de ses supporters.

La créature Mitnick

Enfant du divorce, décrocheur du secondaire et dépourvu d'argent de poche, Kevin Mitnick passe son adolescence à squatter les *RadioShack* californiens des années 70. Il les fréquente assidûment et profite de la distraction des vendeurs pour utiliser les micro-ordinateurs en démonstration. Sinon il passe son temps à jouer avec ses *boxes*. En 1979, le phénomène *phreaker* divertit la jeune Côte Ouest américaine. Des adolescents dégourdis bidouillent des petites

boîtes de métal capables d'émettre des tonalités qui trichent les systèmes de reconnaissance analogiques du téléphone. Pour une poignée de dollars, n'importe quel gamin peut mettre la main sur une *box*. Des *party lines* s'organisent, on ne paie plus le moindre tarif interurbain et le téléphone devient le théâtre des pires pitreries. L'industrie du téléphone était alors incapable d'endiguer le phénomène.

C'est dans un *party line* que Mitnick fait la connaissance de Roscoe, le chef d'un gang de *phreakers* avancé qui se vante d'être le plus expert de l'état. Ensemble, ils s'adonneront à une toute autre forme de *phreaking* qui finira par impliquer l'usage de micro-ordinateurs équipés de modems payés par la prostitution de Susan Headley, la petite amie de Roscoe. De 1979 à 1981, ils parviendront à s'introduire dans d'innombrables systèmes de sécurité, premiers postes avancés d'un parc informatique californien qui commençait à s'interconnecter. Mais la vie de Mitnick bascule quand Susan se fâche avec Roscoe. Elle livre le gang aux policiers. Une entreprise de San Francisco porte plainte pour une mystérieuse affaire de destruction de données. La justice, mal à l'aise avec l'idée de condamner des jeunes qui avaient commis un crime pour lequel il n'existe pas encore de loi (ni de nom), décide d'envoyer tout le monde séjourner trois mois dans une maison pour délinquants. Mitnick associe donc son nom au premier délit d'intrusion à paraître dans les annales judiciaires.

1983. Un technicien de la *University of Southern California* (USC) surprend Mitnick en train d'utiliser un micro-ordinateur de laboratoire sans permission. Cet élève n'est pas inscrit. Chose extraordinaire, un second coup d'œil révèle que Mitnick était connecté à un ordinateur du Pentagone. Le technicien n'en revient pas et appelle immédiatement la sécurité. Seconde condamnation : Mitnick doit purger six mois dans un centre de réhabilitation (*Karl Holton Training School*, Stockton). A sa sortie, il s'achète une vieille Nissan, demande au bureau des immatriculations qu'on lui inscrive « *X Hacker* » sur sa plaque, puis s'évapore.

1986. Mitnick est arrêté une troisième fois après avoir été soupçonné de fraude. Il aurait contrefait une autorisation de crédit pour l'achat d'un micro-ordinateur. Mais quand il est appelé à comparaître, il appert que la preuve informatique a été effacée des registres depuis. La justice maudit le système puis le relâche.

1987. La police défonce la porte de son appartement et lui saute à la gorge. Il reçoit même une baffe dans la mêlée. Il est accusé d'avoir utilisé des numéros de cartes de crédit volées pour payer ses factures de téléphone. L'examen de ses disques durs révèle la présence de logiciels récemment volés à une entreprise de Santa cruz. Cette quatrième arrestation lui vaut une sentence de 36 mois de probation.

1988. Robert Morris, étudiant à la *Cornell University* et fils d'un ponte de la *National Security Agency* (NSA), bricole un « vers » et le lâche sur le réseau. En l'espace de deux jours, 10 à 15% des 60,000 ordinateurs connectés à l'Internet tombent en carafe. L'armée américaine et la NASA sont parmi les plus durement touchés. Il plaide coupable à plusieurs centaines de milliers de dollars en dégâts et est condamnée à 36 mois de probation, 400 heures de travaux communautaires et à 10,000$ d'amende. Manque d'opportunisme, Mitnick se fait ramasser pour une cinquième fois l'année suivante. Maintenant, la justice est beaucoup moins indulgente. Il est accusé de s'être introduit dans les ordinateurs de MCI et *Digital Equipment Corporation*. Il est le premier à véritablement faire les frais de la loi américaine de 1986 sur les crimes informatiques graves. Il passe une année en prison et six autres mois dans une maison de thérapie pour toxicomanes. Le juge compare sa récidive pour l'intrusion à celle du toxicomane pour la drogue dure.

1991. Il sort donc cette année-là mais s'empresse de violer ses conditions de remises en liberté. Il accuse son agent de probation de l'empêcher de se trouver du travail. Celui-ci préviendrait trop sévèrement les employeurs potentiels qui ont encore envie de faire confiance à Mitnick. Il prend un faux nom et part refaire sa vie à Las Vegas un moment, puis déménage à Seattle où il occupe des

emplois dans le renseignement privé. Son employeur (*Tectec Investigations*) témoigne de son talent pour dérober n'importe quel renseignement sensible. Mais quand ledit employeur est mis sous enquête par le FBI pour pratiques illégales, Mitnick choisit de s'enfuir.

Débute ensuite la plus invraisemblable des chasses à l'homme. Mitnick est considéré comme très dangereux. De 1992 à 1995, il accumule une série d'intrusions allant de la falsification de son dossier de conduite au vol de données militaires en passant par le bris de dispositifs informatiques, l'usurpation de comptes d'accès personnels, la rapine de cartes de crédit et l'occupation illégale d'espaces disque appartenant à de puissantes institutions (Motorola, Fujitsu, Nokia, Sun, Novell, Nec, etc.). Il signe ses intrusions *El Condor*. Des dizaines d'agents du FBI, du CERT, de la NSA et même de la *US Air Force* sont affectés à la capture du fugitif. Excédée par les commentaires de la presse qui prétend Mitnick impossible à retracer, la poursuite y va d'efforts extraordinaires. Le FBI place même son nom sur sa liste des *Most Wanted*. Il faut briser les ailes du condor. Pendant ce temps, John Markoff excite la presse en publiant une série d'articles dressant de Mitnick le portrait d'une créature maléfique se riant de ses poursuivants. En effet, le journaliste a déjà publié un travail d'enquête en 1991 intitulé *Cyberpunk* dans lequel il s'est longuement attardé au phénomène Mitnick. Il s'impose comme le grand spécialiste et prépare déjà un second livre en 1995.

Plutôt que de se terrer, Mitnick choisit de narguer ses poursuivants publiquement en contactant Jonathan Littman, un journaliste indépendant. Il lui fait le récit au jour le jour de ses péripéties, lesquelles se retrouvent dans la presse du lendemain. Il s'en prend aussi directement à Shimomura, un *hacker* de grande réputation, en s'introduisant dans son ordinateur la veille de Noël 1994. Mandaté par une société privée et appuyé par le FBI, Shimomura décide de se lancer à sa poursuite. Ce sera lui, qui en février 1995, finira par localiser le fugitif : il est à Raleigh, en Caroline du Sud. Une antenne d'écoute de type *Tampest* arpente les rues de la ville durant plusieurs heures à la recherche du signal. Les techniciens du FBI arrêtent finalement leur choix sur l'appartement

202 d'un immeuble à logement. La porte est enfoncée et les policiers se saisissent d'un Mitnick étonné. Quand Shimomura arrive sur les lieux, le fugitif s'adresse à lui : « Je respecte tes talents ».

La preuve est accablante. Les disques de Mitnick sont gravés de logs prouvant ses connexions à des serveurs piratés. Il a aussi 20,000 numéros de cartes de crédit en sa possession et de nombreux logiciels. La plupart n'ont pas encore été commercialisés et leur développement est évalué à plusieurs dizaines de millions de dollars.

Incarcéré pour la sixième fois, Mitnick reste 49 mois dans sa cellule avant d'obtenir son procès. Un record absolu dans les annales de la justice américaine. Les charges retenues contre lui n'étaient pas satisfaisantes au goût du juge. Il plaide finalement coupable à 5 des 24 chefs d'accusation et obtient une libération conditionnelle au terme d'une peine totale de 54 mois.

Depuis, sa légende n'a fait que croître. Les journalistes Markoff, Littman et Goodell ont publié respectivement *Takedown*, *The Fugitive Game* et *The Cyberthief and the Samurai*. Des livres qui dressent de Mitnick le portrait d'une créature possédée de pouvoirs surnaturels. Un mythe qui continue de grandir avec la sortie récente de plusieurs films inspirés de l'affaire (*Operation Swordsfish*, *Hackers* et *Takedown*).

Pourtant, nombreuses sont les personnes qui contestent les pouvoirs de la créature, à commencer par Mitnick lui-même. Il déclare en entrevue : « Quand j'entends parler de moi dans les médias, je ne me reconnais pas. Mais j'avoue que le mythe Kevin Mitnick est finalement plus intéressant que la réalité de Kevin Mitnick. De toute façon, personne ne s'intéresserait à cette ennuyeuse réalité. » Il l'admet lui-même : « Je ne maîtrise aucun langage de programmation ». Il se décrit plutôt comme un opportuniste qui savait profiter des faiblesses du genre humain pour obtenir les informations essentielles à ses intrusions. C'est son aplomb extraordinaire et ses talents de comédiens au téléphone qui lui auraient

permis de déjouer tant de systèmes. Cette technique s'appelle le *social engineering*. Elle consiste à tromper son interlocuteur en se faisant passer pour un co-usager légitime du système. Mitnick se souvient d'avoir abusé de la naïveté de nombreuses secrétaires qui lui cédaient volontiers leur mot de passe après qu'il se soit identifié comme un technicien chargé de la maintenance du réseau. Le reste relevait du *script kidding*, activité qui prime l'utilisation de logiciels programmés par d'autres pour achever la besogne d'intrusion. Ses coups les plus brillants, spécialement ceux des derniers temps précédant sa capture de février 1995, avaient été commis avec l'aide de logiciels dérobés chez *Whole Earth Lectronic Link* (WELL) à Sausalito. L'un d'eux avait été programmé par Shimomura lui-même. Mitnick l'avoue finalement : il ne partageait avec les *hackers* que la passion de la connaissance.

Le *hack* de Mitnick refroidi

Dans le film *Operation Swordsfish*, l'acteur Hugh Jackman s'introduit dans des systèmes sans trop d'efforts. Ses moniteurs défilent des bandes de codes sans égard pour la réelle vitesse de rafraîchissement de ce type d'appareil. Essentiellement, Jackman réussit ses *hacks* par imposition des mains. Tout au plus, pianote-t-il aléatoirement quelques touches sur son clavier. Cette représentation du *hack* a la vie dure puisqu'elle date du film *WarGames* sorti en 1983.

L'essence même du *hack* est cependant incompatible avec l'idée de facilité. Dans les années 1960, les jeunes physiciens de Stanford, MIT et Carnegie Mellon décernaient des badges honorifiques aux programmeurs les plus doués d'entre eux. Le *hack* consistait à repousser les limites de l'ordinateur jusque dans ses derniers retranchements. A innover. En 1966 par exemple, un certain Richard Greenblatt parvient à programmer un jeu d'échec qui triomphe de bons joueurs. Plus tard, les années 1970 considéreront les *hackers* comme les plus brillants usagers du hardware. L'informatique, jusque-là réservée aux institutions et à ses membres, commençait à se démocratiser. En 1977, Steve Jobs et quelques acolytes parviennent à assembler un micro-ordinateur

commercialisable. Les années 1980 seront celles des programmeurs. Les meilleurs concepteurs de jeu obtiennent reconnaissance. C'est finalement à partir de 1990, avec l'explosion de l'Internet, que le *hacking* d'intrusion commence véritablement à occuper toute la place. D'une part la cryptographie avec *l'Electronic Frontier Foundation* en tête qui parvient par exemple à briser une clef de 56 bits en 1997. De l'autre, les *crackers* qui s'adonnent à l'intrusion des serveurs. Les *Masters of Deception*, *Legion of Doom*, *Hacking for Girlies* et autres gangs populaires s'attirent une notoriété certaine en réussissant des coups d'éclat.

Les frasques de Mitnick n'impressionnèrent pas la *scène hacker* qui continue de bouder le *social engineering*. Le *hacking* renvoie à une pratique technique détachée du facteur humain. C'est la machine qu'il s'agit de défier. Selon les dires de Shimomura, 85% de la science de Mitnick n'était qu'une habile synthèse de *script kidding*, de fraude téléphonique et de *social engineering*. Shimomura exprima toujours son mépris pour Mitnick qu'il qualifiait de « peu intelligent », « nul en programmation » et simplement « nuisible ». Un avis partagé par l'ensemble de ses poursuivants dont l'équipe tactique du CERT (*Computer Emergency Response Team*) et celle du FBI. Le *social engineering* dont aurait abusé Mitnick demeure l'une des activités les plus méprisées par les *hackers* qui n'y accordent pas la moindre valeur technique.

Dans une entrevue accordée à Ed Bradley pour l'émission *60 Minutes*, Mitnick confirme sa bouffonnerie. Pour obtenir les codes des téléphones cellulaires Motorola, rien de plus simple : il s'agit d'appeler le support technique en se faisant passer pour un représentant sur la route. Ensuite, de demander les plans de la nouvelle génération d'appareils TAC. L'information est immédiatement télécopiée.

Keith Rhodes, directeur technologique au *General Accounting Office*, explique à M.J. Zuckerman (*USA Today*) : « Ecoutez, si je parviens à vous convaincre de me donner le mot de passe, j'entre. Pour ça, je n'ai besoin d'aucune habileté technique ».

Sensations fortes

Les véritables intentions de Mitnick restent floues. « Un *hacktiviste* agissant pour la liberté d'accès à l'information », disent les supporters du site www.freekevin.com En effet, Mitnick émergea en 1991 dans un contexte coïncidant avec la première formulation du *hacktivisme* par le *Critical Arts Ensemble*, un groupe d'artistes américains qui prônait la désobéissance civile électronique. Le *hacktivisme*, voile de légitimité dont se drapent les *hackers* d'intrusion depuis, consisterait à défendre une cause en préconisant le *hack*. Ainsi, la guerre du Kosovo fut l'occasion pour une bande de *hackers* serbes de dénoncer l'attitude de l'OTAN en massacrant arbitrairement quelques dizaines de serveurs américains. Au hasard bien sûr. Mais chez Mitnick, nulle cause défendue. Pas même celle d'une démocratisation de l'information. Sans cause particulière, il aurait simplement agit par goût du risque. Un flirt avec le danger. Il déclare au journaliste Littman : « C'est le contrôle, la puissance, l'adrénaline ».

Et Mitnick est conscient du danger. A partir de 1991, il décide de ne plus endommager les systèmes qu'il visite. Au terme de son procès de 1999, le juge convient qu'il n'a rien détruit ni tiré quelque profit que ce soit de ses activités. En clair, Mitnick connaissait la loi et il était terrorisé à l'idée d'une condamnation pour un tel crime. En revanche, narguer des institutions en s'introduisant secrètement dans leur système restait une activité peu risquée. Il s'insurge depuis: « J'ai été trop sévèrement puni! » Mais poursuit : « J'étais un enfant qui agissait pour le plaisir. Je ne peux pas changer le passé. Mais je sais que je peux être pardonné ».

Le plaisir de l'adrénaline. Un *hacker* anonyme explique sur *BigWonk* : « Le *Hacking* c'est seulement une autre manière de s'injecter une dose d'adrénaline dans le corps ». Le *hacking* d'intrusion intéresse de plus en plus les psychologues. *L'Hôpital McLean* de Cambridge a été créée en 1996 pour soigner les malades du net, spécialement les *hackers*. La psychiatre Maressa Orzack estime que cette quête de l'adrénaline en ligne représente une véritable drogue à accoutumance. Une excitation fantastique s'empare du *hacker* en train de

s'introduire dans un lieu défendu. *FozZy*, un *hacker* français : « Pour isoler le réseau local du reste du monde, ces rusés admins ont donc inventé le *firewall* (mur de feu en français, of course). Ce mot déclenche chez le pirate en herbe comme chez le vieux routard du net un frisson d'adrénaline ». Maressa Orzak explique : « Nous ne pouvons malheureusement pas les traiter comme des alcooliques car l'abstinence n'est pas possible dans un monde d'ordinateurs ».

Dans un article publié en septembre 1998, le journaliste Michael Surkan (*PC Week Online*) assimile le *hacktivisme* à du terrorisme. Un terrorisme souvent sans cause. Il écrit : « Les *hackers* ne portent pas de revolvers et ne font pas exploser de bombes, mais ils sont possédés par le désir terroriste de contrôler les autres. Que vous posiez une bombe à un endroit où on l'attend le moins ou que vous trouviez une faille permettant de pénétrer le système informatique d'une entreprise, la montée d'adrénaline est la même ».

Mitnick a finalement trouvé du boulot cette année. Un boulot loin des préoccupations *hacker*. Il donne des conférences sur le *social engineering*.

Conclusion

Le *hacking* est une activité peu théorisée et dont le mot lui-même ratisse large. Le philosophe finlandais Pekka Himanen, auteur de *L'Éthique hacker*, déclare à *Libération* que Socrate est son *hacker* préféré. Il s'explique :

> Toute son attitude, cette relation passionnée et modeste au savoir, 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 (Latrive, 2001).

Socrate, peut-être. Chez Himanen, le *hacking* est une attitude bien plus qu'une capacité. Une telle représentation du *hacker* flatte l'incapable et minimise l'idée même de la prouesse. Là-dessus, le débat est lancé. Mais une chose est sûre. Le *hacker* commet un *hack*. Il réalise un accomplissement assisté par ordinateur pouvant lui attirer la reconnaissance ou la désapprobation. Ce sera sur la seule base de ce *hack* que seront jugés ses pouvoirs. Le jeune *Mafiaboy*, auteur d'un *hack* par saturation sur des sites de vente en ligne, accomplissement à la portée de n'importe quel quidam, ne reçut pas la moindre considération. Ni de la part des *hackers*, ni de celle de la presse. En revanche, quand John Gilmore de *l'Electronic Frontier Foundation* parvint à casser une clef d'encryption de 56 bits en 1998, cela en moins de soixante heures, il s'attira les plus beaux compliments. Cet accomplissement relevait presque du miracle compte-tenu que les organisateurs du concours (RSA Inc, prestigieux fabricant de logiciels d'encryption) avaient déclaré qu'il en prendrait dix ans à tous les ordinateurs interconnectés du monde pour découvrir la clef.

J'ai expliqué dans le premier chapitre que le *hack* était soumis à supputation. Des gens de tous les horizons, qu'ils soient informaticiens, philosophes, écrivains, etc., mesurent les *hacks* et accordent une considération aux capacités de leurs auteurs. Mais si le *hack* reste sujet à toutes les

interprétations, sa réalité informatique exclut toutes les causes surnaturelles. Un ordinateur ne s'active pas par magie. Son *output*, le *hack* donc, est le résultat d'une manipulation réalisée à l'intérieur de ses limites, de ses règles et de ses logiques d'opération. L'agitation folle des mains au-dessus du clavier, comme dans le film *Operation Swordfish*, n'accouchera pas d'un *hack*.

Dans le deuxième chapitre, j'ai exposé ce manque de scepticisme de la part de la presse qui tolère aisément l'idée de l'intervention surnaturelle comme étant la cause des *hacks* les plus extraordinaires. Particulièrement ceux concernant les *hacks* d'intrusion. Puisque le *hack* est le résultat d'un événement (geste) fini, le journaliste est contraint à l'observation de symptômes. La cause s'est évaporée. Elle s'évapore alors même que le *hacker* procède avec son *hack* car l'interface de l'ordinateur (l'écran) est un dispositif affichant des symptômes. C'est ainsi que le canular Valor embarrassa la presse en 1998, cela même si des journalistes avaient pourtant assisté à ses passes in situ.

J'ai aussi expliqué pourquoi la presse est si vulnérable devant le phénomène *hacker*. Le journaliste est contraint d'évaluer la qualité d'un *hack* en fondant son analyse sur des apparences, laissant toute la place au plausible. Les causes du *hack* restent invisibles. Ses symptômes demeurent le seul matériel avec lequel le journaliste peut travailler pour établir son jugement. Ce symptôme prend la forme de témoignages, de rapports (logs) incomplets, d'aveux, etc. Bref, de données de seconde main.

Rolland Barthes disait que le mythe « déformait », qu'il était une « inflexion », c'est-à-dire une manière d'interpréter l'histoire. Une histoire soufrant de la « déperdition de la qualité historique des choses ». En convenant que les *hacks* extraordinaires sont la conséquence de gestes extraordinaires, le journaliste procède d'un raisonnement qui infléchit l'histoire. Justement, le journaliste est obligé d'adopter cette inflexion. Il occupe une position de médiateur qui le contraint à choisir parmi des faits pour ensuite proposer une représentation de l'événement. C'est ainsi que la presse choisit Kevin Mitnick. Pourchassé par plusieurs institutions, dont le FBI qui en fit un *Most Wanted*,

passible d'une peine d'emprisonnement de 460 ans et imputé de dégâts évalués à 80 millions de dollars, la presse fit de lui une icône *superhacker* aux pouvoirs surnaturels. Un mythe indémontable, faute de preuves. Il ne restait plus que des indices pouvant défendre une représentation plausible des pouvoirs et des intentions du personnage.

La presse fut durement accusée d'avoir contribué à diaboliser Mitnick. Un diable redouté parce que capable de déchaîner ses pouvoirs, c'était le portrait. Mais les autres *hackers*, s'ils défendaient la créature, ne lui reconnaissaient pas de véritables pouvoirs. Brian Martin (alias *Jericho*) collabora personnellement pour démonter la preuve technique appelée à la cour et ainsi défendre Mitnick (Richard, 1999). Pour Martin, les pouvoirs de Mitnick étaient une légende et il accusait la presse de l'avoir écrite. Peirce avait théorisé ce phénomène en 1938 en écrivant que l'icône « est un signe possédant un rapport de ressemblance avec la chose qu'il représentait ». Il ajoutait : « L'icône est un signe qui posséderait le caractère qui le rend signifiant, même si l'objet n'existait pas » (Peirce, 1978). Selon Martin, la presse avait justement dressé le portrait d'une créature qui n'existait pas.

Dans le troisième chapitre, j'ai analysé les couvertures de trois journalistes d'enquête (Markoff, Littman et Goodell) qui ont tenté de dresser un portrait plus éclairé de Kevin Mitnick. Plus précisément, un jugement de valeurs au niveau de ses pouvoirs et de ses mobiles. Leurs conclusions ont été influencées par une série de facteurs auxquels ils ont tous été confrontés : un contexte d'observation, des antécédents vis-à-vis du sujet, un biais personnel et l'adoption d'une stratégie d'enquête. Leurs couvertures les ont conduits à exprimer de vifs désaccords concernant les véritables intentions (mobiles) de Mitnick. Toutefois, ils se sont entendus pour reconnaître des pouvoirs extraordinaires à l'icône.

En considérant que le *hack* ne pouvait impliquer une quelconque manifestation surnaturelle, j'introduisais un quatrième biais. J'étais maintenant capable de reprendre la richesse de leurs couvertures pour en tirer une iconographie plus fidèle à la réalité. J'ai donc commis un article de 3500 mots au

quatrième chapitre qui reprenait les faits saillants des couvertures concernées. Mon article aboutit à de nouvelles hypothèses sur les mobiles de Mitnick. Des hypothèses tout aussi plausibles que celles de ces journalistes mais qui s'appuyaient sur une représentation plus juste du *hack* lui-même. J'évacuais enfin entièrement cette idée de facilité dans le geste (cause) *hacker* qui ne convient pas avec le principe même de l'activité.

En conclusion, le *hacking* reste une pratique mystérieuse car l'archéologie du *hack* est impraticable. Bien sûr, les *hacks* peuvent conduire à des manifestations extraordinaires qui peuvent effrayer. Kevin Mitnick paya justement pour avoir effrayé. Mais il y parvint non pas en déchaînant ses pouvoirs extraordinaires mais en profitant d'iconographies fabriquées par une presse déjà prédisposée pour le surnaturel.

Bibliographie

Allbritton, Chris, « *YaHoo!! HaCkEd!!* », Associated Press, 9 décembre 1997.
http://www.infowar.com/hacker/hack_121397a.html-ssi

Arquilla, John, « *The Great Cyberwar of 2002* », Wired News, février 1998.

Associated Press, « *Hackers plead guilty in cyberattacks* », The Augusta Chronicle, 30 juillet 1999.
http://www.augustachronicle.com/stories/073198/tec_124-6681.shtml

Barthes, Roland, « *Mythologies* », Seuil, 1957.

Barthes, Rolland, « *L'empire des signes* », Skira, 1970.

Berghen, Christian Vanden, « *Les mythes* », 2000.
http://www.kyberco.com/Rotasolis/mythes.htm

Bernier, Marc-François, « *Les journalistes sont des acteurs et ne doivent pas l'ignorer* », Compte rendu d'un débat organisé par la section de Québec de la Fédération professionnelle des journalistes du Québec, 10 juin 1997.
http://www2.globetrotter.net/metamedia/acteurs.html

Berinato, Scott, « *Linus on Linux: Inventor Torvalds discusses the OS phenomenon* », ZDNet, 28 janvier 1999.

Berners-Lee, Tim, « *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by its Inventor* », Harper San Francisco, 1999.

Bernz, « *The complete social engineering FAQ* », 2000.
http://netsecurity.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fmorehouse.org%2Fhin%2Fblckcrwl%2Fhack%2Fsoceng.txt

Bougnoux, Daniel, « *La communication par la bande. Introduction aux sciences de l'information et de la communication* », La Découverte, Paris, 1991.

Brain, Marshall, « *How C Programming Works* », Howstuffworks.com, 2000.
http://www.howstuffworks.com/c.htm

Brand, Stewart, « *SPACEWAR : Fanatic Life and Symbolic Death Among the Computer Bums* », Rolling Stone, 1972.
http://www.wheels.org/spacewar/stone/rolling_stone.html

Broch, Henri, « *Au cœur de l'extraordinaire* », Édition L'horizon chimérique, 1992.

Brody, David, « *Mosaic Netscape: One Small Step for the Web…* », Urban Desire, 1994.
http://desires.com/1.1/Features/netscape_2.html

Broersma, Matthew, « *Letsbuyit.com sets debut amid dot-com blues* », ZDNet UK News, 4 juillet 2000.
http://news.zdnet.co.uk/story/0,,t269-s2079940,00.html

Brunker, Mike, « *Mitnick goes free, but must remain totally unplugged* », MSNBC, 21 janvier 2000.
http://www.msnbc.com/news/178825.asp

Bullock, Jim, « *Companies come and go, but your career is forever* », IFBC.ca, mars 1998.
http://www.ifbc.ca/Downloads/bulletin_mar98.html

Burke, Lynn, « *Hot On the Trail of Mafiaboy* », Wired News, 15 février 2000.
http://www.wired.com/news/politics/0,1283,34354,00.html

Busack von, Richard, «*Electronic Hive* », Metroactive, 6 juillet 2000.
http://www.metroactive.com/papers/metro/07.06.00/sunnyvale-0027.html

Cailliau, Robert, « *A Little History of the World Wide Web* », World Wide Web Consortium, 1995.
http://www.w3.org/History.html

Calkins, Keith, G., « *The COMPUTER That Will Not Die: The SDS SIGMA 7* », Andrews University Computing Center, juin 1984.
http://www.andrews.edu/~calkins/profess/SDSigma7.htm

Christensen, John, « *The trials of Kevin Mitnick* », CNN Interactive, 18 mars 1999.
http://www.cnn.com/SPECIALS/1999/mitnick.background

Cilluffo, Frank G., « *The Happy Hacker* », Happyhacker.org, 1999.

Clio, « *Poséidon/Neptune* », 1999.
http://www.chez.com/clio/mytho/poseidon.htm

Cloutier, Jean-Pierre, « *Projet britannique de surveillance du courrier* », Chroniques de Cybérie, 5 décembre 2000.
http://www.cyberie.qc.ca/chronik/20001205.html

Cloutier, Jean-Pierre, « *Plaidoyer de culpabilité* », Chroniques de Cybérie, 23 janvier 2001.
http://www.cyberie.qc.ca/chronik/20010123.html#b

CNN News, « *Master hacker Analyzer held in Israel* », CNN Interactive, 18 mars 1998.
http://www.cnn.com/TECH/computing/9803/18/analyzer/

Coquelle, Barbara, « *Mythologie générale* », 2000.
http://perso.libertysurf.fr/barbara/myth/mythgen.htm

Coupland, Douglas, « *Generation X : tales for an accelerated culture* », St. Martin's Press, 1991.

Cyb's Base, « *So you wanna be a hacker?* », 17 mars 2000.
http://www.accessorl.net/~cyberwar/hacker.html

Darwin, Ian, « *Computing History: Myths and Legends* », Ian Darwin's Web Site, 2000.
http://www.darwinsys.com/history/

Davidson Consulting, Fax Time Line, 2000.
http://www.davidsonconsulting.com/Timeline.htm

Deglise, Fabien, « *Réforme de l'audiovisuel controversée* », Branchez-vous!, 30 juin 2000.
http://www.branchez-vous.com/actu/00-06/04-237502.html

Deutsch, Linda, « *Computer Hacker Fined $4,125* », Associated Press, 2000.
http://www.beachbrowser.com/Archives/News-and-Human-Interest/ August-99/Computer-Hacker-Fined-4125.htm

Dube, Jonathan & Ross, Brian, « *Mafiaboy arrested* », ABC News, 19 avril 2000.

Dubois, Philippe, « *Musée d'Histoire Informatique* », 2000.
http://mo5.com/MHI/index.htm

Dufresne, David, « *Comme la bande à Bonnot* », Libération, 27 août 1999.

Dujay, John, « *Will The Real 'Hackers' Stand Up?* », Channel 4000, 24 février 2000.
http://www.channel4000.com/sh/technology/techviews/dujayonth ewww/stories/dujay-20000223-225532.html

Dvorak, John C., « *Hack Attacks Spreading !* », ZDNet News, 4 octobre 1999.

Eads, Stefani, « *The Hacker Ethic: All Work and All Play?* », Business Week, 7 mars 2001.
http://www.businessweek.com/bwdaily/dnflash/mar2001/nf2 0010 37_989.htm

Eudes, Yves, « *L'odyssée des pirates dans la jungle Internet* », Le Monde diplomatique, juin 1995.
http://www.monde-diplomatique.fr/1995/06/EUDES/1526.html

Fallows, James, « *An Outlaw in Cyberspace* », New York Times, 4 février 1996.
http://mbhs.bergtraum.k12.ny.us/cybereng/nyt/0204fall.htm

FedCIRC Report, « *Computer Security in the news – 1998* », 1999.

Fillaire, B. « *Les sectes* », Flammarion (collection Dominos), 1996.

Fine, Doug, « *Why is Kevin Lee Poulsen Really in Jail?* », Well, 1995.
http://www.well.com/user/fine/journalism/jail.html

Fonseca, Brian, « *Kevin Mitnick: The hacker extraordinaire speaks out on security in today's Internet age* », InfoWorld, 1er décembre 2000.

Fontaine, Didier, « *Encyclopaedia Gentium Boni* », 2001.
Adresse électronique : http://www.ifrance.com/EGB/

Ford, Nelson, « *The History of Shareware & PsL* », Public Software Library, 2000.
http://www.pslweb.com/history.htm

Freiberger, Paul et Swaine, Michael, « Fire in the Valley. The Making of the Personal Computer: Second Edition », McGraw-Hill, janvier 2000.
http://www.fsbassociates.com/mcgrawhill/fireinthevalley.htm

Fuhs, Howard, « *Telecommunication Security* », Fuhs Security Consultants, 1994.
http://www.fuhs.de/fachartikel/Telecommunication_Security.htm

Garfinkel, Simson L., « *Is Stallman Stalled ?* », Wired Magazine, mars-avril 1993.
http://www.wired.com/wired/archive//1.01/stallman.html?person=richard_stallman&topic_set=wiredpeople

Garfinkel, Simson L., « *Unofficial Markoff, Mitnick, Shimomura FAQ* », 1996.
http://simson.net/clips/96.IU.MitnickMarkoff.html

Gauthier, Benoît, « *La structure de la preuve* », Recherche sociale, Presses de l'Université du Québec, 1997.

Gelernter, David, « *Cyberwar's Literacy Fallout Rivals Cyberwar* », New York Times, 27 février 1996.
http://mbhs.bergtraum.k12.ny.us/cybereng/nyt/hacker-b.htm

Glasner, Joanna, « *Mitnick Movie Spurs suit* », Wired News, 30 mars 2000.
http://www.wired.com/news/business/0,1367,35327,00.html

Glave, James, « *Israeli PM: Analyzer Damn Good* », Wired News, 19 mars 1998.
http://www.wired.com/news/politics/0,1283,11055,00.html

Goodell, Jeff, « *The Cyberthief and the Samurai* », Dell, 1996.

Goodell, Jeff, « *Wooing the Geeks* », Rolling Stone, 15 octobre 1998.

Goodell, Jeff, « *The Rise and Fall of a Silicon Valley Family* », Barnes & Noble, Random House, 2000.

Goodell, Jeff, « *A Conversation with Jerry Yang* », Rolling Stone, 30 mars 2000.

Goodell, Jeff, « *Who Needs Privacy* », Rolling Stone, 30 mars 2000.

Goodell, Jeff, « *Inside the World of Paul Allen* », Rolling Stone, 22 juin 2000.

Graetz, J.M., « *The origin of Spacewar* », Creative Computing magazine, 1981.
http://www.enteract.com/~enf/lore/spacewar/spacewar.html

Grant, David, « *A new improved script-kiddy* », GeekNews, 13 juin 1999.
http://geeknews.efront.com/articles/DavidGrant/061399.shtml

Grimwood, Jon Courtenay, « *An interview with William Gibson* », Infinity Plus, 17 janvier 1998.
http://www.users.zetnet.co.uk/iplus/nonfiction/intwg.htm

Grolleau, Frédéric, « *Dantec, le Bloy techno pop* », Paru, 29 mai 2000.
http://www.paru.com/redac/critiqueLitterature/axxxx563.htm

Guide de déontologie de la Fédération professionnelle des journalistes du Québec, 2002.
http://www.fpjq.org/cgi-bin/corps.cfm?section=5&soussection=8

Gulker, Chris, « *The Cyberthief and the Samurai Review* »,Gulker.com, 15 janvier 1998.

Gulker, Chris, « *The Kevin Mtinick/Tsutomu Shimomura affaire* », Gulker.com, 17 septembre 2001.
http://www.gulker.com/ra/hack

Halazy, Caroline, « *Les liens intimes entre pirates et sexe* », Le Monde, 3 janvier 2002.

Heitz, Bernard, « *Icônes rares* », Télérama, 23 juin 1993.
http://www.mallat.com/articles/icones%20rares.htm

Hesseldahl, Arik, « *After the Hack* », Columbia Journalism Review, janvier/février 1999.
http://www.cjr.org/year/99/1/hack.asp

Himanen, Pekka, « *L'éthique Hacker* », Exils, 2001.
http://www.exils.fr/hacker/

Hunter, Christopher D., « *The Uses and Gratifications of Project Agora* », Annenberg School for Communication, University of Pennsylvania, 21 avril 1997.
http://www.asc.upenn.edu/usr/chunter/agora_uses/index.html

Hurley, Ed, « *Hackito, Ergo Sum* », 2001.
http://www.sls.lcs.mit.edu/~hurley/prog.html

Hurwicz, Mike, « *Virtual private networks offer some serious savings -- if you know the secret.* », TechWeb, juillet 1997.
http://telehealth.net/subscribe/newslettr_8.html

Internet Software Consortium, Internet Survey Number of Internet Hosts, 2000.
http://www.isc.org/ds/host-count-history.html

Jodelet, D. « *Les représentations sociales, sociologie d'aujourd'hui* », PUF, 1989.

Johnson, Keith, « *Hackers caught in security honeypot* », ZDNet News, 19 décembre 2000.

Jud, Emmanuel, « *Spamming et mailbombing : tiens, c'est bizarre, on dirait que ma boîte-aux-lettres électronique a explosé...* », Secuser News, mars 2000.

Jupiter Media Metrix, 2002.
http://ca.mediametrix.com/xp/ca/press/releases/pr_020400.xml

Kantrowitz, Mark, « *Milestones in the Development of Artificial Intelligence* », 2000.
http://128.174.194.59/cybercinema/aihistory.htm

Kehoe, Brendan P., « *Zen and the Art of the Internet* », A Beginner's Guide to the Internet, janvier 1992.

Kennedy, Dana, « *A Bug in the System* », Entertainment Weekly, 2 février 1996.
http://www.dearsally.org/alias/articles/020296_mitnick_ew.html

Key, Virginia, «*What is Solar Sunrise?* », SANS Institute Resources, 2000.
http://www.sans.org/newlook/resources/IDFAQ/solar_sunrise.htm

Kreider, Aaron, « *Ambiguous Definitions of Hacker: Conflicting discourses and their impact upon the possibilities of resistance* », Sociology of culture, Term Paper, University of Notre Dame, 2 janvier 1999.
http://www.nd.edu/~akreider/essays/hackers.htm

Kurtz, Howard, « *Computer Thief Scoop Nets Book Deal* », Washington Post, 1995.
http://www.takedown.com/coverage/book-deal.html

Latrive, Florent, « *Analyzer, pirate et technohéros des ados* », Libération, 30 avril 1998.
http://www.liberation.fr/multi/pirates/art983004.html

Latrive, Florent, « *Piratage sur le site du FN* », Libération, 5 mars 1999.

Launet, Edouard, « *Cyberguérilla sino-américaine* », Libération, 2 mai 2001.

Launet, Edouard, « *Un mouvement potentiellement puissant* », Libération, 13 août 2001.

Latrive, Florent, « *La drôle de guerre électronique* », Libération, 11 mai 2001.

Leibowitz, Brian, « *The Institute for Hacks, Tomfoolery & Pranks* », MIT Press, 1990.
http://hacks.mit.edu/Hacks/books/ihtfp_leibowitz/

Le Monde, « *Ehud Tannenbaum, pirate et héros* », Le Monde, 24 mai 1999.

Lemos, Robert, « *Script kiddies: The Net's cybergangs* », ZDNet News, 12 juillet 2000.

Lemos, Robert, « *Mitnick teaches social engineering* », ZDNet News, 17 juillet 2000.
http://news.zdnet.co.uk/story/0,,s2080227,00.html

Lemos, Robert, « *Security sites hit by graffiti gang* », ZDNet News, 23 juillet 2001.
http://techupdate.zdnet.com/techupdate/stories/main/0,14179,5092645,00.html

Levy, Steven, « *Heroes of the Computer Revolution* », Dell, New York, 1985.
http://ibiblio.org/pub/docs/books/gutenberg/etext96/hckrs10.txt

Littman, Jonathan, « *Once Upon A Time In ComputerLand* », Simon & Schuster, 1990.

Littman, Jonathan, « *The Last Hacker* », Los Angeles Times, 26 septembre, 1993.
http://www.phrack.com/show.php?p=44&a=27

Littman, Jonathan, « *It takes a hacker to catch a hacker* », Mercury News, 8 décembre 1994.

Littman, Jonathan, « *Forward Spin: The secret to success* », PC Week, 27 janvier 1995.

Littman, Jonathan, « *The Fugitive Game: Online With Kevin Mitnick* », Little Brown & Company, 1996.

Littman, Jonathan, « *The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulsen* », Little Brown & Company, 1997.

Littman, Jonathan, « *Hacked, cracked and phreaked* », PC Week, 27 janvier 1997.

Littman, Jonathan, « *New twist: Feds recant on Mitnick's fugitive status* », ZDNet News, 19 juin 1997.
http://www5.zdnet.com/zdnn/content/zdnn/0619/zdnn0015.html

Littman, Jonathan, « *Gone Corporate* », Red Herring, 1 août 2001.
http://www.redherring.com/mag/issue100/270019827.html

Littman, Jonathan, « *Digital wiretapping in the future* », CNET.Com, 20 novembre 1997.

Lohr, Steve, « *Once rejected as science fiction, the threat of sabotage looms in an age of increasing computer dependency* », New York Times, 29 octobre 1996.
http://www.newslibrary.com/nlsearch.asp

Markoff, John & Hafner, Katie, « *Cyberpunk : Outlaws and Hackers on the Computer Frontier* », Simon & Schuster, 1991.

Markoff, John, « *Cyberspace's Most Wanted: Hacker Eludes F.B.I. Pursuit* », New York Times, 4 juillet 1994.
http://www.takedown.com/coverage/most-wanted.html

Markoff, John, « *How a Computer Sleuth Traced a Digital Trail* », New York Times, 15 février 1995.
http://www.takedown.com/coverage/digital-trail.html

Markoff, John, « *Hacker and Grifter Duel on the Net* », New York Times, 19 février 1995.
http://home.indy.net/~sabronet/news/kmit6.html

Markoff, John, & Shimomura, Tsutomu, « *Takedown* », Hyperion, 1996.

Markoff, John, « *U.S. Drafting Plan for Computer Monitoring System* », New York Times, 28 juillet 1999.

Martel, Gaétan, « *De vous à moi...* », Québec Micro, 15 juillet 1996.

Martin, Brian, « *Is it worth it? : Dispelling the myths of law enforcement and hacking* », Hacker News Network, 1999.
http://www.hackernews.com/bufferoverflow/99/worthit.html

Martin, Brian, « *Carolyn Meinel Hall of Shame* », Attrition.org, 2000.
http://www.attrition.org/shame/index2.html

Massey, David, « *Phone Phreaking : The Telecommunications Underground* », 2000.
http://www.navyrelics.com/tribute/phonephreaking.html

Mauriac, Laurent, « *Un exercice de logique et de patience* », Libération, 10 février 2000.
http://www.liberation.fr/multi/pirates/20000210jeug.html

McCandless, David, « *Warez Wars* », Wired News, avril 1997.

McKay, Niall, « *The Golden Age of Hacktivism* », Wired News, 22 septembre 1998.
http://www.wired.com/news/politics/0,1283,15129,00.html

Meeks, Brock N., « *The mixture of hacker and activist is a myth* », ZDNet News, 3 mai 2001.
http://www.zdnet.com/zdnn/stories/comment/0,5859,2714981,00. html

Mellos, Koula, « *Une science objective ?* », Recherche sociale, Presses de l'Université du Québec, 1997.

Mirik, John, « *Bill Gates: Before Microsoft* », 29 septembre 1996.
http://ei.cs.vt.edu/~history/Gates.Mirick.html

Mitnick, Kevin, « *They call me a criminal* », The guardian, 22 février 2000.

Muller, Joann, « *Compaq will buy Digital in a record $9.6b deal* », Boston Globe, 27 janvier 1998.
http://www.boston.com/globe/business/packages/compaq_dec/

Myles, Brian, « *Piratage informatique : Mafiaboy plaide coupable* », Le Devoir, 19 janvier 2001.

Nagaraj, Sudha, « *Dangerous Liaison* », Computers Today, 16 avril 1999.
http://www.india-today.com/ctoday/16041999/pcuser.html

Neumann, Peter G., « *Better DES challenge solved by John Gilmore and Deep Crack* », Risk Digest, 17 juillet 1998.
http://catless.ncl.ac.uk/Risks/19.87.html

O'Brien, Miles, « *Books present two sides of super-hacker Mitnick* », CNN Interactive, 7 février 1996.
http://www.cnn.com/TECH/9602/hacker

Peek, Richard, « *In Mitnick's Defense, Annotation on The Fugitive Game* », Ethercat, 1997.

Peirce, Charles S., « *Écrits sur le signe* », Paris, Seuil, 1978.

Peirce, Charles S., « *Textes anticartésiens* », Aubier Montaigne, 1984.

Penenberg, Adam L., « *Vigilante hacker* », Forbes, 17 avril 1998.
http://www.forbes.com/1998/04/17/feat.html

Penenberg, Adam L., « *We were long gone when he pulled the plug* », Forbes Global, 16 novembre 1998.

Penenberg, Adam L., « *Hackers for Girlies interview* », Infowar.com, 15 décembre 1998.
http://www.infowar.com/hacker/hack_121598c_j.shtml

Penenberg, Adam, « *Mitnick Speaks!* », Forbes, 4 mai 1999.
http://www.forbes.com/1999/04/05/feat.html

Peter, H., « *A Quarter Century of UNIX* », Addison-Wesley, 1994.
http://virtual.park.uga.edu/hc/unixhistory.html

Platt, Charles, « *The Mad-Scientist Myth Figure* », Computer Underground Digest, vol. 7, 10 décembre 1995.

Poulsen, Kevin, « *Mitnick: I was never a malicious person* », ZDNet News, 30 juillet 1999.
http://zdnet.com.com/2100-11-501183.html?legacy=zdnn

Poulsen, Kevin, « *eBay pulls Kevin Mitnick trinkets* », The Register, 22 novembre 2000.
http://www.theregister.co.uk/content/1/14908.html

Raykow, David, « *Debunking the hacker threat myth* », ZDNet News, 13 août 1999.

Raymond, Eric S., « *A Brief Hostory of Hac*kerdome », Tuxedo.com, 5 mai 2000.
http://www.tuxedo.org/~esr/writings/hacker-history/hacker-history.html

Raymond, Eric S., « *Comment devenir un hacker* », 11 septembre 2000.
http://www.tuxedo.org/%7Eesr/faqs/hacker-howto.html

Raymond, Eric, « *The New Hacker's Dictionary* », MIT Press, 29 juin 2001.
http://www.tuxedo.org/~esr/jargon/jargon.html

Reboul, « *Egalité et différence: la place des femmes dans la cité* », Le Rasoir Philosophique, 18 octobre 1999.
http://sylvainreboul.free.fr/ega.htm

Reuters, « *China Sentences Hackers To Death For Bank Theft* », InfoWar.com, 29 décembre 1998.
http://www.infowar.com/hacker/hack_122998b_j.shtml

Rheingold, Howard. « *Tools for Thought* », MIT Press 2000.
http://www.rheingold.com/texts/tft/8.html

Richard, Emmanuelle, « *Ces pirates qui montent des bateaux* », Libération, 28 mai 1999.
http://www.liberation.fr/multi/pirates/art990528.html

Richard, Emmanuelle, « *Kevin Mitnick, Pirate de légende* », Libération, 20 juillet 1999.

Ritchie, Dennis, « *The development of the C language* », Lucent Technologies, 1996.
http://cm.bell-labs.com/cm/cs/who/dmr/chist.html

Rosenberg, Scott, « *The Net Still Has Too Many Holes, Experts Warn* », Digital Culture, 5 juillet 1995.
http://www.wordyard.com/dmz/digicult/netsecurity-7-5-95.html

Rosenberg, Scott, « *Mitnick's Malice, Shimomura's Chivalry* », Salon.com, 30 décembre 1995.
http://www.salon.com/30dec1995/features/mitnick1.html

Rosenberg, Scott, « *21st: Kiddie porn: Drudge falls for Yahoo hackers' nonsense* », Salon.com, 11 décembre 1997.

Rossi, Serge, « *Histoire de l'informatique* », 2000.
http://histoire.info.online.fr/pdp1.html

Sabatier, Patrick, « *Washington se prépare à la guerre de la Toile* », Libération, 11 février 2000.
http://www.liberation.fr/multi/pirates/20000211ven.html

Sanderson, William Thomas, « *MITS/Pertec Altair 8800/680b/MITS 300/Attache and the stories of those who build and use them* », 1998.
http://exo.com/~wts/wts10005.HTM

Sédallian, Valérie, « *Commentaire de l'affaire Yahoo!* », Juriscom.net, Lionel Thoumyre, 20 novembre 2000.
http://www.juriscom.net/chr/2/fr20010112.htm

Shuman, Ellis, « *Analyzer - Israeli Hero or International Criminal?* », About.com, Israeli Culture, 20 mars 1998.
http://israeliculture.about.com

Silberman, Steve, « *Kid-Porn Vigilante Hacked Media* », Wired News, 8 février 1999.
http://www.wired.com/news/culture/0,1284,17775,00.html

Silverstein, William, « *A Guide to the Real Programmer!* », Sorehands.com, 2001.
http://www.sorehands.com/humor/real8.htm

Simoneau, Sylvain, « *Carnivore, l'outil espion du FBI, révolte les Américains* », ZDNet France, 18 juillet 2000.
http://www.zdnet.fr/actu/soci/a0015138.html

Slatalla, Michelle, « *Hackers' Hall of Fame* », TLC Life Unscripted, 2001.
http://tlc.discovery.com/convergence/hackers/bio/bio.html

Soldevila, Carlos, « *Cyberterrorisme - La guerre du futur* », Voir, août 1998.

Srivastava, Manish, « *Steven Wozniak* », 29 septembre 1996.
http://ei.cs.vt.edu/~history/WOZNIAK.HTM

Stone, Keith, *« Kevin Mitnick : Dangerous Cyberfelon or Minor Hacker* », Los Angeles Daily News, 18 janvier 1996.
http://technoculture.mira.net.au/hypermail/0069.html

Supnik, Bob, « *The Computer History Simulation Project* », 8 septembre 2000.
http://simh.trailing-edge.com/

Tal, Shlomi, « *For The Masses* », Osopinion.com, 2000.
http://www.osopinion.com/Opinions/ShlomiTal/ShlomiTal12.html

Tasca, Catherine, « *Discours de Catherine Tasca devant le congrès de la presse à Lille* », Ministère de la Culture et des Communications, France, 24 novembre 2000.
http://www.culture.fr/culture/actualites/conferen/lille-presse-tasca .htm

Thomas, Jim, « *The Virus Creation Labs* » , Computer underground Digest, 5 mars 1997.

Thorel, Jérôme, « *Defcon : derrière le paisible consultant, un ex-pirate* », ZDNet France, 2 août 2000.
http://news.zdnet.fr/story/0,,s2060963,00.html

Treble, Bandoppler, « *Stories of a genuine skate poser* », Treble & Spaghetti Publication, novembre 1999.
http://www.bandoppler.com/ef11.html

Tremblay, Jean-Marc, « *Terroristes ou Robin des Bois?* », Infini.com, 4 avril 2000.

Tuomola, Olli, « *Hackers : the plague of the net ?* », 2000.
http://begfor.tripod.com/hackers.htm

Vautravers, Constant, « *Une éthique du reportage* », L'expression lycéenne, Hachette, 1991.
http://www.presse.ac-versailles.fr/Textes/Vautra91.htm

Vulser, Nicole, « *Le groupe Ouest-France confirme son virage vers la presse gratuite* », Le Monde, 13 février 2002.
http://www.lemonde.fr/article/0,5987,3236--262599-,00.html

Walleij, Linus, « *Copyright Does Not Exist* », 1994.
http://home.c2i.net/nirgendwo/cdne/mainindex.htm

Welch, Matt, « *Se7en deadly sins* », Online Journalism Review, 1999.
http://ojr.usc.edu/content/story.cfm?request=153

Wellen, Alex & Poulsen, Kevin, «*Judge to Mitnick: No PC, pal* », ZDNet News, 31 mars 1998.
http://www.zdnet.com/zdnn/content/zdtv/0330/302173.html

Weyhrich, Steven, « *Apple II History* », 1995.
http://www.hypermall.com/History/

Wheeler, Andrew, « *Letter From America : An Interview with Richard Starkings* », Ninthart, 18 juin 2001.
http://www.ninthart.com/display.php?article=42

Williams, Jim, « *Free Kevin* », About.com, 14 septembre 1998.

Williams, Mary Elizabeth, « *Hack and Ye Shall Learn* », Wired Magazine, numéro 14.2, 1997.
http://www.spaziopiu.it/elettrici/gtmhh/cpmeinel.html

Winkless, Nelson, « *Tymshare & SDS* », groupe de discussion, modérateur : David S. Bennahum, 11 juin 1996.
http://www.memex.org/cm-archive2.html

Zuckerman, M.J., « *The latest version of Kevin Mitnick* », USA Today, 20 novembre 2000.
http://www.usatoday.com/life/cyber/tech/cti824.htm

Annexe 1

Liste des principales parades qui ont prévalu sur le net entre 1995 et 2002

Patches : Les logiciels mal rodés (i.e. une période de lancement bêta trop courte) sont souvent atteints de tares que les *hackers* sont naturellement les premiers à découvrir. En ligne, ça se traduit par des failles de sécurité. Aussitôt informé, l'éditeur développe un *patche*, un morceau de programme à coller, qu'il distribue en catastrophes à ses clients. Malheureusement, ceux-ci sont parfois mal installés, surtout quand ces clients sont des administrateurs-réseaux peu compétents, habitués d'installer du software clef en main.

Procédé *hacker* typique pour déjouer cette parade : Code source d'un logiciel cassé par ingénierie inversée (*reversed engineering*) et découverte de nouvelles failles dans le logiciel original. En 1999, *Microsoft* fut accusé par le géant *America Online* (AOL) d'avoir copié son système de messagerie instantanée en procédant ainsi.

Coupe-feu ou **pare-feu** (*Firewall*) : Logiciel qui filtre les paquets de données en transit. Il contrôle aussi les services *proxy*. Un coupe-feu est théoriquement impossible à déjouer.

Procédé *hacker* typique pour déjouer cette parade : Des *crackers* interceptent des paquets de données sortants, lesquels sont subtilement modifiés et substitués à d'autres entrants. Des leurres sont ensuite envoyés pour déjouer la vigilance du coupe-feu tandis que les paquets modifiés traversent la passerelle en catimini.

Mot de passe dynamique : C'est la nouvelle mode. Le client possède une liste de mots de passe statiques et un puissant algorithme les convertit à chaque nouvelle connexion. Même interceptés, ces mots de passe sont inutilisables pour l'intrus.

Procédé *hacker* typique pour déjouer cette parade : Le *cracker* abandonne quelques

paquets renifleurs (*packet sniffers*) dans le no man's land devant le coupe-feu pour intercepter des données non encryptées. Ces paquets restent en état de veille et après une longue période de temps peuvent capturer mots de passe, noms d'usagers, numéros de carte de crédit ou encore des informations formulaires utiles dans les cas de *social engineering*.

Surveillance réseau : Des logiciels enregistrent la circulation bidirectionnelle et génère des rapports (*logs*) en direct de l'activité globale. Ils ralentissent considérablement la vitesse de traitement mais les hébergeurs ne peuvent s'en passer. Par exemple, si le contenu d'une page web est altéré/changé, l'heure et la date ainsi que l'adresse *IP* (position) de l'usagé sont notées dans le rapport.

Procédé *hacker* typique pour déjouer cette parade : Aucun cas connu à ce jour.

Protection contre le refus de service (*Distributed Denial of Service*, ou DoS) : Protège les routeurs contre l'engorgement de données (flood, mailbombing, etc.) et détecte les programmes heuristiques qui tentent une intrusion dans le serveur. Il peut aussi servir à identifier les logiciels de *cracker* connus à ce jour (*Tribe FloodNet TFN* et *TFN 2K*, *Trinoo* et *Stachelddraht*).

Procédé *hacker* typique pour déjouer cette parade : Un ver logique en apparence inoffensif est lancé en direction du serveur. Il arrive à l'éclosion une fois rendu sur le disque dur de la machine infectée. En 1988 un étudiant de *Cornell University* (Robert Morris) parvint ainsi à faire tomber l'ensemble du net nord-américain, causant un hécatombe sans précédent.

Tunnels IP de CenterTrack : Analyse chaque requête et par un intelligent système d'authentifications croisées, positionne les adresses *IP* et leur trajectoire dans le monde. A la moindre erreur, le *cracker* est repéré (la plupart du temps des *scripts kiddies*.

Procédé *hacker* typique pour déjouer cette parade : Faire des bons successifs entre différents hôtes avant de fondre sur la cible. Quand le système essaie de repérer l'intrus, il

ne retrace que le dernier bond. Pour remonter au suivant, l'enquêteur doit communiquer dans l'ordre avec chacun de ces hôtes, travail fastidieux d'autant plus que selon la juridiction nationale, certains hôtes ne sont pas tenus de collaborer. En 1994, *Datastream Cowboy* faillit s'en sortir ainsi après avoir dérobé des rapports sur la Guerre du Golfe (laboratoire ROME à New York au coeur du dispositif de défense de l'OTAN). Mais cette technique est risquée et le génie de la chose réside dans la capacité à redéfinir aléatoirement les trajectoires pour chaque paquet de données.

Encryption : Encrypter et coder l'information pour la rendre incompréhensible. Les méthodes sont nombreuses : DES (*Data Encryption Standard*, une clé à 56 bit), RSA (de l'éditeur *Rivest-Shamir-Adelman*), PGP (*Pretty Good Privacy*), irréversibilité (du type clé Salt d'Unix), algorithme de chiffrement en continu (type Rivest Cypher de *RSA Data Security*), protocole SET (*Secure Electronic Transactions*, utilisé par *American Express*, *IBM*, *Mastercard*, *Netscape*, *SAIC*, *Terisa Systems*, *Verisign* ou *Visa*). Sur les serveurs, les pages dynamiques (ASP, PHP, etc.) sont pilotées par des bases de données encryptées. Des dispositifs de sécurités tels que *SecurePage* (*Creative Digital Technology*) automatisent la gestion des pages. Durant le changement, chacune d'elle est comparée à un *master* qui contient le site original en entier, celui-ci étant supposé inviolable. Le *master* refuse systématiquement tout changement qui ne correspond pas avec son propre jeu d'instructions.

Procédé *hacker* typique pour déjouer cette parade : Le cassage d'une clef d'encryption supérieure ou égale à 56 bits est mathématiquement impossible. En 1997 pourtant, des *hackers* purs de *l'Electronic Frontier Foundation* (EFF) à San Francisco ont réussi à décoder un message protégé par la norme DES. Chose incroyable puisqu'il aurait fallu des années à tous les ordinateurs interconnectés de la planète pour vérifier l'ensemble des combinaisons possibles. L'EFF y parvint en 56 heures avec une vieille carcasse Sun contenant 1000 puces affectueusement surnommée *Deep Crack*. Un *hack* de génie.

Sécurité humaine : Les hébergeurs adoptent des politiques vis-à-vis de la sécurité. Chaque employé doit respecter une procédure lorsqu'il manipule de l'information. Chez *Videotron*.ca, avant de divulguer une information au téléphone, le service à la clientèle

exige le nom de jeune fille de la mère du client.

Procédé *hacker* typique pour déjouer cette parade : L'homme est le maillon le plus faible d'un système informatisé. Avant d'élaborer des techniques d'intrusions plus tordues les unes que les autres, le *cracker* exploite les faiblesses du genre humain. L'utilisation du téléphone pour tromper des gens est un classique. Par exemple, un *cracker* appelle un technicien et se fait passer pour un supérieur. D'une voix autoritaire, il lui ordonne de lui révéler certaines informations confidentielles voire d'exécuter des manœuvres. Il s'agit là de *social engineering*, un bluff qui se joue entre êtres humaine et contre lequel aucun système de sécurité ne peut quoi que ce soit.

Mais le *social engineering* n'est pas du *hacking*. Cette tactique est à la disposition de n'importe quel bluffeur habile. C'est d'ailleurs en envoyant un courriel sec à des administrateurs-réseaux intimidés que les *Hacking for Girlies* obtinrent les mots de passe nécessaires au piratage du *New York Times* en 1999.