Ali EL AZZOUZI

La Cybercriminalité au Maroc

Préface du Président de l'Association Internationale de Lutte Contre la Cybercriminalité Mohamed CHAWKI

Dépôt légal : 2010 MO 1585
ISBN : 978-9954-9072-0-7

A mon fils Ismail

Remerciements

Ce livre n'aura pas été possible sans le soutien de plusieurs personnes. Mes pensées vont notamment à :

- Jean-Guy RENS, auteur du livre « L'empire invisible » et président de l'association canadienne des technologies avancées qui m'a fait part de ses précieux conseils tout au long de la rédaction de ce livre.
- Mohamed CHAWKI, auteur du livre « Combattre la cybercriminalité » et président de l'association internationale de lutte contre la cybercriminalité qui a accepté de rédiger la préface de ce livre.
- Nabil OUCHN, co-fondateur de Netpeas et expert en sécurité qui a apporté sa contribution et son témoignage sur l'univers de *l'Underground* marocain.
- Tous les consultants sécurité de la société DATAPROTECT, notamment Hamza HAROUCHI et Othmane CHAFCHAOUNI qui m'ont soutenu tout au long de ce travail.
- Tous mes anciens collègues de BT NET2S avec qui j'ai partagé des moments forts pendant plus de trois ans. Je pense notamment à mon équipe sécurité. Rabii AMZERIN, Younes BOURRAS, Younes ZAKIDDINE et Mohamed Amine LEMFADLI.

Je vous remercie tous !

Table des matières

Table des illustrations

Préface

La cybercriminalité fait partie des conduites les plus odieuses que l'on ait pu imaginer. Hélas, l'apparition de nouvelles technologies comme celle de l'internet a permis l'amplification de ce phénomène insupportable, au point que cette infraction est devenue l'une des sources majeures de profits pour les organisations criminelles. Au Maroc des nouvelles lois ont été promulguées, et des nouvelles organisations ont été créées pour combattre les cyberdélits. Dès lors, l'utilité d'un ouvrage sur les nouveaux développements de cette forme de criminalité au Maroc ne saurait être contestée.

C'est à cette tâche que M. El Azzouzi s'est attelé. Compte tenu de toutes ses qualités, celui-ci était particulièrement bien placé pour réaliser ce travail. En effet, d'une part M. El Azzouzi a mené plusieurs missions d'audit et de recherche dans le domaine de la cybersécurité. D'autre part, après un parcours qui l'a ramené à gérer des projets d'envergure en sécurité au Canada et au Maroc, il dispose aujourd'hui d'un retour d'expérience riche et varié dans le domaine de la sécurité de l'information.

De façon très structurée, l'auteur étudie en plusieurs parties le phénomène de la cybercriminalité au Maroc. Ainsi, il a notamment envisagé d'élucider les multiples visages de la cybercriminalité tout en prenant soin de décortiquer l'écosystème qui gravite autour de ce phénomène et ce sans négliger les aspects juridiques et législatifs.

Compte tenu de la qualité du contenu apporté par l'auteur, on ne peut que recommander très fort la lecture de ce livre écrit par un expert international qui a consacré plusieurs années à l'étude du phénomène de la cybercriminalité.

Mohamed CHAWKI
Conseiller d'Etat adjoint
Président de l'AILCC, France

Introduction

L'internet a transformé le monde en un village planétaire. Il améliore la productivité des entreprises, révolutionne les méthodes de travail et rend possible l'émergence de nouveaux modèles d'affaires permettant de communiquer, négocier, échanger et de commercialiser en temps réel. En ce sens, son apport est capital pour nos sociétés. Il est devenu au fil des temps si indispensable que peu d'organisations et de particuliers peuvent s'en passer aujourd'hui. Or cette révolution a également rendu possibles de nouvelles formes de criminalité liées au cyberespace. En effet, l'internet n'a pas été développé, dès le départ, de manière sécurisée. Ses multiples composants matériels, logiciels et protocolaires étaient et demeurent empreints de nombreuses failles de sécurité qui peuvent avoir en cas d'exploitation des conséquences bien réelles. Ce qui a favorisé l'émergence des comportements déviants dans le cyberespace. La cybercriminalité est ainsi née.

L'anonymat que procure le cyberespace, la vulgarisation des techniques d'attaques, l'adoption à grande échelle du web 2.0 ont accéléré la croissance des actes cybercriminels ces dernières années. En 2009, la cybercriminalité a généré plusieurs milliards de dollars selon une récente étude de Symantec. Pas étonnant de voir de plus en plus d'adeptes s'y intéresser. L'attractivité du phénomène est telle que des milliers d'internautes, en quête d'argent facile, n'hésitent pas à franchir le pas. En effet, en cette période de marasme économique, l'argent honnête est plus difficile à gagner. De plus en plus d'individus sont attirés par le monde de la fraude pour arrondir leurs fins du mois. Ainsi, le « cybercriminel de dimanche » fait son apparition dans l'écosystème qui gravite autour de la cybercriminalité.

Finie donc l'époque où les actes de déviance dans le cyberespace ne sont que les œuvres des acteurs en quête de reconnaissance sociale. Aujourd'hui, la cybercriminalité est une activité qu'on pratique d'abord pour l'appât du gain. Pour attirer l'attention de son auteur, une opération cybercriminelle doit générer de l'argent. Ceci a permis une reconfiguration de l'écosystème lié à la cybercriminalité. En effet, si avant l'essentiel des actes de déviance était

perpétré par des individus experts en sécurité certes, mais désorganisés et souvent introvertis, aujourd'hui l'économie souterraine de la cybercriminalité obéit à des règles de rationalité économique exigeant un travail en équipe, une organisation efficace et une spécialisation à outrance. En outre, il n'est pas nécessaire d'être un surdoué en informatique pour se lancer dans la cybercriminalité. De nombreux forums proposent des packages complets permettant même à un profane de perpétrer des actes cybercriminels. Il n'est pas rare de constater par exemple qu'une attaque virale a été conçue par une équipe composée par plusieurs programmeurs qui ne se sont probablement jamais vu réellement et exploitée par d'autres individus ayant récupérés le programme malveillant en contre partie d'un service ou de l'argent. Certains groupes, pour faire valoir leurs produits, vont jusqu'à proposer un engagement de résultat et un service après vente 24h/24h et 7j/7j.

Avec cette menace grandissante qui devient plus visible pour les masses, les forces de l'ordre dans le monde entier redoublent d'efforts pour combattre la cybercriminalité. Bien que la coordination internationale soit entravée par une approche globale inexistante, les structures de partage des informations et des ressources s'améliorent et un certain nombre d'arrestations et de procès ont eu lieu en 2009.

Au Maroc, la cybercriminalité, qui était jusqu'à une date récente un phénomène marginal, attire de plus en plus l'attention des pouvoirs publics. De nouvelles lois ont été promulguées, de nouvelles organisations ont été créées et un programme ambitieux de confiance numérique proposé dans le cadre de la stratégie « Maroc Numeric 2013 » a été lancé. Ainsi, la culture de sécurité, bien qu'elle n'est que dans un état embryonnaire, commence à s'installer non seulement dans les institutions publiques et privés mais aussi dans l'esprit de tout un chacun.

Chapitre 1 : Démystification de la cybercriminalité

« Dans les révolutions, il y a deux sortes de gens :
ceux qui les font et ceux qui en profitent »
Napoléon Bonaparte

Août 2005 : les serveurs de Microsoft, CNN, ABC, du New York Times et de plus d'une centaine d'entreprises américaines sont attaqués par le virus Zotob, provoquant des dégâts évalués à plusieurs dizaines de millions de dollars. Une enquête rondement menée au niveau international aboutit quelques semaines plus tard à l'arrestation de Farid Essebar, alias Diab10, un jeune cyberpirate marocain qui agissait depuis un cybercafé. Les journaux parlent de « cyber-diable » et de « génie informatique ». Cette image de l'adolescent cherchant désespérément à exploiter une vulnérabilité d'un serveur lointain ne doit pas nous induire en erreur.

Les cyberpirates qui font la une sont des amateurs qui se font prendre plus ou moins rapidement. C'est d'ailleurs pour cela que leurs noms se retrouvent sur la place publique. Le véritable danger vient plutôt de nouveaux groupes très structurés qui sont à l'origine d'une véritable industrie de la cybercriminalité. Celle-ci s'impose désormais comme un métier à part. Elle dispose, certes de ses propres spécificités. Cependant, à l'instar de l'activité économique conventionnelle, elle obéit de plus en plus aux logiques économiques de la croissance, de la rentabilité financière, de la gestion des risques, de l'organisation et de la division du travail.

1. La cybercriminalité : concepts et enjeux

1.1 La cybercriminalité : Un nouveau concept

Il n'existe pas de définition universelle pour le terme cybercriminalité. Celui-ci est utilisé généralement pour décrire l'activité criminelle dans laquelle le système ou le réseau informatique est une partie essentielle du crime. Il est également employé pour décrire des activités criminelles traditionnelles dans lesquelles les ordinateurs ou les réseaux sont utilisés pour réaliser une activité illicite. Dans le premier cas, les technologies sont la cible de l'attaque. Dans le second, elles en sont le vecteur.

1.2 La cybercriminalité : Une activité en pleine croissance

Grâce notamment à la diffusion sur le Web de nouveaux services et outils s'adressant à une population mondiale de plus en plus disposée à les adopter, la croissance des actes cybercriminels s'est particulièrement accélérée ces trois dernières années. Cette tendance s'amplifie rapidement depuis la vogue du Web 2.0, notamment les réseaux sociaux qui ont atteint un niveau de popularité élevé parmi les sites Web. Ils sont devenus des vecteurs privilégiés de propagation de programmes malveillants et de courrier indésirable. L'efficacité d'une telle diffusion est d'environ 10%. Ce qui est bien supérieure à l'efficacité des méthodes classiques de diffusion des programmes malveillants par courrier électronique[1]. Autre, les réseaux sociaux, les nouveaux services afférents aux blogs, aux forums, aux wikis, à YouTube, à Twitter, etc… sont à l'origine de la croissance d'attaques. En effet, tous ces services en ligne jouent sur la confiance établie entre les membres d'un même réseau, la facilité de téléchargement, de publication et d'autres techniques d'échange des informations, qui rendent leurs utilisateurs vulnérables aux infections de logiciels malveillants[2]. Ces nouveaux services ont donné une ampleur sans précédent à certaines formes de fraude, qui se sont particulièrement épanouies sur l'internet. Les moyens techniques modernes permettant une répétition quasiment à l'infini dans l'espace et dans le temps de ces activités.

L'augmentation du nombre des serveurs clandestins qui permettent aux organisations criminelles de vendre des informations volées (données personnelles émises par les

[1] Baromètre annuel sur la cybercriminalité en 2008 par Kaspersky Lab.

[2] Eugène Kaspersky « Défis de la cybercriminalité », dossier « Cybercriminalité, une guerre perdue ? » Documentation française. Hiver 2008-2009

gouvernements, cartes de crédit ou débit, numéros d'identification personnels, numéros de comptes bancaires, listes d'adresses courriel) pour faciliter le vol d'identité démontre clairement la croissance dont réjouit l'activité cybercriminelle. Les Etats-Unis, l'Allemagne et la Suède viennent en tête de la liste des pays qui hébergent des serveurs clandestins, avec des pourcentages respectifs de 69 %, 12 % et 9 % de ce marché[3]. Le Maroc peut également être une source de cybercriminalité. Ce qui s'est passé avec le jeune marocain de 18 ans qui a conçu le virus « Zotob » est une preuve concluante que la menace peut émaner de votre voisin immédiat. Depuis un cybercafé du quartier Yacoub Mansour à Rabat, Farid Essebar a mis hors fonctionnement le site des deux chaînes américaines CNN & ABC, et celui du journal New York Times, du Boeing, et de l'aéroport de San Francisco.

Rappelons qu'en cette période de marasme économique, les attaques cybercriminelles sont censées connaître une forte hausse. En effet, il est reconnu que les périodes de ralentissement économique sont systématiquement caractérisées par des augmentations de la criminalité. Les experts de l'éditeur de solutions de sécurité PANDA[4] ont même établi une corrélation intéressante entre l'activité cybercriminelle et la conjoncture économique[5]. Les licenciements dans le secteur des technologies de l'information et l'abandon de projets dans le secteur entraînent un brusque mouvement ascendant de l'activité criminelle en général, et l'on doit s'attendre dans le ralentissement actuel à une forte croissance de l'activité cybercriminelle.

1.3 La cybercriminalité : Une activité rentable

Pour attirer l'attention de son auteur, une opération cybercriminelle devrait désormais générer du revenu. La cybercriminalité est devenue au fil des temps une activité extrêmement profitable. Des sommes importantes ont été détournées avec succès. Rien qu'en 2008, la cybercriminalité a coûté 1.000 milliards de dollars d'après une étude de McAfee[6] présentée au forum de Davos. Certaines sources estiment que la cybercriminalité a

[3] Symantec Internet Security Threat Report, 2007

[4] http://www.pandasecurity.com/

[5] http://www.mag-securs.com/spip.php?article12038

[6] « La sécurité des économies de l'information » présentée par l'éditeur McAfee au Forum économique mondial de Davos. http://www.lemonde.fr

dépassé le commerce illégal de la drogue en termes de profits en 2007. Voici quelques exemples d'actions cybercriminelles perpétrées en 2007[7].

- ✓ Janvier 2007 : Des pirates russes, avec l'aide d'intermédiaires suédois, auraient détourné 800 000 euros de la banque suédoise Nordea.
- ✓ Février 2007 : La police brésilienne arrête 41 pirates pour avoir utilisé un cheval de Troie pour voler les accès à des comptes bancaires et détourner 4,74 millions de dollars.
- ✓ Février 2007 : Dix-sept membres du « Gang de fraudeurs d'internet » sont arrêtés en Turquie après avoir volé plus de 500 000 dollars.
- ✓ Février 2007 : Li Jun est arrêté pour s'être servi du virus « *Panda burning Incense* » pour le vol de comptes d'accès utilisateurs de jeux en ligne et de messagerie instantanée. Les ventes de son programme malveillant auraient rapporté prés de 13 000 dollars.
- ✓ Mars 2007 : Cinq ressortissants d'Europe de l'Est sont emprisonnés au Royaume-Uni pour une fraude à la carte bancaire. Ils auraient dérobé 1,7 million de livres.
- ✓ Juin 2007 : 150 cybercriminels sont arrêtés en Italie. Ils sont accusés d'avoir bombardé des utilisateurs italiens avec des faux messages qui leur auraient rapporté 1,25 million d'euros sous forme de gains frauduleux.
- ✓ Juin 2007 : Des cyberdélinquants russes sont accusés d'avoir utilisé un cheval de Troie pour voler 500 000 dollars dans des banques de Turquie.
- ✓ Août 2007 : Maxim Yastremsky (alias « Maksik ») est arrêté en Turquie. Il est accusé d'avoir empoché 10 millions de dollars après le vol d'identificateurs.
- ✓ Septembre 2007 : Gregory Kopiloff est condamné aux Etats-Unis pour avoir utilisé les logiciels de partage de fichiers (*P2P*) *Limewire* et *Soulseek* pour collecter des données qu'il employait pour usurpation d'identité. Il aurait gagné des milliers de dollars par la commercialisation de données volées.

Ces exemples montrent bien le caractère rentable des activités cybercriminelles. Les cas d'infraction perpétrées dans une perspective d'appât du gain sont désormais monnaie courante dans le cyberespace. La cybercriminalité est depuis quelques années une source de rémunération, une activité que l'on pratique d'abord pour l'argent.

[7] Eugène Kaspersky, dossier « Cybercriminalité, une guerre perdue ? » Documentation française. Hiver 2008-2009

1.4 La cybercriminalité : Une activité facile

Avec la vulgarisation des modes opératoires cybercriminels sur l'internet, aujourd'hui il n'est pas nécessaire de disposer de compétences techniques pour lancer une opération cybercriminelle. Le niveau d'expertise technique requis pour un projet cybercriminel n'a plus du sens du moment où il est possible aujourd'hui d'acheter librement les logiciels espions les plus élaborés ainsi que les données collectées par ces mêmes logiciels : informations bancaires et informations personnelles suffisantes pour acheter en ligne ou transférer des fonds. En outre, il est aussi possible de commander un acte cybercriminel ponctuellement auprès de prestataires spécialisés qui viennent chacun apporter leur part d'expertise dans l'opération, chaque maillon générant des bénéfices dont le montant répond uniquement aux lois de l'offre et de la demande, la rareté d'une compétence augmentant les prix en conséquence.

Il existe de nombreuses ressources disponibles permettant de mettre au point des solutions complètes. Ces solutions vont de l'usage de la simple vulnérabilité, jusqu'à l'emploi des chevaux de Troie permettant d'automatiser des réseaux d'ordinateurs ou « *botnets*[8] ».

1.5 La cybercriminalité : Une activité à faible risque

L'internet est parfaitement adapté à l'activité frauduleuse (anonymat, faibles barrières à l'entrée, difficultés d'application de la loi à des juridictions multiples), et donc, comparé à la perpétration d'un crime « traditionnel » les coûts sont plus faibles et il est beaucoup moins probable d'être arrêté. Il s'agit donc d'une activité à faible risque comparé aux chances de réussite. Dans le monde réel, la dimension psychologique avec la prise de risques concrets du crime assure un certain effet de dissuasion. Mais dans le monde virtuel, les criminels ne sont jamais directement en contact avec leurs victimes ni avec les différentes sociétés qu'ils décident d'attaquer.

1.6 La cybercriminalité : Une activité organisée

Une étude conjointe entre le CERT et le FBI démontre que dans 81% des incidents recensés dans les entreprises, les attaquants avaient planifié leur action à l'avance. Il ne s'agit donc nullement d'opérations lancées au hasard. La réussite d'un acte cybercriminel exige une discipline de fer en amont, durant et en aval de toute opération cybercriminelle. Cette

[8] Un *botnet* est un réseau d'ordinateurs zombies contrôlés à l'insu de leurs propriétaires

discipline a comme pré requis de base, un travail en équipe dont les membres ne se sont probablement jamais rencontrés réellement. Ce travail d'équipe engage une segmentation et une spécialisation à outrance dans les différents maillons de la chaîne cybercriminelle. Ainsi au lieu de maîtriser l'ensemble de la chaîne des opérations, les cyberdélinquants se concentrent sur l'un de ses maillons, afin de le maîtriser à la perfection, ce qui permet de réduire considérablement leurs prises de risques. Analysons l'écosystème qui gravite autour par exemple des chevaux de troie. Souvent, ils sont conçus par des développeurs de logiciels, qui en général n'exploitent plus par eux-mêmes leurs créations. Ils concentrent leurs efforts sur l'innovation technologique nécessaire à la conception de ces codes malicieux, et s'organisent en micro-entreprises de deux ou trois développeurs, comprenant une cellule de support technique et un « commercial » chargé de développer les débouchés économiques du groupe. Ces développeurs vendent leurs créations comme de véritables produits, packagés avec une documentation utilisateur dans la langue de leurs clients. Certains groupes proposent même un support client 24/24 et offrent même une garantie de non détection du malware par l'antivirus[9].

2. Démystification de la notion de la sécurité de l'information

Pour mieux comprendre le phénomène de la cybercriminalité, il est important de s'attarder sur la notion de la sécurité de l'information. En effet, le phénomène tient son expansion à l'insécurité qui entoure l'utilisation des technologies d'information. Or la sécurité est un concept qui est souvent mal compris. D'où la nécessité de lever le voile sur cette notion afin de mieux en comprendre les enjeux.

2.1 La sécurité n'est pas seulement un enjeu technologique

Pour de nombreuses organisations, assurer la sécurité du système d'information (SI) se limite à la mise en place d'un pare feu et d'un antivirus. Or, ces dispositifs ne sont pas d'une grande utilité quand il s'agit par exemple d'attaques type « Ingénierie sociale[10] » qui connaît ces dernières années une évolution spectaculaire. En effet, dés fois pour avoir une information aussi critique soit-elle, il suffit de la demander. Inutile de se lancer dans des

[9] Joël Rivière « Criminalité et Internet, une arnaque à bon marché », dossier « Cybercriminalité, une guerre perdue ? » Documentation française. Hiver 2008-2009

[10] L'ingénierie sociale (social engineering en anglais) est une forme d'escroquerie utilisée en informatique pour obtenir un bien ou une information. Cette pratique exploite l'aspect humain et social de la structure à laquelle est lié le système informatique visé. Utilisant ses connaissances, son charisme, l'imposture ou le culot, le pirate abuse de la confiance, l'ignorance ou la crédulité de personnes possédant ce qu'il tente d'obtenir.

attaques sophistiquées ayant comme pré-requis un *background* technique évolué. Il suffit de prendre son téléphone et d'appeler. Au bout de fil vous avez un interlocuteur qui n'est pas sensibilisé aux risques liés à la diffusion de l'information. Face à ce genre de menaces, la protection physique et logique du SI, aussi robuste soit-elle, ne sert à rien.

La dimension organisationnelle de la sécurité est souvent négligée. Si des organisations comme la *CIA*, le *FBI* ou le *Pentagone* ont fait l'objet d'attaques, ce n'est surtout pas par manque de moyens techniques de protection. Ces organisations disposent de moyens colossaux pour assurer un niveau de sécurité adéquat. La faille est plutôt organisationnelle, voir humaine.

Certes, investir en matière technologique est inévitable pour mettre en place les outils nécessaires à la prévention, détection et correction des failles de sécurité. Cependant, l'aspect organisationnel qui consiste à mettre en place une politique de sécurité de l'information, une charte d'utilisation des ressources et l'ensemble des processus et procédures opérationnels permettant d'assurer un niveau de sécurité minimal est aussi important voir vital pour l'organisation. D'ailleurs, souvent lors des audits de sécurité, nous constatons que le volet technologique est plus ou moins maîtrisé. La nature des failles que nous identifions est plutôt organisationnelle. L'absence de politique de sécurité, le manque de formalisation du mode opératoire de la sauvegarde, le manque de l'inventaire des actifs critiques sont quelques exemples de lacunes en matière de sécurité organisationnelle.

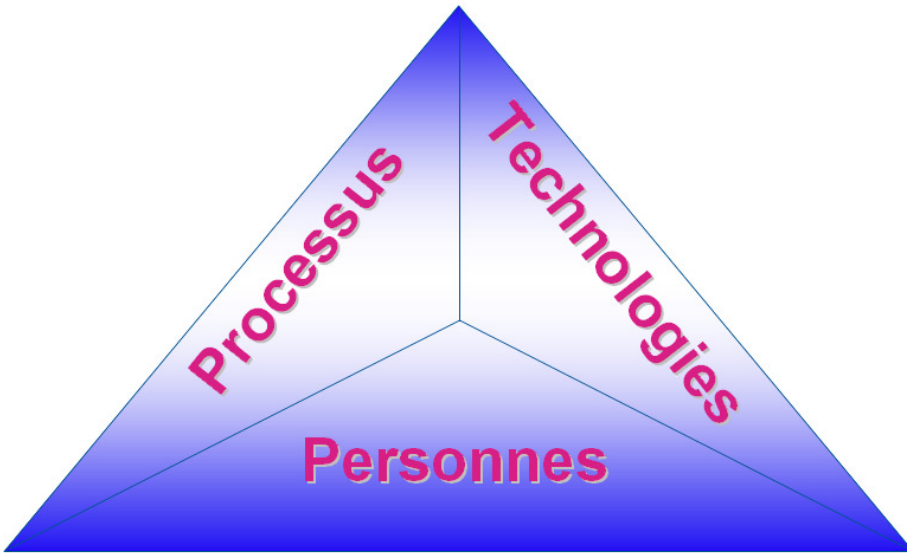

Figure 1 : Les trois dimensions de la sécurité

Le départ d'un employé

Le départ volontaire ou forcé d'un employé est un événement qui peut avoir lieu dans n'importe quelle organisation. Avons-nous eu le réflexe de verrouiller tous les comptes auxquels l'employé avait accès. Avons-nous supprimé son compte de messagerie. Avons-nous procédé à la récupération de tous les actifs dont l'organisation est propriétaire (badge, téléphone, ordinateur portable, etc…). Ce qui est mis en évidence ici, c'est la formalisation de la gestion des départs. C'est un aspect purement organisationnel de la sécurité qui fait impliquer le département de gestion des ressources humaines et le département de système d'information. Entre les deux entités, il faudra mettre en place une procédure de gestion des départs de telle sorte à ce que lors de chaque départ ou de changement de poste, un mécanisme instantané se déclenche pour verrouiller ou changer tous les comptes auxquels l'employé avait accès. Combien d'anciens collaborateurs continuent toujours à utiliser, dés fois même à des fins illicites, leur compte de messagerie et ce après avoir quitté l'organisation depuis des mois voir même depuis des années.

2.2 L'être humain est le maillon faible de la chaîne de la sécurité

La dimension humaine est aussi à prendre au sérieux. Pour se protéger des attaques traditionnelles de type « *phishing*[11] » par exemple, il faut sensibiliser l'utilisateur. Aucune technologie ne permettra à l'organisation de se prémunir totalement contre ce type d'attaques. Seule une campagne de sensibilisation donnera les effets désirables. Les experts de sécurité sont unanimes pour qualifier l'être humain de maillon faible de la chaîne de sécurité. Les pirates, l'ont bien compris. Ils orientent souvent leurs techniques de récupération d'informations vers cette perspective. *Kevin Mitnick*[12], l'un des célèbres pirates informatiques qui a publié plusieurs livres sur les techniques de *hacking* n'a été autre qu'un

[11] Le *phishing*, appelé en français l'hameçonnage, est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc.. Le *phishing* peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques.

[12] Kevin David Mitnick est un ancien pirate informatique américain. Il se faisait appeler « le Condor » en référence au film de Sydney Pollack « Les Trois Jours du condor ». Il est célèbre notamment pour avoir accédé illégalement aux bases de données des clients de Pacific Bell, ainsi qu'aux systèmes de Fujitsu, Motorola, Nokia et Sun Microsystems. Il est le premier pirate informatique à avoir figuré dans la liste des dix criminels les plus recherchés par le FBI aux Etats-Unis.

surdoué en matière d'ingénierie sociale qui consiste à exploiter les failles humaines pour récupérer de l'information.

Prenons l'exemple suivant : la plupart des organisations mettent en place un plan d'évacuation, qui permettra le cas échéant aux employés d'avoir accès à des sorties de secours en cas de danger, par exemple, un incendie. Examinons l'exemple ci-dessous, la porte de secours ne doit être ouverte que dans le cas d'activation d'une opération d'évacuation, et c'est bien mentionné sur la porte. L'organisation a collé un message stipulant que la porte doit toujours rester fermée. L'axe organisationnel de la sécurité est donc bien rempli. Il en est de même pour l'axe technologique. L'organisation a en effet investi dans l'acquisition d'une porte qui se ferme automatiquement une fois elle est ouverte. La faille doit être recherchée du côté de l'être humain. L'employé n'a pas respecté la consigne en immobilisant la porte pour la garder toujours ouverte. Ce comportement est fort probablement dû à un manque de sensibilisation. Il suffit que l'utilisateur ne suive pas la consigne pour que l'arsenal de protection mis en place tombe dans l'inutilité. C'est pourquoi l'être humain reste le maillon faible de la chaîne de sécurité.

Figure 2 : Un exemple de la faille humaine

2.3 Les incidents de sécurité ne viennent pas juste de l'externe

Souvent les organisations orientent leurs stratégies de sécurité uniquement dans la perspective externe. Elles supposent en effet, que la menace est de nature externe. Or, les statistiques montrent qu'à l'interne, il y a lieu aussi de s'inquiéter. Plus de 70% de dénis d'accès par exemple sont recensés depuis l'interne. Nous n'avons qu'à penser à un collaborateur à la fois motivé et mécontent. Même la compétence n'est pas un pré requis. En effet, avec la vulgarisation des attaques, il n'est pas nécessaire d'être un surdoué en informatique pour lancer telle ou telle opération. Aujourd'hui, grâce notamment à l'internet tout est accessible. Vous n'avez qu'à surfer sur *Google* pour vous rendre compte des possibilités illimitées qu'offre l'internet pour nuire.

Les incidents de sécurité à l'interne ont monté en puissance ces dernières années. Ils ont fait à plusieurs reprises la « Une » de l'actualité. Prenons l'exemple de ce qui s'est passé à la Société Générale en France fin 2007. Un employé de la banque du nom Jérôme Kerviel[13] a déjoué les mécanismes du contrôle interne et il a ainsi dissimulé de nombreuses positions qui ont failli mettre en péril la banque. Quand on examine bien cette affaire, on se rend compte que ce qui s'est passé n'est autre qu'une histoire de mauvaise gestion des accès.

Vengeance, besoin de reconnaissance sont souvent les premier éléments de motivation des attaques internes. Les enquêtes menées par les organismes spécialisés regorgent d'exemples de données volées ou détruites par des employés licenciés. Le rapport du *CSI/FBI* intitulé «*Computer crime and security survey 2005*[14]» signale que la plupart des incidents affectant les entreprises américaines ont une cause interne. Souvent aussi, leurs conséquences sont bien plus graves que les dommages causés par les attaques externes. A titre d'exemple, les responsables de la représentation d'*UBS* à Tokyo ont admis la disparition d'un disque dur contenant des données hautement confidentielles sur la clientèle. La délimitation peu claire des compétences et le non-respect des directives internes sont à l'origine de cette perte.

[13] Jérôme Kerviel est un opérateur de marché de la Société générale accusé par son employeur d'être le responsable de 4,82 milliards d'euros parmi les pertes de la banque en janvier 2008 résultant de prises de positions dissimulées et contraires aux règlements de la Société générale d'environ 50 milliards d'euros sur des contrats à terme sur indices d'actions entre 2007 et début 2008.

[14] http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf

Les actes de malveillance ne représentent pas l'unique typologie d'incidents internes. Les accidents et les erreurs représentent aussi une bonne partie d'incidents recensés à l'interne. Ainsi, une banque marocaine a vu son système d'information indisponible pendant plusieurs heures et à travers toutes ses agences suite à un déploiement non contrôlé d'un correctif[15]. Le cas de la Bourse de Casablanca, qui par carence collective grave au niveau de son management[16], a vu des informations relatives aux ordres cachés, dits icebergs, véhiculés par le système de diffusion de la BVC à travers le site de Bourse en ligne Boursomaroc, est un exemple qui rappelle que les conséquences des erreurs peuvent être aussi scandaleuses que celles des actes de malveillance.

Chantage auprès de la Direction Générale

Les employés d'une société marocaine ont reçu une photo compromettante remettant en cause le caractère moral de l'un de leurs directeurs. Après enquête, il s'est avéré que l'attaque venait de l'interne. Un employé de la société n'étant pas dans les bons termes avec sa hiérarchie utilisait une boite de messagerie externe pour envoyer la dite photo à l'ensemble des employés pour faire du chantage auprès de la direction générale.

2.4 La sécurité, ce n'est pas juste la confidentialité

La sécurité des SI repose sur les quatre piliers suivants :

La disponibilité

La disponibilité se manifeste en terme d'accessibilité aux ressources du SI (Ordinateurs, Serveurs, Bases de données, Réseaux, services, etc…). L'indisponibilité est probablement l'événement indésirable le plus ressenti par les utilisateurs du SI. En effet, souvent quand un service est indisponible, on ressent les effets immédiatement. Incapacité à remplir les tâches quotidiennes, interruption des services et dysfonctionnements au niveau des activités de l'entreprise, sont quelques exemples de conséquences qu'une indisponibilité peut provoquer.

[15] Un correctif est une section de code que l'on ajoute à un logiciel, pour y apporter des modifications mineures afin de corriger la faille de sécurité.

[16] http://www.financesnews.ma/article_detail.php?id_art=4983

L'indisponibilité peut être provoquée par plusieurs typologies d'attaques malveillantes. Elle est visée notamment par les attaques qualifiées de déni de service « *DoS* [17]» et déni de service distribué « *DDoS*[18] ». Une attaque virale, une intrusion ou l'exploitation d'une vulnérabilité peuvent avoir aussi comme effet une indisponibilité totale ou partielle du SI. A cette liste, on peut ajouter les attaques physiques sur les installations informatiques ou le câblage des réseaux qui ne requièrent que peu de technologie et qui engendrent les mêmes effets.

L'intégrité

De manière générale, l'intégrité des données désigne l'état de données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation. L'intégrité des données comprend quatre éléments : l'intégralité, la précision, l'exactitude/authenticité et la validité[19].

L'atteinte à l'intégrité peut avoir de lourdes conséquences sur la fiabilité d'un SI. A titre d'exemple, la mise en cause de l'exactitude des données stockées dans un système de banque aurait des conséquences immenses. La fausseté de celles stockées dans un système médical représenterait un danger mortel. Ce type d'altération peut même faire l'objet de menaces de tentatives d'extorsion envers des organismes ciblés. Les virus ou autres logiciels malveillants peuvent aussi entraîner la destruction ou l'altération partielle de données.

La preuve

La preuve est la garantie de ne pas pouvoir réfuter une transaction avec possibilité de pouvoir auditer les résultats fournis (exemple : un virement de fonds et la vérification du journal comptable à partir des informations d'entrée). Lorsqu'il n'y avait que le niveau technique de la preuve (numérique), l'auditabilité était restreinte à de la traçabilité (capacité

[17] Denial of Service (DoS), Dénis de Service en français, est une attaque ayant pour but de rendre indisponible un service.

[18] Distribued Denial of Service (DDoS), Dénis de Service Distribué en français, est une attaque ayant pour but de rendre indisponible un service impliquant une multitude d'ordinateurs « zombies ».

[19] http://fr.wikipedia.org/wiki/Intégrité_des_données

à garder la trace des décisions prises et des actions entreprises), voire à de l'imputabilité (capacité à attribuer à un auteur une décision ou à un exécutant une action).

La confidentialité

La confidentialité demeure le pilier le plus difficile à cerner. En effet, une atteinte à la confidentialité est irréversible. On ne peut procéder à un « lavage des cerveaux » des personnes ayant eu un accès accidentel ou illicite à une information confidentielle. Alors qu'une atteinte à la disponibilité, intégrité ou à la preuve peut être redressée.

La copie de secrets commerciaux, l'identification des informations sensibles concernant les réseaux ou les utilisateurs suite à une intrusion dans un SI, l'accès aux bases de données sont quelques exemples d'une attaque logique visant l'atteinte à la confidentialité. Cette dernière peut être aussi violée physiquement. On néglige souvent la copie physique et le vol des supports de stockage de données notamment les clés *USB*, qui impliquent un faible niveau de maîtrise technologique.

2.5 Faire de la sécurité, c'est être « fermé » dans un environnement complètement ouvert

L'internet, en tant qu'environnement n'appartenant à la fois à personne et appartenant à tout le monde, offre des opportunités d'affaires illimitées. Plusieurs entreprises l'ont bien compris. Elles ont construit leurs modèles d'affaires sur cette base. Le cas d'Amazon[20] qui n'est autre qu'une immense base de données de livres, offrant la possibilité de se procurer un livre en « *one clic* » est à appréhender. En effet, Amazon n'est pas un éditeur de livre. Pourtant, elle s'engage à vous fournir le livre que vous souhaitez avoir, sous réserve qu'il soit disponible, dans un délai très court. Autrement dit, Amazon est une entreprise en réseau ayant un système d'information interconnecté avec celui de ses fournisseurs, partenaires et clients. Sans le web, le modèle d'affaires de Amazon n'aurait pas été possible. L'exemple de Dell[21]est aussi à méditer. L'entreprise ayant comme stratégie de différenciation, la personnalisation des offres et la vente directe des ordinateurs, n'est pas un constructeur d'ordinateur, c'est un assembleur. Néanmoins, elle s'engage à vous fournir l'ordinateur que vous souhaitez avoir dans un délai très court. La carte mère étant fabriquée dans un pays,

[20] http://www.amazon.com

[21] http://www.dell.com

l'écran dans un autre, l'assemblage se fait quelque part dans le monde. Dell n'est autre qu'une entreprise en réseau qui tire profit du Web pour faire aboutir son modèle d'affaire. Il est d'ailleurs, extrêmement difficile de délimiter les frontières du SI d'une entreprise comme Dell. Les fournisseurs, les partenaires logistiques, les clients se trouvent sur le même SI. Sans le Web ce modèle d'affaire ne serait pas possible.

S'ouvrir donc, attire plus d'opportunités. Mais, ceci ramène aussi de nouvelles menaces auxquelles il faudra faire face. En opérant dans un environnement ouvert, les organisations se trouvent exposées à des attaques qui ne peuvent avoir lieu dans un environnement complètement fermé. Une entreprise qui propose à ses clients des services transactionnels sur son site Web, se voit contrainte d'investir en sécurité pour mieux protéger ses intérêts et ceux de ses clients.

Etant donné qu'aujourd'hui, les organisations sont contraintes sous l'effet de la concurrence de plus en plus féroce d'imaginer de nouvelles façons d'opérer en proposant des services à valeur ajoutée, la tendance est plutôt vers l'ouverture. Les entreprises marocaines n'y échapperont pas pour longtemps. Dans cette perspective, continuer à sécuriser son SI reviendra à être « fermé » dans un environnement complètement ouvert. Ce qui est loin d'être simple. Cet équilibre est très difficile à aller chercher.

2.6 La fin de la sécurité périmétrique

La première chose à laquelle nous pensons pour sécuriser le SI d'une organisation est le périmètre externe. Déployer un Pare-Feu, mettre en place des mécanismes de filtrage de contenu et de filtrage *URL*, installer un système de détection et de prévention d'intrusion, sont quelques exemples de la sécurité périmètrique.

Depuis quelques années, nous constatons une meilleure prise en compte des recommandations à ce niveau. Il en résulte qu'une attaque est plus difficile à opérer sur le périmètre externe. Il fallait donc monter dans les couches du modèle *OSI*[22] pour notamment passer au travers les défenses périmétriques directement par les serveurs applicatifs et les applications métiers et indirectement via les postes utilisateurs qui sont généralement moins

[22] Le modèle OSI (Open Systems Interconnection) est un modèle de communications entre ordinateurs proposé par l'ISO (Organisation internationale de normalisation). Il décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions.

protégés et qui offrent plus de fonctionnalités et de services (accès au réseau interne, accès à l'Internet, etc…). L'intérêt est multiple :

- Flux autorisés vers les serveurs (http, ftp, etc….) ;
- Produits ayant d'avantage de vulnérabilités (Web) ;
- Applications métiers propriétaires (non éprouvées, peu auditées, etc…) ;
- Lien direct avec les données métiers.

Il en résulte qu'aujourd'hui la menace est de plus en plus applicative. Quand on développe une application, la sécurité reste le dernier souci. Nous développons en fonction d'un cahier des charges qui précise les fonctionnalités cibles qu'il va falloir couvrir. Par conséquent, nous arrivons avec une application qui certes, répond à des exigences fonctionnelles, mais sur le plan de sécurité présente souvent des vulnérabilités critiques allant jusqu'à la possibilité de prise en main à distance d'un serveur applicatif. Des statistiques récentes montrent à quel point la menace applicative est devenue sérieuse.

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	A7 – Failure to Restrict URL Access
<not in T10 2007>	A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	A10 – Insufficient Transport Layer Protection
A3 – Malicious File Execution	<dropped from 2010>
A6 – Information Leakage and Improper Error Handaing	<dropped from 2010>

Figure 3 : Top 10 des vulnérabilités applicatives[23]

Sur l'ensemble des vulnérabilités identifiées en 2008, 63 % concernaient des applications Web, contre 59 % en 2007[24].

[23] Source : OWASP http://www.owasp.org

[24] «Symantec Internet Security Threat Report :2008»
http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20090414_01

2.7 L'exploit d'une vulnérabilité est de plus en plus rapide

S'il y a quelques années, le temps moyen entre la publication d'une vulnérabilité et son exploitation était quelques semaines, en 2008, 80% des exploits de vulnérabilité étaient disponibles après 1 à 9 jours de la divulgation de vulnérabilité au public. Durant la même année, *Qualys Labs* à identifié 56 exploits de failles zéro-jour, y compris la vulnérabilité *RPC* qui produisait *Conficker*[25]. En 2009, la première vulnérabilité publiée par *Microsoft, MS09-001* avait un exploit disponible dans un délai de sept jours[26].

En 2003, un ordinateur non protégé, doté d'un système type *Windows* et connecté à l'internet, pouvait résister 40 minutes avant d'être infecté par un virus. En 2004, 20 minutes. En 2009, un ordinateur non sécurisé est infecté, en moyenne, au bout de 4 minutes selon des conclusions récentes de l'institut *SANS*[27].

Comme on peut le constater sur la figure ci-dessous, le nombre de « victimes » évolue rapidement. Seule une veille de vulnérabilités permettra de réagir au bon moment afin d'apporter les corrections nécessaires.

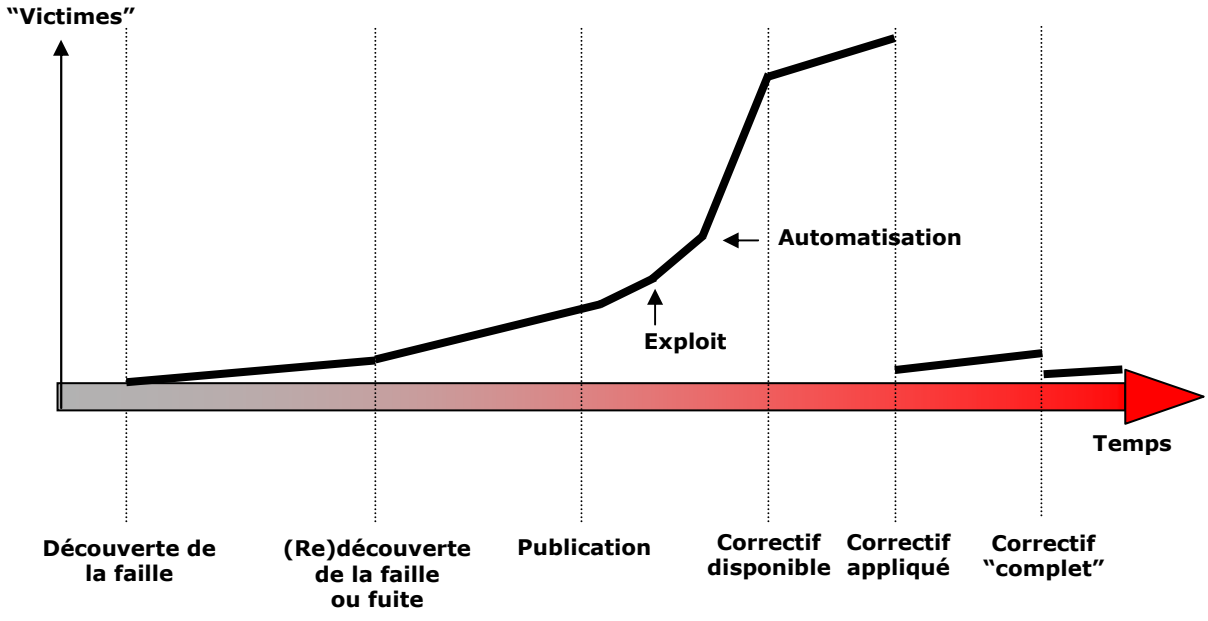

Figure 4 : Le cycle de vie de la vulnérabilité

[25] Il s'agit d'un virus apparu fin novembre 2008, connu aussi sous les noms de Downup, Downandup et Kido). Il est principalement installé sur les machines fonctionnant sous Windows XP

[26] « Les lois de vulnérabilités 2.0 », Qualys http://www.qualys.com/docs/Laws_2.0.pdf

[27] https://isc2.sans.org/survivaltime.html

2.8 Assurer la sécurité de son SI est de plus en plus une contrainte réglementaire

Les organisations ayant un niveau de maturité élevé en matière de sécurité n'investissent en sécurité qu'après avoir mené un *Business Impact Analysis.* Seule donc, une analyse de risque permettra à l'organisation de savoir quels sont les risques qu'elle court et surtout quel sera l'impact si jamais ils se matérialisent. Cette démarche aboutit à un choix plus ou moins rationnel en termes d'investissements en sécurité.

La démarche de *Business Impact Analysis* a cédé la place depuis quelques années à la pression réglementaire qui impose notamment aux banques, opérateurs télécoms et filiale de multinationale une conduite stricte en matière de sécurisation du SI. Plusieurs cadres réglementaires ont vu le jour. Nous retenons ici :

2.8.1 Les accords de Bâle II

Initialement basées sur une approche purement financière des risques, les recommandations du comité Bâle ont été profondément étendues en 2004 via l'accord Bâle II. Ces recommandations sont mises en œuvre par l'immense majorité des établissements financiers au niveau mondial.

L'innovation majeure de ce nouvel accord par rapport à celui de 1988 tient à l'introduction du risque opérationnel, recouvrant les risques relatifs à la sécurité des biens et des personnes (incendies, vol et fraude, etc.), les risques informatiques (développement, maintenance et exploitation des systèmes) et les risques liés aux procédures de gestion interne (erreurs humaines, malveillance, etc.). Différentes approches sont possibles pour évaluer ce risque opérationnel, mais la plus performante est basée sur l'historique des événements et des pertes associées.

L'accord Bâle II vise à mettre sous contrôle l'ensemble des risques auxquels sont soumis les établissements financiers, et non plus seulement les risques financiers directement liés à leur activité. Tout en restant spécifiquement adapté au secteur bancaire, et notamment à sa grande maturité en matière de gestion des risques, il se rapproche ainsi de réglementations plus génériques comme la loi *Sarbanes-Oxley*.

Au Maroc, de nombreux projets de sécurisation SI ont vu le jour dans les établissements bancaires sous la pression des accords Bâle II. Nous citons, notamment :

- ✓ La mise en place d'une cartographie des risques (y compris les risques liés à la sécurité des SI) ;
- ✓ La mise en place d'un plan de continuité d'activité ;
- ✓ La mise en place de solutions de détection et de prévention de fraudes.

2.8.2 PCI DSS

Tous les acteurs économiques qui traitent, stockent et transmettent des données et transactions de cartes bancaires, doivent intégrer la norme *PCI DSS* (*Payment Card Industry Data Security Standard*). Cette norme est encadrée par le *PCI Security Standards Council*, une organisation fondée en 2005 par les principaux acteurs du secteur des cartes bancaires : *MasterCard, Visa, American Express, Discover Financial Services et JCB*.

La norme *PCI* est présentée comme la garantie d'un haut niveau de sécurité. Elle correspond à une série de douze exigences auxquelles sont assujetties les organisations dont les réseaux, les serveurs et les applications entrent en contact avec les données des titulaires de carte. Concrètement, ces organisations doivent :

1. Installer et gérer une configuration de pare-feu afin de protéger les données des titulaires de carte ;
2. Ne pas utiliser les paramètres par défaut du fournisseur pour les mots de passe et les autres paramètres de sécurité de système ;
3. Protéger les données des titulaires de cartes stockées ;
4. Crypter la transmission des données des titulaires de carte sur les réseaux publics ouverts ;
5. Utiliser et mettre à jour régulièrement un logiciel antivirus ;
6. Développer et gérer des applications et systèmes sécurisés ;
7. Limiter l'accès aux données des porteurs de carte aux cas de nécessité professionnelle absolue ;
8. Attribuer une identité d'utilisateur unique à chaque personne disposant d'un accès informatique ;
9. Limiter l'accès physique aux données des titulaires de carte ;
10. Suivre et surveiller tous les accès aux ressources du réseau et aux données des titulaires de carte ;
11. Tester régulièrement les systèmes et procédures de sécurité ;

12. Disposer d'une politique régissant la sécurité de l'information.

Si une ou plusieurs des exigences *PCI* ne sont pas satisfaites, les organisations s'exposent à des mesures punitives qui pourraient comprendre des amendes proportionnelles à l'infraction, pouvant atteindre des centaines de milliers de dollars, la révocation du privilège de traitement des cartes de crédit et le refus d'émettre un certificat de conformité. L'inobservation des normes *PCI* pourrait en outre porter préjudice à la marque et à la réputation de l'entreprise, et même entraîner sa faillite. Les commerçants peuvent aussi recevoir des incitatifs importants pour se conformer aux exigences de la norme *PCI DSS.*

Au Maroc, Attijariwafa Bank, Banque Marocaine du Commerce Extérieur, Banque Populaire, Centre Monétique Interbancaire, Poste Maroc et Maroc Télécommerce ont démarré, sous la pression notamment de *VISA*, les chantiers de conformité aux exigences de la norme *PCI DSS*.

2.8.3 Sarbanes Oxley

La loi *Sarbanes Oxley* (*SOX*), du nom respectif des deux sénateurs Paul Sarbanes et Michael G. Oxley, a été adoptée par le congrès américain en Juillet 2002. Elle a vu le jour suite aux multiples scandales comptables et financiers : *Enron*, *Tyco International* ou encore *WorldCom*. Plusieurs points liés à la sécurité des SI doivent faire l'objet d'un contrôle strict au sens de SOX. Il s'agit notamment de :

1) La gestion des mots de passe

- ✓ Le niveau de sécurité des mots de passe ;
- ✓ La vérification du changement des mots de passe tous les six mois ;
- ✓ L'étude des notes délivrées par le responsable sécurité aux employés sur la politique des choix de mots de passe ;
- ✓ Un exemple concret de test consisterait à évaluer la sécurité des mots de passe de 30 utilisateurs, et à identifier la proportion de mots de passe faibles.

2) L'étude de réseau informatique

- ✓ Vérification de l'authentification des accès VPN ;
- ✓ Protection du réseau interne par 2 niveaux de pare-feux ;
- ✓ Contrôle et journalisation des accès à Internet ;
- ✓ Signature d'une charte de bon usage d'Internet ;
- ✓ Authentification des utilisateurs pour accéder à Internet ;
- ✓ Révocation des certificats lors du départ des collaborateurs ;

- ✓ Filtrage des emails vis-à-vis des menaces connues: virus, chevaux de Troie, etc.

3) Plan de reprise en cas de désastres

- ✓ Sauvegarde des serveurs principaux ;
- ✓ Externalisation des supports de sauvegarde ;
- ✓ Rédaction d'un document de procédure de restauration pour chaque serveur.

4) La journalisation & Audits

- ✓ Mener des audits internes afin d'assurer le bon fonctionnement des mesures de sécurité prises par l'entreprise ;
- ✓ Vérification de l'existence des fichiers de logs des serveurs mails, des navigateurs internet et des accès VPN ;
- ✓ Traçabilité des accès aux applications financières et ressources humaines ;
- ✓ Sauvegardes des emails conservées durant 1 mois minimum (destinataire, l'envoyeur, le sujet, la date et l'heure et l'*IP*).

2.9 Le RSSI : un nouveau métier

S'il y a quelques années, la fonction de sécurité n'était, au mieux, qu'un ensemble de tâches réalisées par le responsable des réseaux, aujourd'hui elle s'impose comme un métier à part. Une organisation ayant atteint une taille minimale en termes de nombre d'ordinateurs (plus de 500 postes de travail) dans son parc informatique, ne peut continuer à traiter la fonction de la sécurité d'une façon éparpillée. En effet, en remettant la sécurité aux mains de l'expert informatique (généralement le responsable des réseaux ou le responsable de l'exploitation), seulement l'aspect technologique de la sécurité est pris en compte. Souvent, assurer la sécurité dans une telle configuration se limite à l'acquisition de logiciels adéquats. Les risques purement organisationnels et humains ne peuvent être pris en charge dans un tel contexte. Beaucoup d'organisations ont bien saisi les limites d'une telle approche. Elles disposent aujourd'hui d'une fonction entièrement dédiée à la sécurité prise en charge par ce qui est communément appelé RSSI (Responsable de Sécurité des Systèmes d'Information).

Dépendamment du niveau de maturité de la sécurité au sein de l'organisation, le RSSI peut être rattaché hiérarchiquement à différentes entités de l'entreprise. Le rattachement à la direction générale peut être fait au sein de très grandes entreprises mais avec un rôle beaucoup plus large tendant plus vers le management du risque de la société toute entière[28]. Souvent, dans des organisations structurées, le RSSI est rattaché à la direction des systèmes

[28] Bernard Foray « La fonction RSSI », Edition Dunod, 2007

d'information. Dans les structures de taille moyenne, le RSSI a souvent un positionnement orienté vers l'expertise technique. Il garantit avant tout la pérennité et l'évolution de l'infrastructure pour faire face aux attaques et aux risques extérieurs. Il n'encadre généralement pas d'équipe. Alors que, en raison notamment d'une culture interne forte en matière de gestion des risques, le poste de RSSI revêt un enjeu stratégique et dispose en conséquence de moyens plus importants qu'ailleurs. Il gère son budget, encadre généralement une équipe d'experts techniques, voire fonctionnels, et occupe un positionnement transverse dans l'entreprise.

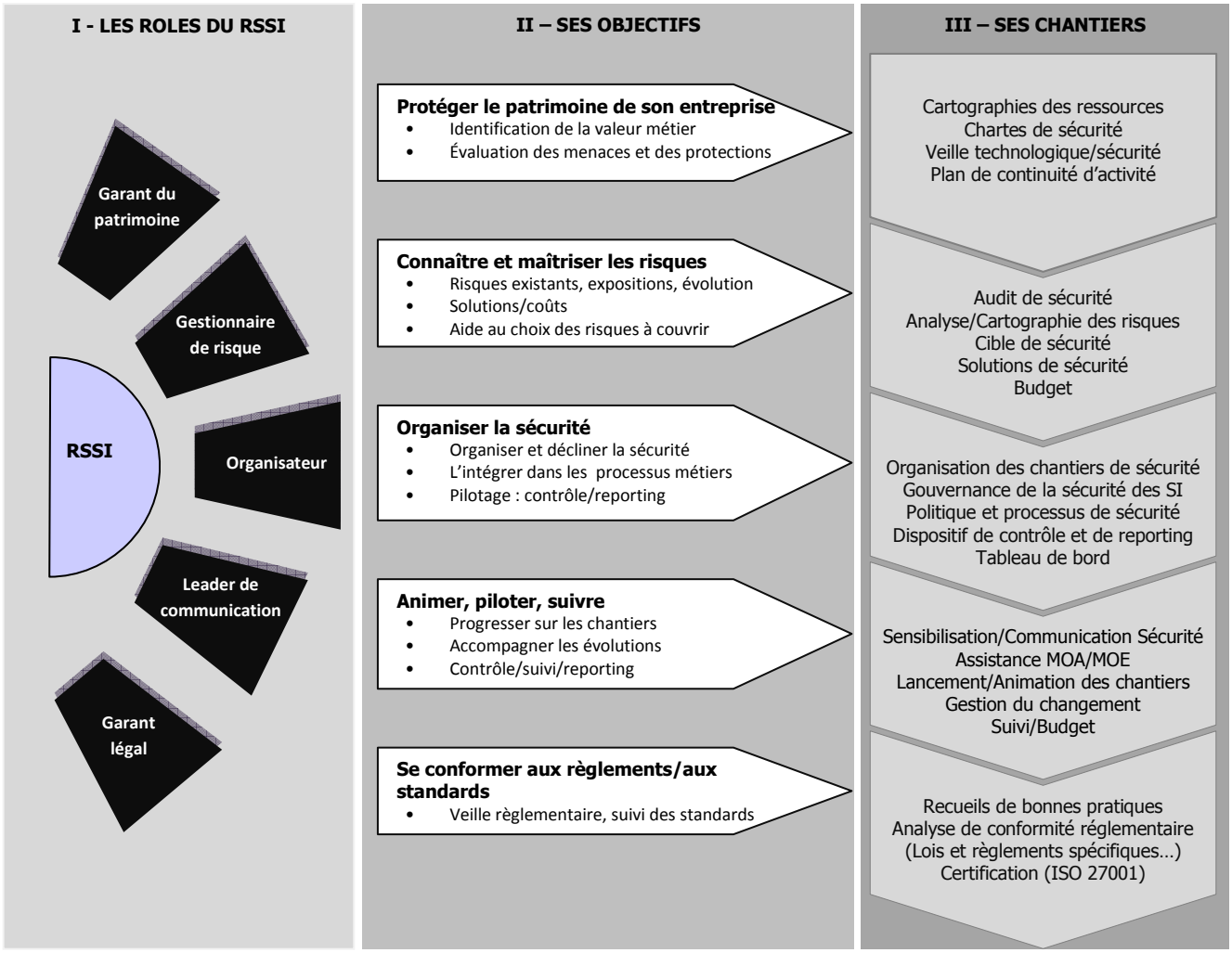

Figure 5 : Les rôles, les objectifs et les chantiers du RSSI

2.10 La sécurité est une question de gouvernance

La sécurité de l'information a été longtemps épargnée des mouvements de meilleures pratiques et de référentiels. Les RSSI se trouvaient souvent désarmés face à la bonne canalisation des énergies en matière de sécurisation SI. L'absence de repère en la matière compliquait constamment leurs tâches. Aujourd'hui, grâce à l'émergence de plusieurs référentiels de sécurité, notamment la famille des normes ISO 27000, les RSSI disposent de la matière pour mettre en place la gouvernance de la sécurité de l'information. Parmi ces référentiels, ISO 27002, en tant que bibliothèque de meilleures pratiques, demeure le référentiel le plus utilisé quand il s'agit d'aborder la sécurité dans une perspective transversale. En effet, outre les aspects liés à la sécurité logique, les aspects liés à la sécurité physique, à la sécurité liée aux ressources humaines et aux aspects juridiques sont largement couverts à travers cette norme.

2.10.1 ISO 27001

L'ISO/CEI 27001 est une norme internationale de système de management de la sécurité de l'information (SMSI), publiée en octobre 2005 par l'*ISO*.

L'ISO/CEI 27001 définit l'ensemble des tests et contrôles à effectuer pour s'assurer du bon respect d'ISO/CEI 27002. Elle s'est inspirée du modèle PDCA (Roue de Duming) rappelée, ci-après :

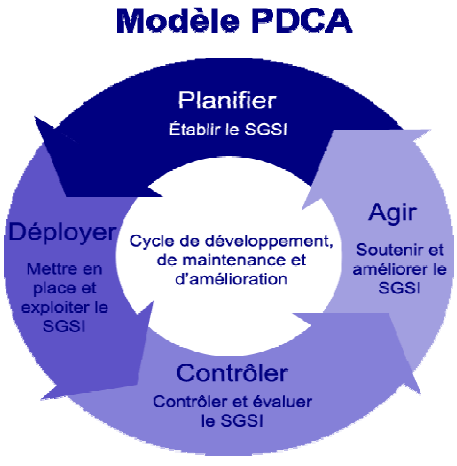

Figure 6 : Le modèle PDCA

Le modèle PDCA (Planifier, Déployer, Contrôle et Agir) impose le respect des points contrôles par rapport à chaque section.

1) Planification : Etablir le SMSI

L'organisme doit respecter les points de contrôles suivants :

- Définir le champ détaillé d'application du SMSI (processus métiers, organisation, location, biens, technologies) ;
- Définir la politique du SMSI ;
- Définir l'approche d'évaluation des risques (méthode, critère d'acceptation, etc.) ;
- Identifier les risques (biens traités, menaces, vulnérabilités potentielles, impacts) ;
- Analyser et évaluer les risques (impact métier, probabilité, gravité) ;
- Définir la stratégie de traitement des risques (transfert, accepte, etc.) ;
- Définir les mesures (objectifs, points de contrôle) de limitation des risques ;
- Obtenir l'accord du management sur la stratégie de traitement des risques ;
- Obtenir l'accord du management pour implémenter le SMSI ;
- Formaliser la stratégie de traitement des risques (choix des mesures à mettre en œuvre, liste des mesures déjà appliquées, justification de l'élimination de points de contrôle).

2) Déploiement : Mettre en place et exploiter le SMSI

L'organisme doit respecter les points de contrôles suivants :

- Définir un plan d'actions de traitement des risques (mesures de protection, ressources, responsabilités, priorité, etc.) ;
- Organiser le déploiement du plan d'actions de traitement des risques ;
- Déployer les points de contrôle / les mesures de protection ;
- Définir la stratégie de suivi et de mesure de l'efficacité des actions ;
- Déployer un programme de formation / sensibilisation ;
- Piloter / gérer les aspects opérationnels du SMSI ;
- Mettre en œuvre des procédures et des moyens de détection et de traitement des incidents.

3) Contrôle : Contrôler et évaluer le SMSI

L'organisme doit respecter les points de contrôles suivants :

- Mettre en œuvre les procédures et les moyens de suivi (détection d'erreurs, suivi des incidents, des tentatives d'exploitation de failles, contrôle des performances humaines et technologiques, etc…) ;
- Organiser le suivi de l'efficacité du SMSI prenant en compte les résultats d'audit, les relevés d'incidents, les mesures d'efficacité, les suggestions et avis des intervenants dans le SMSI, etc.)
- Mesurer et contrôler l'efficacité des mesures déployées ;

- Réévaluer régulièrement les risques ;
- Effectuer régulièrement des audits du SMSI ;
- Organiser le suivi du SMSI au niveau du Management (Direction Générale) ;
- Adapter / mettre à jour le plan d'actions sécurité (prendre en compte les indicateurs de suivi d'efficacité) ;
- Enregistrer / les actions et les évènements qui peuvent avoir un impact sur l'efficacité du SMSI.

4) Action : Soutenir et améliorer le SMSI

L'organisme doit respecter les points de contrôles suivants :

- Implémenter les modifications identifiées dans le SMSI ;
- Prendre des mesures correctives et préventives (prendre en compte les retours d'expérience internes ou externes) ;
- Communiquer sur les mesures et les adaptions du SMSI aux personnes impliquées ;
- Vérifier que les correctifs/modifications répondent aux objectifs fixés.

2.10.2 ISO 27002

L'ISO/CEI 27002 est un ensemble de 133 mesures dites « *best practices* », destinées à être utilisées par tous ceux qui sont responsables de la mise en place ou du maintien d'un Système de Management de la Sécurité de l'Information (SMSI). La sécurité de l'information est définie au sein de la norme comme la « préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information ».

Cette norme n'a pas de caractère obligatoire pour les entreprises. Son respect peut toutefois être mentionné dans un contrat : un prestataire de services pourrait ainsi s'engager à respecter les pratiques normalisées dans ses relations avec un client.

La norme ISO/CEI 27002 est composée de onze sections principales, qui couvrent le management de la sécurité aussi bien dans ses aspects stratégiques que dans ses aspects opérationnels. Chaque section constitue un chapitre de la norme :

- ✓ Chapitre 1 : Politique de sécurité
- ✓ Chapitre 2 : Organisation de la sécurité de l'information
- ✓ Chapitre 3 : Gestion des biens
- ✓ Chapitre 4 : Sécurité liée aux ressources humaines
- ✓ Chapitre 5 : Sécurité physique et environnementale

- ✓ Chapitre 6 : Gestion des communications et de l'exploitation
- ✓ Chapitre 7 : Contrôle d'accès
- ✓ Chapitre 8 : Acquisition, développement et maintenance des systèmes d'information
- ✓ Chapitre 9 : Gestion des incidents liés à la sécurité de l'information
- ✓ Chapitre 10 : Gestion de la continuité d'activité
- ✓ Chapitre 11 : Conformité légale et réglementaire

Chaque section spécifie les objectifs à atteindre et énumère un ensemble de mesures (les « best practices ») permettant d'atteindre ces objectifs. La norme ne détaille pas les mesures, car chaque organisation est censée procéder à une évaluation de ses propres risques afin de déterminer ses besoins avant de choisir les mesures qui seront appropriées dans chacun des cas possibles.

Cette norme est de plus en plus utilisée par les entreprises du secteur privé comme un référentiel d'audit et de contrôle, en complément de la politique de sécurité de l'information de l'entreprise. Le fait de respecter cette norme permet de viser, à moyen terme, la mise en place d'un Système de Management de la Sécurité de l'Information, et à long terme, une éventuelle certification ISO/CEI 27001.

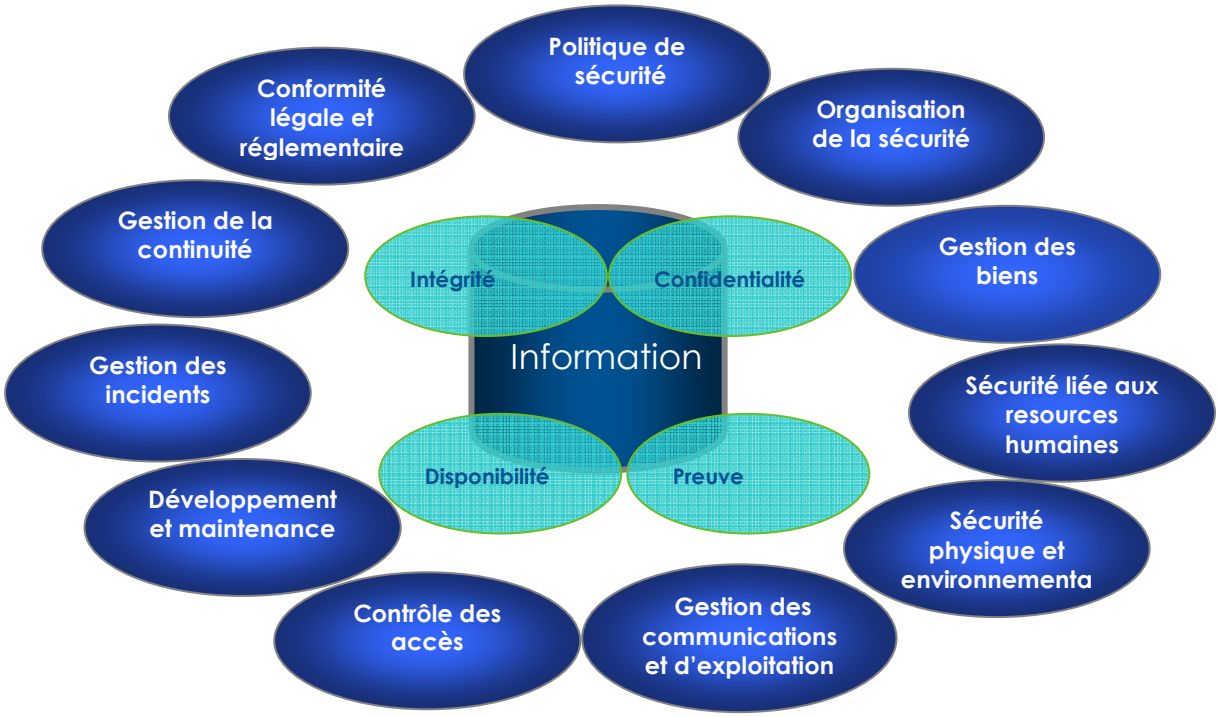

Figure 7 : Les 11 chapitres de la norme ISO 27002

Conclusion du chapitre

La cybercriminalité est un business organisé, facile, à faible risque et surtout très rentable. De nombreux utilisateurs peu scrupuleux et en quête d'argent facile n'hésitent pas à s'y lancer. L'incompréhension qui entoure l'univers de la sécurité de l'information leur facilite grandement la tâche. En effet, la sécurité est souvent appréhendée comme un pur phénomène technologique. Or, la menace organisationnelle peut avoir un impact aussi important qu'une faille technique. En outre, l'être humain reste le maillon faible de la chaîne de la sécurité et il faut le considérer en tant que tel. A quoi sert la sécurité d'un SI, aussi robuste soit-elle, si l'utilisateur continue à mettre son mot de passe sur un bout de papier et à le coller sur son ordinateur.

Une bonne gouvernance de la sécurité SI doit s'inspirer des meilleures pratiques en la matière. Le recours à un référentiel adressant les trois dimensions de la sécurité à savoir : la dimension organisationnelle, la dimension technologique et la dimension humaine est vital pour toute organisation souhaitant sécuriser son SI.

Chapitre 2 : Les multiples visages de la cybercriminalité

« Deux choses sont infinies :
L'Univers et la bêtise humaine »
Albert Einstein

La cybercriminalité a de multiples visages. Chaque jour, elle se manifeste d'une nouvelle manière. Tantôt elle n'est que la virtualisation d'anciennes méthodes d'escroqueries tantôt elle nous surprend par le caractère « novateur » du mode opératoire qu'elle applique. Les attaques cybercriminelles sont potentiellement illimitées. En effet, l'émergence de nouvelles applications va nécessairement générer des failles de sécurité[29]. Le lancement de chaque logiciel comporte des failles non référencées que des cybercriminels s'empresseront d'exploiter à des fins de racket ou d'espionnage industriel ou autre (type attaque Zero Day). Les cybercriminels ont donc de beaux jours encore devant eux. Il y aura toujours une activité déviante dans le cyberespace tant que nous continuons à utiliser des applications potentiellement vulnérables.

Pour présenter les différentes formes de la cybercriminalité, il nous a semblé pertinent de les appréhender à travers les objectifs visés par rapport aux quatre piliers de la sécurité à savoir, la disponibilité, l'intégrité, la confidentialité et la preuve. Par ailleurs, nous tenons à préciser que plusieurs typologies d'attaques peuvent avoir un impact sur plusieurs piliers de sécurité. A titre d'exemple, une attaque virale peut avoir comme conséquence une atteinte à la disponibilité, à l'intégrité, à la confidentialité ou à la preuve dépendamment de la nature des objectifs visés.

[29] Il est généralement reconnu dans l'industrie logicielle que chaque 1000 ligne de code peuvent générer en moyenne 7 à 8 failles de sécurité.

1. L'ordinateur comme moyen ou cible d'actes cybercriminels

1.1 L'atteinte à la confidentialité

A l'heure du tout informatique, la confidentialité semble être l'un des piliers le plus touché par la cybercriminalité. De nombreuses attaques ont souvent pour but de rechercher des données sensibles au moyen de programmes robots ou autres logiciels malveillants pour les utiliser ou les revendre. Selon *Symantec*[30], 24% des demandes des « clients » des pirates porteraient en effet sur des informations détaillées relatives à des cartes de crédit, et 18% sur des informations relatives à des comptes bancaires[31]. L'accès à ces données ne peut être considéré comme une fin en soi. Ce n'est qu'un objectif transitoire. Les données de cartes de crédit par exemple pourront être utilisées ultérieurement pour commettre des fraudes en ligne, ce qui classera ce délit dans la catégorie des objectifs convertibles.

Le coût des données personnelles dérobées dépend directement du pays où vit le détenteur légitime de ces données. Par exemple, les données complètes de résidents des Etats-Unis valent entre 5 et 8 dollars. Sur le marché noir, les données d'habitants de l'Union européenne sont particulièrement recherchées : elles coûtent deux à trois fois plus que les données de résidents des Etats-Unis et du Canada[32].

L'appât du gain n'est pas le seul but recherché par l'atteinte à la confidentialité des données. L'espionnage industriel voir même politique s'appuie de plus en plus sur les attaques cybercriminelles pour récupérer de l'information confidentielle. Ainsi, mener des intrusions dans le système d'information d'une organisation concurrente dans le but de récupérer de l'information stratégique sur ses produits et services est devenu une pratique courante dans de nombreuses organisations. Sous couvert de l'intelligence économique, tous les moyens sont bons pour gagner plus de parts de marché.

La confidentialité des informations peut être aussi violée physiquement. On néglige souvent la copie physique et la destruction d'informations installées sur un CD ou un dispositif de stockage de type clé *USB*. De nombreuses attaques peuvent s'appuyer sur des techniques

[30] Editeur de logiciels de sécurité

[31] « Symantec Report on the Underground Economy July 07–June 08 » http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008_14525717.en-us.pdf

[32] Yury Namestnikov « Economie des réseaux de PC zombies », Kaspersky Lab http://www.viruslist.com/fr/analysis?pubid=200676201

conventionnelles de récupérations de données stockées sur un support physique électronique ou documentaire. Ainsi, la société *Sunsilk*, filiale de la multinationale *Unilever*, a vu ses poubelles explorées par une société d'intelligence économique qui a été mandatée par son concurrent *Procter & Gamble*. L'opération s'est soldée par la récupération de plus 80 documents dont le plan de lancement de nouveaux produits, la politique des ressources humaines et la stratégie commerciale[33].

Parmi les attaques portant atteinte à la confidentialité, le *Phishing* ainsi que les logiciels malveillants notamment les chevaux de Troie restent les plus utilisés. Appuyées de plus en plus sur un réseau d'ordinateurs zombies[34], ces attaquent génèrent une grande partie d'argent de la cybercriminalité.

1.1.1 L'attaque virale

L'époque des virus infectant des machines pour rendre indisponible un service donné et gêner le travail de l'utilisateur est révolue. Aujourd'hui, l'attaque virale est de plus en plus orientée vers l'appât du gain. Pour y parvenir, les infections dues à ces virus sont dirigées pour rechercher des données sensibles et les envoyer à l'adresse électronique d'un tiers sur ordre du concepteur du virus. Ainsi, une nouvelle génération de virus appelée *malware*[35] ou cheval de troie[36] est née. Au fil du temps, elle est devenue la pierre angulaire de la majorité d'attaques cybercriminelles. Le détenteur d'un tel code malicieux peut récupérer des informations sensibles sur les postes de ses victimes telles que les informations liées à sa carte bancaire, son code d'accès à ses services de banque en ligne, ses identifiants d'accès à d'autres sites privatifs notamment les sites des réseaux sociaux et de la messagerie personnelle. Le caractère multifonctions de ces codes malveillants a d'ailleurs rendu obsolètes les définitions usuelles des notions de « virus », « cheval de troie », « porte

[33] « Panorama de la cybercriminalité », Clusif 2001
http://www.clusif.fr/fr/production/ouvrages/pdf/PanoCrim2k1-fr.pdf

[34] Une machine zombie est un ordinateur contrôlé à l'insu de son utilisateur par un pirate informatique. Ce dernier l'utilise alors le plus souvent à des fins malveillantes, par exemple afin d'attaquer d'autres machines en dissimulant sa véritable identité.

[35] Un logiciel malveillant (malware en anglais) est un logiciel développé dans le but de nuire à un système informatique. Les virus et les vers sont les deux exemples de logiciels malveillants les plus connus.

[36] Un cheval de Troie (ou trojan) est un logiciel d'apparence légitime, mais conçu pour exécuter subrepticement (de façon cachée) des actions à l'insu de l'utilisateur. En général, un cheval de Troie tente d'utiliser les droits appartenant à son environnement pour détourner, diffuser ou détruire des informations, ou encore pour ouvrir une porte dérobée qui permettra à un attaquant de prendre, à distance, le contrôle de l'ordinateur.

dérobée »[37]. Aujourd'hui un malware moderne répond à lui seul à plusieurs de ces définitions.

Le phénomène d'attaques virales perpétrées dans le but de récupérer des données sensibles monnayables semble connaître une croissance phénoménale ces dernières années. Une récente étude menée par *Symantec* confirme cette tendance. Le nombre de virus a progressé de 165% entre 2007 et 2008[38]. Plus de 1,6 million de nouveaux programmes malveillants ont été détectés au cours de la seule année 2008. Depuis sa création, l'éditeur a recensé 2,6 millions de virus. Ceux apparus en 2008 représentent donc 60% de l'ensemble de ces codes malveillants. La tendance à l'explosion du nombre de virus se poursuit donc, et s'accélère comme le montre le graphe suivant.

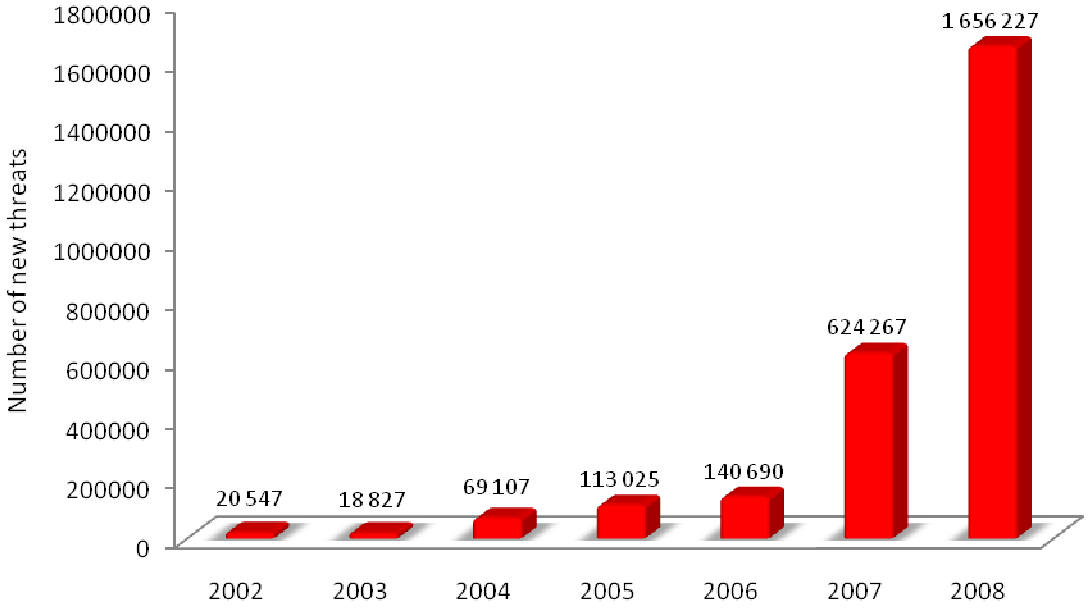

Figure 8 : L'évolution du nombre de virus[39]

Autre les failles des navigateurs et des systèmes d'exploitation, l'attitude de confiance par défaut envers les sites web visités et l'ouverture des pièces jointes reçues d'expéditeurs

[37] Didier Sanz, « Un nouveau terrain d'action : la chasse aux données personnelles », La délinquance électronique, Problèmes économiques et sociaux, Octobre 2008

[38] « Symantec Global Internet Security Threat Report. Trends for 2008 http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

[39] Idem

inconnus sont autant de vecteurs d'infection dans le cyberespace. Selon une étude menée par *Trend Micro* en 2008[40], le téléchargement en direct sur l'internet est de loin le vecteur le plus utilisé (plus de 53%). En deuxième position, on trouve la présence préalable d'un code tiers (43%), les interactions avec des emails frauduleux (12%) prennent la 3éme place, suivi de très près par les infections par périphériques de stockage amovibles (10 %) comme les clés *USB* dont les risques liés aux fonctionnalités d'exécution automatiques ne sont pas nouveaux. Le graphe suivant montre la place occupée par les différents vecteurs d'infection virale.

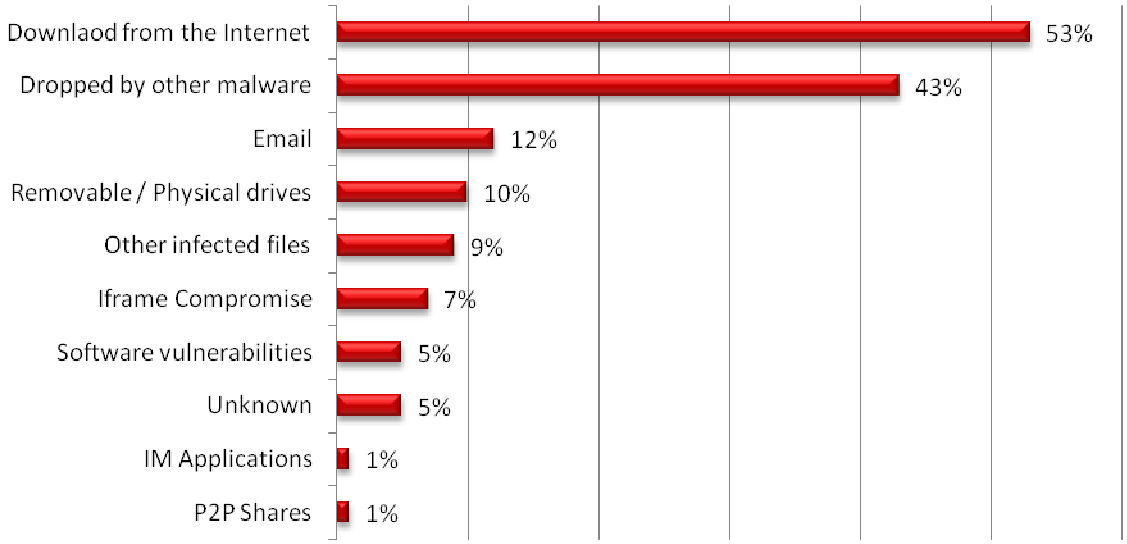

Figure 9 : Les vecteurs d'infection virale[41]

La multiplication des vecteurs d'infection virale et l'ascension fulgurante du nombre de codes malicieux compliquent le travail des éditeurs de logiciels antivirus. Rien qu'en 2007, plus 3.000 souches ont été identifiées en moyenne chaque jour[42]. Rappelons, qu'il est de plus en plus difficile d'obtenir un échantillon de chaque souche virale en circulation. Les mutations incessantes de ces codes malicieux leur assurent un niveau de détection très faible. Il est devenu donc extrêmement difficile aux éditeurs de solutions de sécurité uniquement basées sur les signatures de suivre le rythme. Le processus allant de la détection, à l'analyse et enfin à la diffusion des mises à jour est trop lent. Plusieurs éditeurs commencent à

[40] « Trend Micro 2008 Annual Threat Roundup» http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/trend_micro_2009_annual_threat_roundup.pdf

[41] « Malware Blog », Trend Lab, http://blog.trendmicro.com/most-abused-infection-vector/

[42] « Les malwares atteignent un stade épidémique » http://www.darkreading.com/document.asp?doc_id=143424

développer une approche à plusieurs couches, avec contrôle d'applications, prévention d'intrusion et analyse comportementale. Cette situation incite même certains experts de la sécurité à annoncer la mort de l'antivirus comme le montre l'image suivante :

Figure 10 : 10 ans de lutte antivirale

Prenons l'exemple du virus *Conficker*. Le 16 janvier 2009, l'éditeur de logiciels de sécurité *F-Secure* déclarait que *Conficker* avait infecté presque 9 000 000 ordinateurs, ce qui en ferait une des infections les plus largement répandues des années 2000[43].La propagation du virus se fait par tous les moyens de contamination existants : sites Internet piégés, réseaux *peer-to-peer*, clés *USB*, mails, etc...

Une fois le virus *Conficker* est introduit dans l'ordinateur, il installe discrètement un petit serveur qui lui permet de rester en contact avec le réseau des machines pilotées à distance. Le centre de sécurité Windows Update est aussi désactivé et les points de restauration du système sont supprimés pour interdire à l'utilisateur de rétablir une configuration valide. Ce code malicieux prévient aussi les utilisateurs que leurs ordinateurs sont attaqués par un virus en leur offrant un antivirus fictif intitulé (*spyware Brockt 2009*) à 49,95 dollars et si les utilisateurs l'achètent, le virus récupère les coordonnées de leurs cartes de crédit. Au Maroc, au début du mois de mai 2009 et après avoir changé son mode opératoire, ce virus a infecté plusieurs entreprises privées et organismes publiques. Ainsi, plusieurs grandes structures ont vu leurs systèmes d'informations indisponibles pendant plusieurs heures.

[43] Barry Neild, « *Downadup virus exposes millions of PCs to hijack* », CNN, 16 janvier 2009

1.1.2 Le Phishing

Une attaque de *phishing* classique peut se dérouler comme suit[44] :

- Étape 1. L'hameçonneur envoie à sa victime potentielle un message électronique qui semble en apparence provenir de la banque de cette personne ou d'une autre organisation susceptible de détenir des informations personnelles. Dans cette tromperie, l'hameçonneur reproduit avec soin les couleurs, le graphisme, les logos et le langage d'une entreprise existante.
- Étape 2. La victime potentielle lit le message électronique et mord à l'hameçon en donnant à l'hameçonneur des informations personnelles, soit en répondant au message électronique, soit en cliquant sur un lien et en fournissant l'information au moyen d'un formulaire sur un site web qui a l'apparence de celui de la banque ou de l'organisation en question.
- Étape 3. Par le biais de ce faux site web ou du courrier électronique, les informations personnelles de la victime sont directement transmises aux cybercriminels.

Le succès des attaques *phishing* s'explique largement par le recours à des techniques d'ingénierie sociale, c'est-à-dire à des mises en scène bâties sur des conventions sociales admises en vue de troubler psychologiquement les victimes et de recueillir des informations sensibles[45]. D'après une récente étude présentée par le Groupe *Intrepidus*[46], compte tenu des méthodes de plus en plus personnalisées employées par les hamçonneurs 23% des personnes dans le monde seront vulnérables aux attaques *phishing*. En outre, les attaques *phishing* qui utilisent un ton autoritaire ont 40% plus de succès que ceux qui tentent d'attirer les utilisateurs par le biais de récompenses ou des donations. Tout en continuant à viser les banques et sites de commerce électronique bien connus, les hameçonneurs tentent maintenant d'atteindre des victimes moins nombreuses mais de manière plus personnalisée, ce qui pourrait les rendre encore plus dangereux. Un rapport de McAfee daté de 2006[47] révèle que les fraudeurs abandonnent les messages de type « mettez à jour vos renseignements personnels tout de suite » au profit de messages plus personnalisés. Les

[44] « Document exploratoire sur le vol d'identité en ligne », OCDE 2007

[45] Olivier Iteanu, « L'identité numérique en question », Edition EYROLLES, 2008

[46] La compagnie derrière le site web http://www.phishme.com qu'est un service de sensibilisation aux enjeux de *phishing*

[47] McAfee Virtual Criminology Report, 2006
http://www.mcafee.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf

techniques d'hameçonnage sont de plus en plus perfectionnées et difficiles à détecter. Les formes principales sont les suivantes :

- Le « *pharming* » : ce type de message utilise le même genre de faux identifiants que dans une attaque d'hameçonnage classique et, en même temps, redirige les utilisateurs d'un site web authentique vers un site frauduleux qui reproduit l'apparence de l'original.
- Le « *smishing* » : l'utilisateur d'un téléphone mobile reçoit un message (« *SMS* ») en vertu duquel une entreprise confirme son abonnement à l'un de ses services, indiquant qu'une certaine somme lui sera facturée quotidiennement s'il n'annule pas sa commande sur le site web de cette entreprise.
- Le « *spear-phishing* » (« harponnage ») : l'expéditeur se fait passer pour un collègue ou employeur du destinataire dans le but de saisir les mots de passe et noms d'utilisateur de membres du personnel pour finalement accéder au système informatique de l'entreprise.

Selon une étude réalisée par *The Radicati Group*, le nombre d'attaques par *phishing* aura plus que doublé en 2008[48]. Cela corrobore la tendance identifiée par *Symantec* qui signalait que l'activité de *phishing* est en hausse de 66% par rapport à 2007. Ces attaques visaient essentiellement les acteurs du secteur des services financiers. De même, 12 % de tous les vols de données constatés en 2008 concernaient les numéros de carte de crédit[49]. Cette forte croissance s'explique notamment par l'utilisation des réseaux zombies qui facilitent l'utilisation de la technologie *Fast-flux* permettant ainsi de modifier à intervalle de quelques minutes l'adresse IP des sites tout en conservant le nom de domaine, ce qui prolonge la durée de vie de ces réseaux et complique leur découverte et leur mise hors-service[50].

Tout comme pour le cas d'une attaque virale à base de code malicieux, une attaque *phishing* n'est pas une fin en soi, elle n'est qu'une étape intermédiaire pour se livrer à diverses fins telles que l'obtention d'un crédit, de l'argent, des biens, des services, ou toute autre chose de valeur utilisée sous le nom de la victime sans son consentement. Parfois, les voleurs d'identité n'utilisent pas eux-mêmes l'identité de la victime pour commettre une fraude. Ils la vendent à d'autres parties qui commettront elles-mêmes la fraude ou généreront de nouvelles formes illégales d'identité personnelle (comme un certificat de naissance, un permis de conduire ou un passeport). D'après une enquête auprès de victimes menée par

[48] http://www.radicati.com/

[49] « Symantec Global Internet Security Threat Report ». Trends for 2008

[50] « Les réseaux de PC zombies rapportent des millions de dollars aux cybercriminels », Kaspersky Lab http://www.kaspersky.com/fr/news?id=207217176

l'Identity Theft Resource Centre (ITRC) aux Etats-Unis en 2006, les actes de vol d'identité sont classés en trois grandes catégories :

- L'ouverture de nouveaux comptes (cartes de crédit, comptes bancaires ou emprunts) et autres types de fraude (par exemple, bénéficier de soins médicaux) ;
- L'utilisation illicite de comptes sans carte de crédit ;
- L'utilisation illicite de cartes de crédit seulement.

Naturellement, les banques restent la cible idéale à ce genre d'attaques. La croissance des activités de banque en ligne ne peut qu'accélérer ce phénomène. Selon les chiffres publiés en 2008 par *l'Anti-phishing Working Group*[51] *(APWG),* la majorité des entreprises ciblées par le *phishing* appartiennent au domaine de la banque et de la finance. Parmi elles, sept marques (non citées dans le rapport) occupent à elles seules 80% des campagnes de *phishing*. On imagine sans peine qu'il s'agit des grandes banques américaines et européennes et de quelques services en ligne tels *PayPal* ou *eBay*. Mais, elles ne sont pas les seules touchées par le *phishing*. En 2007, il suffisait à un internaute marocain de commettre une légère faute de frappe sur le site web institutionnel de Attijariwafa bank (www.atijariwafabank.com au lieu de www.attijariwafabank.com) pour se retrouver sur un vrai-faux site web du premier groupe financier marocain. Derrière cette opération, il y avait un jeune informaticien sans antécédents judiciaires. Au début, son but était d'acheter des noms de domaines qui prêtent à confusion avec celui d'attijariwafa bank et de les revendre après pour réaliser une plus value. C'est de la pure spéculation. Cependant, après avoir envoyé plusieurs courriels à Attijariwafa bank sous couvert du pseudonyme « Mol Mol », il s'est rendu compte de l'inefficacité de son plan d'attaque. Le jeune informaticien ira dans un deuxième temps jusqu'à cloner le site d'attijariwafa bank et l'héberger sur le site qu'il avait acheté sous le nom de domaine www.atijarwafabank.com. Cette opération lui a valu une amende de 600 000 DH pour la partie civile[52].

Le secteur financier marocain n'est pas le seul à être victime d'attaque de *phishing*, les opérateurs télécoms, ont subi aussi plusieurs attaques de ce type. Ainsi, Meditel a découvert en 2007 qu'une tentative de piratage visait ses clients utilisant les cartes téléphoniques pré payées. La technique consistait à envoyer un courriel qui propose d'acheter par cartes bancaires des recharges Meditel à travers le faux site web http://meditel.medi-recharge.ma (site web cloné à partir du site web institutionnel http://www.meditel.ma).

[51] http://www.antiphishing.org

[52] http://www.bladi.net/attijariwafa-piratage-internet.html

1.2 L'atteinte à la disponibilité

Les organisations sont de plus en plus dépendantes de leurs systèmes d'information. L'indisponibilité peut avoir un impact important sur le chiffre d'affaires et sur l'image de marque de l'organisation. Par exemple, l'indisponibilité d'un lien pour un opérateur télécom pendant quelques minutes peut se chiffrer en millions de dirhams. C'est la raison pour laquelle, tous les moyens sont envisageables pour rétablir la situation. Quitte même à payer une rançon à une organisation cybercriminelle en contre partie d'un retour à la normale.

L'atteinte à la disponibilité peut se faire de diverses façons. Du piratage jusqu'au recours aux logiciels malveillants en passant par les attaques de dénis de service, aujourd'hui les attaques sont orientées vers l'appât du gain. Finie donc l'époque où on lançait des attaques contre des géants d'industries informatiques, juste pour manifester son désaccord idéologique ou pour avoir plus de renommée dans l'univers *Underground.*

La disponibilité peut aussi être atteinte suite à des attaques physiques, ne requérant que peu de technologies, sur les installations informatiques ou le câblage des réseaux. Mais la forme d'attaque la plus dangereuse et la plus répandue dans l'univers *Underground* reste incontestablement l'attaque *DDoS*.

1.2.1 Le DoS et le DDoS

Les attaques en Dénis de Service *(DoS)* ont pour objectif de consommer tout ou partie des ressources d'une cible, afin de l'empêcher de pouvoir rendre ses services de façon satisfaisante. En effet, les routeurs qui ont la charge de fluidifier et de rationnaliser le trafic *IP* [53]ne peuvent quelques fois plus supporter une telle masse de requêtes. Par conséquent, ils sont submergés et ne peuvent assurer le trafic non seulement sur le site attaqué mais également sur les sites qui lui sont connectés[54]. C'est un effet boule de neige assuré. Les premiers types d'attaques en Dénis de Service ne mettaient en cause qu'un seul attaquant *(DoS)*, mais rapidement, des attaques évoluées *(DDoS)* sont apparues, impliquant une multitude d'ordinateurs « zombies ».

[53] Internet Protocol

[54] Franck Franchin et Rodolphe Monnet, « Le business de la cybercriminalité », Edition LAVOISIER, 2005

S'il y a quelques années, les opérations *DDoS* étaient assez compliquées et nécessitaient des connaissances pointues en informatique, aujourd'hui elles se sont démocratisées. De nombreux outils ont été développés pour rendre l'attaque plus accessible. Il en résulte une recrudescence des attaques par dénis de service. Selon *Verisign*[55], elles croissent plus rapidement que la bande passante allouée à l'internet[56]. Ainsi plus de 190 000 attaques par déni de service distribué ont été organisées en 2008, ce qui aurait rapporté aux cybercriminels plus de 20 millions de dollars[57].

Pour mieux comprendre le phénomène, il s'avère important d'étudier les techniques les plus utilisées dans ce domaine, qui doivent leur notoriété à des célèbres attaques ayant visées des sites web d'entreprises de renom. Le tableau ci-dessous résume les techniques de dénis de services les plus utilisées.

Techniques d'attaques	Description
SYN flood	Cette attaque consiste à envoyer une multitude de demandes de connexions TCP afin de monopoliser les ressources d'un serveur. Une connexion TCP normale s'établit ainsi : 1) Demande de connexion au serveur en envoyant un message SYN (*synchronize*) 2) Le serveur accepte la connexion au client en envoyant un message SYN-ACK (*synchronize acknowledgment*) 3) Le client répond en envoyant un message ACK (*acknowledgment*) pour établir la connexion. 4) Le pirate ne renvoie pas le message ACK, une latence du serveur ainsi qu'une consommation excessive des ressources-serveur se fait alors sentir et entraîne un déni de service.
UDP flood	L'UDP flood consiste en une multitude de requêtes UDP envoyées sur un serveur (les paquets UDP sont prioritaires sur les paquets TCP) afin de saturer celui-ci.
Packet Fragment (attaque par fragmentation)	Le pirate va s'attaquer à la fragmentation de la pile TCP/IP en plaçant des informations de décalage (*offsets*) erronées empêchant le réassemblage des paquets (*overlapping*).
Ping of Death (Ping de la Mort)	Le Ping of Deatth consiste à envoyer un ping supérieur à 65535 octets (taille maximale) provoquant un *crash* système.

[55] Firme en charge notamment de gérer les noms de domaines en .com

[56] http://www.generation-nt.com/commenter/attaque-dos-internet-verisign-deni-service-actualite-45530.html

[57] Yury Namestnikov « Economie des réseaux de PC zombies », Kaspersky Lab http://www.viruslist.com/fr/analysis?pubid=200676201

Techniques d'attaques	Description
Smurf attack (attaque par réflexion)	Le smurf repose sur l'envoi d'un maximum de ping (protocole ICMP) à un réseau en broadcast. La cible se fera alors inondée de « réponses ping » par l'ensemble des machines du réseau saturant complètement sa bande passante.
Land Attack	Le pirate envoie des paquets ayant la même adresse IP (et port) au niveau de son adresse source et de son adresse destination. De plus, cette technique utilise le flag SYN armé (voire SYN flood).
Buffer overflow (débordement ou dépassement de tampon)	Le buffer overflow consiste à envoyer plus de données qu'un programme est capable d'en gérer. Les instructions en attente d'exécution sont stockées dans un buffer (pile ou stack). Si la taille des données est supérieure à la capacité du buffer, l'application renverra une erreur : une adresse de retour invalide. Le pirate remplace l'adresse écrasée par une autre pointant vers un code arbitraire (injection de code lui permettant par exemple d'ouvrir un terminal : shellcode) pour prendre le contrôle de l'ordinateur-cible.
Mail Bombing	Cette attaque permet l'envoi massif d'e-mails à un destinataire pour saturer le serveur mail.

Tableau 1: Les techniques d'attaques par Déni de Service

En terme de popularité des attaques par saturation, celles visant les applicatifs (serveurs web, bases de données *SQL* par exemple) et celles par saturation des ports utilisés pour les services (*UDP*, *ICMP* par exemple) restent les plus populaires[58].

De nos jours, le moyen le plus couramment utilisé pour lancer des attaques par dénis de services est l'utilisation des réseaux de zombies. Si on prend comme hypothèse que chacun de ces zombies a accès à une bande passante typique de l'ADSL, la victime doit faire face à une attaque forte de plusieurs dizaines de Gigabits par seconde, répartie en termes de provenance sur l'internet mondial. Selon un rapport publié en Novembre 2008 par Arbor Networks[59], les attaques *DDoS* ont franchi durant l'année 2008 la barrière des 40 gigabits par seconde soit 64% de l'échelle des attaques par rapport à l'année 2007. Peu d'organisations peuvent y faire face.

[58] http://www.zdnet.fr/actualites/informatique/0,39040745,39384798,00.htm

[59] « 2008 Worldwide Infrastructure Security Report », Arbor Networks http://www.arbornetworks.com/report

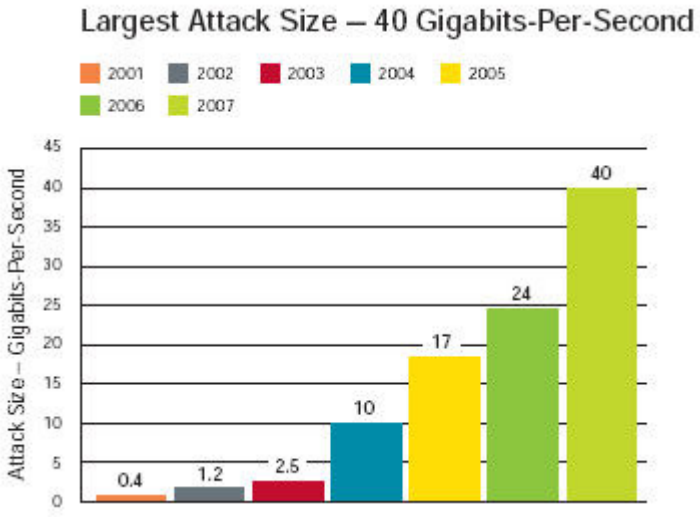

Figure 11 : L'évolution des attaques *DDoS*[60]

Si à l'origine des géants comme *Microsoft, Cisco, eBay, Facebook, Google, Twitter*[61] et même les serveurs racines de noms de domaines[62] (le cœur du réseau de l'internet) ont fait l'objet d'attaques par déni de services, ce n'était absolument pas dans le but de leur demander une rançon. Cibler de telles organisations revenait tout simplement à se faire une place de renommée dans l'univers *Underground*. Aujourd'hui, de telles motivations se font de plus en plus rares. Le véritable but recherché est désormais l'appât du gain. En effet, avec la forte augmentation du nombre d'échanges commerciaux sur l'internet, le nombre de chantages au déni de service est lui aussi en très forte progression. Toute entreprise réalisant un chiffre d'affaire important dans une activité en ligne à fort effet de levier, est potentiellement vulnérable aux attaques par dénis de service. Il est évident que le ralentissement, voir même le blocage de leurs services pendant quelques heures est synonyme de pertes substantielles et pourrait occasionner beaucoup de désagréments pour leurs clients. Ces sociétés ont donc tout intérêt à obéir ou à trouver une parade pour s'en protéger, sans quoi les menaces seraient mises à exécution et pourraient perdurer[63]. Voici quelques exemples d'attaques par dénis de service perpétrées ces dernières années.

- ✓ Mars 2003 : Le site web de la chaîne d'information Al Jazzera a été l'objet d'attaque par dénis de service. La page d'accueil du site a été remplacée par un logo représentant une bannière étoilée accompagnée de l'inscription. « *let freedom Ring* ». Replacée dans son contexte, cette attaque s'est inscrite dans le sillage de la

[60] Idem

[61] http://www.itespresso.fr/attaque-dos-twitter-facebook-et-google-pris-pour-cible-30841.html

[62] http://www.cases.public.lu/fr/actualites/actualites/2007/02/06_internet/index.html

[63] La revue MISC, « Dossier spécial cybercriminalité ». Janvier 2009.

seconde guerre du golf, où la diffusion par cette télévision d'images de soldats de la coalition morts avait choqué l'opinion publique américaine.

- ✓ Juillet 2004 : La police russe a arrêté des personnes soupçonnées d'avoir organisé un racket de sites britanniques d'entreprises et de paris. Elle a par ailleurs, indiqué que ce gang avait lancé des dizaines d'attaques contre des sites Web. Il a fallu une collaboration active et poussée entre les polices russes et britanniques pour aboutir à une telle arrestation.
- ✓ Juillet 2004 : La société *DoubleClick* a vu le trafic sur son site web fortement paralysé pendant de longues heures, entraînant dans son infortune les sites de ses clients, qui dépendent de sa technologie pour gérer leurs bannières de publicité.
- ✓ Septembre 2008 : La cour de *Balakov* a condamné trois pirates informatiques à 8 ans de prison suite à un chantage envers des sites de jeux en ligne. Les internautes demandaient plusieurs dizaines de milliers de dollars pour ne pas faire subir aux sites des attaques par dénis de service distribué.
- ✓ Août 2009 : *Twitter, Facebook* et *Google* ont subi une attaque par déni de service. Une opération unique, massive et coordonnée selon *Twitter*. Un bloggeur géorgien serait la cible des pirates qui ont paralysé ces trois sites. Il utilise *LiveJournal*, *Facebook, YouTube* et *Twitter* pour militer sur le web en faveur de la Géorgie. Un militantisme qui n'aurait pas plu à des "activistes" russes et qui auraient décidé de bloquer ses comptes (*blogs, Twitter et Facebook*). Seule façon d'y parvenir : envoyer un grand nombre de messages vers ces sites pour les bloquer.
- ✓ Août 2009 : Le site de la loterie nationale danoise a subi une attaque par déni de service. Le communiqué de presse officiel mentionne en effet 10 millions de tentatives d'ouvertures de session pour le samedi 15 août. Le serveur de *Command & Control* (C&C) du *botnet* à l'origine de cette attaque est opéré, sans grande surprise, sur un nom de domaine russe, lui-même hébergé sur un serveur localisé à Taiwan.

Les entreprises privées ne sont pas les seules organisations ciblées par les attaques par déni de service, les Etats à travers notamment ses institutions publiques peuvent aussi faire l'objet de ces attaques. En Juillet 2009, une série de sites gouvernementaux américains et sud-coréens ont quasi-simultanément été ciblés par une attaque de déni de service. Cette attaque massive visait à les rendre inaccessibles, et de fait, les sites des départements du Trésor, des Transports, de la Commission fédérale des Echanges (*FTC)*, du Secret Service et de plusieurs autres départements fédéraux étaient inaccessibles pendant plusieurs heures. En Corée du Sud, des cibles similaires ont été attaquées, telles que les sites de la Présidence

sud-coréenne, des ministères de la Défense et des Affaires Etrangères, et de l'Assemblée Nationale. En France, l'attaque par déni de service est considérée comme le deuxième risque pour le pays derrière le terrorisme[64].

L'attaque contre l'Estonie

Tout a commencé par une action symbolique, l'enlèvement dans un jardin public de Tallin (capitale de l'Estonie), d'un mémorial de guerre datant de la période soviétique. Pour l'Estonie, c'était une façon d'affirmer un peu plus la jeune indépendance du pays face au grand voisin russe. Mais à Moscou, certains y ont vu au mieux une provocation, au pire un outrage. Et la réplique fut terrible.

En quelques heures, ce pays, qui compte parmi les plus connectés d'Europe, fut l'objet d'une série d'attaques par déni de service distribué sans précédent à l'échelle d'un pays. Les sites gouvernementaux furent les premiers visés. Puis vint le tour des banques, des médias et des partis politiques. Le numéro des urgences (ambulances, incendies) est même resté indisponible pendant plus d'une heure.

Les attaques *DDoS* furent si virulentes que certaines administrations, dont celles de la défense nationale, ont été obligées de couper l'accès de leur site web à toutes les IP étrangères au pays pendant plusieurs jours.

La densité des requêtes était telle que les experts ont enregistré une création de trafic allant jusqu'à 5 000 clics par seconde sur certains sites ciblés[65].

1.3 L'atteinte à l'intégrité

L'atteinte à l'intégrité est rarement l'objet d'attaque cybercriminelle ayant pour but l'appât du gain. La modification non autorisée ou l'altération de données ne peuvent être exploitées dans une perspective directement liée à l'argent. Cependant, comme cela a déjà était le cas, des organisations peuvent recourir aux services de cybercriminels afin d'altérer les données

[64] « Le livre blanc sur la défense et la sécurité nationale en France ».
http://lesrapports.ladocumentationfrancaise.fr/BRP/084000341/0000.pdf

[65] http://www.01net.com/editorial/350759/lestonie-denonce-les-cyber-attaques-terroristes-russes/

d'une organisation cible. Il s'agit notamment d'attaques ayant pour objet de nuire à l'image de marque d'une entreprise concurrente ou d'une organisation « ennemie ». Le défacement des sites web reste la meilleure manifestation de ce genre d'attaques. Il s'agit d'attaques provoquées par l'utilisation de failles présentes sur une page Web ou tout simplement une faille du système d'exploitation du serveur Web. La plupart du temps, les sites défacés le sont uniquement sur la page d'accueil.

1.3.1 Défacement des sites web

Un défacement, défaçage ou défiguration (defacing en anglais) est un anglicisme désignant la modification non sollicitée de la présentation d'un site Web, suite au piratage de ce site. Il s'agit donc d'une forme de détournement de site Web par un pirate[66].

Une page défacée peut contenir plusieurs éléments :

- ✓ Un fond uni, qui peut être le seul indice de défacement d'un site; la plupart du temps la page d'accueil est blanche ou noire ;
- ✓ Un simple mot, comme *owned*, *hacked* ou bien le pseudonyme du défaceur ;
- ✓ Une image est assez souvent présente, et affiche les revendications du défaceur. On trouve souvent des symboles se référant à la mort (crânes…), un drapeau sous lequel le défaceur est fier d'agir etc ;
- ✓ Parfois plus qu'un simple mot, plusieurs phrases, pouvant être de différente nature (insultes envers des états, des défaceurs adverses; une revendication spécifique…) ;
- ✓ Une explication simple de la façon dont le défaceur a acquit l'accès en écriture sur le site, accompagnée à l'occasion d'une moquerie envers le webmestre ou l'administrateur du site en question ;
- ✓ Plus rarement un fichier audio.

Au Maroc, l'ampleur du phénomène de défacement des sites web est arrivée à un point tel que certains analystes avancent que les sites marocains constituent un terrain d'entraînement pour les pirates étrangers[67]. Notons par ailleurs, que le défacement des sites web est un acte identitaire à presque tous les pays en voie de développement. Les statistiques de Zone-H[68] donnent une idée précise sur l'origine des assaillants (turcs,

[66] http://fr.wikipedia.org/wiki/D%C3%A9facement

[67] http://www.1stpaca.com/actualites-paca/actualite.php?debut=96&idactu=569

[68] http://www.zone-h.org/

iraniens, tunisiens, algériens, saoudiens et marocains).

Le tableau ci-dessous représente une liste non exhaustive des sites web institutionnels des organismes gouvernementaux ayant fait l'objet d'un défacement[69].

Date	Attaquant	Domaine	Système
2009/05/28	Dr.Anach	www.marocainsdumonde.gov.ma/im...	Linux
2009/04/27	Hmei7	www.habous.gov.ma/sidishiker/i...	Win 2003
2009/01/08	GANG hackers ARABS	Docs.justice.gov.ma/ang.txt	Win 2003
2008/11/21	Old.Zone	www.equipementransport.gov.ma/...	Win 2003
2008/11/20	Old.Zone	www.mtpnet.gov.ma/index.htm	Win 2003
2008/09/23	ExSploiters	www.lagencedusud.gov.ma	Win 2003
2008/09/16	NetKiller	www.affaires-generales.gov.ma/...	Win 2000
2008/08/17	mor0ccan nightmares	agadir-indh.gov.ma	Linux
2008/08/17	mor0ccan nightmares	www.essaouira-indh.gov.ma	Linux
2008/08/04	Sm4rT Security Cr3w	www.dapr.gov.ma	Linux
2008/08/02	Handrix	www.invest.gov.ma/all4one.htm	Win 2003
2008/06/30	Mafia Hacking Team	www.environnement.gov.ma/feedd...	Win 2000
2008/06/28	Mafia Hacking Team	www.minenv.gov.ma/feedd/defaul...	Win 2000
2008/05/29	Swan	Marocurba.gov.ma/du/forum/down...	Win 2000
2007/12/09	Fox Team	www.social.gov.ma/fr/index.asp	Win 2003
2007/10/08	United Arab Hackers	www.marocainsdumonde.gov.ma/fo...	Win 2003
2007/05/01	Arabian-FighterZ	www.mce.gov.ma/index.html	Win 2003
2006/06/11	Arabian-FighterZ	www.minculture.gov.ma/owned.html	Win 2003
2005/10/24	WizardZ	asl.minculture.gov.ma/r0v.htm	Win 2000
2005/10/14	WizardZ	www.minculture.gov.ma/r0v.htm	Win 2000
2005/06/05	Arabian-FighterZ	www.septi.gov.ma/livreor/defau...	Win 2003
2005/05/13	PRI[ll	www.septi.gov.ma/livreor/defau...	Win 2003
2005/01/18	Fatal Error	www.mhu.gov.ma	Win 2000

Tableau 2 : Liste de sites web marocains défacés[70]

Le phénomène de défacement des sites web gouvernementaux a atteint un niveau insupportable en 2010[71]. En effet, après plusieurs attaques contre les sites de la primature, du ministère de l'énergie et de la justice, la cellule de la lutte contre la cybercriminalité de la Sûreté Nationale a multiplié les coups de filet. Plusieurs groupes ont été arrêtés. Il s'agit notamment du groupe de pirates baptisé « Team Rabat-Salé » connu dans l'univers

[69] http://www.zone-h.org/archive/filter=1/domain=gov.ma/page=1

[70] Source : http://www.zone-h.org

[71] Voir les articles publiés par Hamza HAROUCHI à ce sujet sur son blog http://www.hamza.ma

Underground marocain pour ses attaques dirigés contre les sites israéliens et ceux du Polisario.

1.4 L'atteinte à la preuve

La preuve, en tant que pilier de la sécurité, reste le caractère le moins touché par la cybercriminalité. En effet, l'atteinte à la traçabilité notamment des événements de sécurité est rarement monnayable. Cependant, le recours vers les techniques permettant de porter atteinte à la couche de traçabilité, notamment lors des intrusions dans les SI, est de plus en plus fréquent. En effet, lors d'une attaque, l'information contenue dans les fichiers logs peut être vérifiée pour définir les traces de l'attaque et aboutir à une preuve accusatrice. Les informations pertinentes contenues dans les fichiers logs représentent la preuve qui est le besoin indispensable pour l'investigation. C'est le seul moyen pour identifier l'attaquant afin de le poursuivre judiciairement[72]. Un attaquant qualifié pénétrant dans un système a intérêt donc à effacer les fichiers logs ou à modifier leur contenu.

1.4.1 L'atteinte logique

Les données faisant objet de preuve informatique sont générées par le *logging*. Il s'agit des fichiers logs qui tracent tous les événements qui arrivent pendant l'activité d'un système. Ils peuvent contenir la preuve en détail de toute activité exceptionnelle, suspecte ou non désirée.

Les fichiers logs constituent une source critique de preuve pour *Forensics*, ils peuvent contenir les empreintes des attaquants et indiquer les menaces et les attaques en cours. Ils représentent une forme de données qui peut-être effacée ou falsifiée par un attaquant afin d'effacer la trace de l'attaque ou modifier le cours de l'attaque. Si les fichiers logs sont effacés ou erronés, on perd toute preuve d'attaque et par conséquent le processus de *Forenscis* ne peut réussir. Des mesures de protection doivent être prises en compte vis à vis des fichiers logs. La politique de sécurité d'une organisation doit inclure les procédures de protection des fichiers logs des composants du SI[73].

1.4.2 L'atteinte physique

[72] Hassina Bensefia, « Fichiers logs : preuves judiciaires et composant vital pour Forensics » http://www.webreview.dz/IMG/pdf/bensefia.pdf

[73] Idem

La preuve informatique, peut aussi faire l'objet d'une atteinte physique. C'est le cas par exemple de la destruction des documents par le management de la société *Enron*[74] dans le cadre du scandale financier qui a vu le jour en 2001.

C'est le cas aussi de la société *Intel* qui a perdu de nombreux courriers électroniques que la société devait produire devant le juge, dans le cadre de l'affaire de comportement anticoncurrentiel dont l'a accusé son concurrent *AMD* aux Etats-Unis. Selon les avocats *d'Intel*, ces courriers sont perdus, alors qu'ils devaient être conservés pour le procès. Ces documents, la plupart des emails internes de chez Intel, étaient considérés par *AMD* comme des preuves à conviction indispensables[75].

1.5 Les outils utilisés

Chaque opération cybercriminelle s'appuie inévitablement sur l'utilisation des programmes malveillants. L'efficacité de ces outils dépendra de leurs capacités à dissimuler les traces et à éviter au cybercriminel qu'on remonte jusqu'à lui. Parmi ces outils, nous citons notamment les *botnets, les rootkits* et *les keylogger*.

1.5.1 Le Botnet

Un *botnet* est un réseau d'ordinateurs zombies contrôlés à l'insu de leurs propriétaires. Il est souvent utilisé à des fins malveillantes comme envoyer des *spams* et lancer des attaques de type *DoS* contre des entreprises, administrations ou même contre un pays[76]. Les réseaux zombies, qui rassemblent aujourd'hui plusieurs dizaines de millions d'ordinateurs de par le monde[77], peuvent également être utilisés pour commettre des délits comme le vol de données bancaires et identitaires à grande échelle. Ils sont devenus la principale source de propagation du courrier indésirable, des attaques *DDoS* et de diffusion de nouveaux virus[78].

---

[74] Enron fut l'une des plus grandes entreprises américaines par sa capitalisation boursière. Outre ses activités propres dans le gaz naturel, cette société texane avait monté un système de courtage par lequel elle achetait et revendait de l'électricité, notamment au réseau des distributeurs de courant de l'État de Californie. En décembre 2001, elle fit faillite en raison des pertes occasionnées par ses opérations spéculatives sur le marché de l'électricité ; elles avaient été maquillées en bénéfices via des manipulations comptables. Cette faillite entraîna dans son sillage celle d'Arthur Andersen, qui auditait les comptes d'Enron. Source : Wikipédia

[75] http://www.pcinpact.com/actu/news/35071-AMD-Intel-antirust-destruction-preuve.htm

[76] Voir plus haut l'attaque contre l'Estonie

[77] « Votre ordinateur est-il devenu un zombie ? », Orange http://assistance.orange.fr/1185.php?dub=2&

[78] « Baromètre annuel sur la cybercriminalité en 2008 : lutte pour la survie », Kaspersky Lab http://www.kaspersky.com/fr/reading_room?chapter=200463550

Certains experts redoutent même l'utilisation du temps de calcul de ces réseaux d'ordinateurs pour casser des clés de cryptage utilisées pour sécuriser certains protocoles sensibles.

La création d'un *Botnet* se fait en deux étapes au minimum, la première étant d'infecter quelques dizaines de PC (les Maîtres), qui à leur tour se chargeront de corrompre plusieurs dizaines de milliers, voire millions, d'autres ordinateurs (les zombies). Ce processus permet au pirate de conserver un anonymat absolu, plus il y a de machines entre la victime et l'instigateur de l'attaque, plus il est difficile de retrouver sa trace[79].

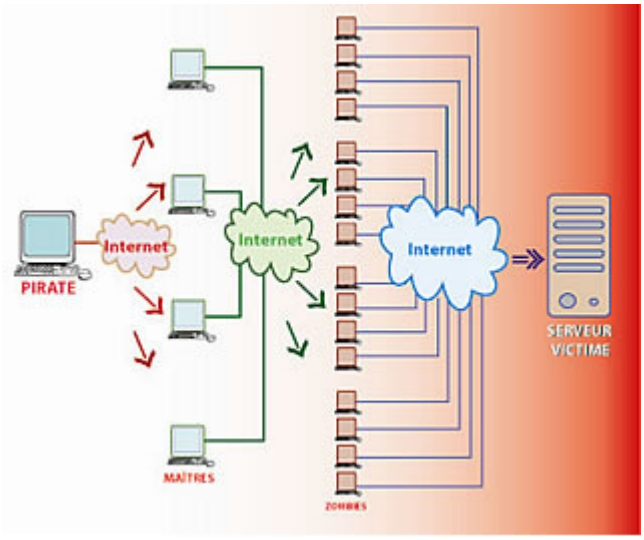

Figure 12 : La structure d'un Botnet[80]

Ce schéma illustre l'effet démultiplicateur dont dispose un *botnet*. Au cours du deuxième trimestre de 2009, près de 14 millions de nouveaux ordinateurs zombies ont été détectés. Cela représente une augmentation de plus de 150 000 nouveaux zombies chaque jour[81]. Cette hausse est en bonne partie attribuable, selon les experts de *Shadowserver*[82], au nombre de plus en plus élevé de sites web contenant des composantes malicieuses. Elle laisse présager dans les années à venir une croissance spectaculaire des revenus générés par les différentes activités cybercriminelles afférentes aux réseaux zombies. Rappelons par

[79] Laurence Ifrah « l'Europe face à la criminalité informatique », Questions d'Europe N°70, 3 septembre 2007 http://www.robert-schuman.eu/question_europe.php?num=qe-70

[80] Idem

[81] Rapport de l'éditeur McAfee sur le paysage des menaces, 2éme trimestre 2009 http://www.3dcommunication.fr/pdf/Threat%20report%20Q2%202009.pdf

[82] http://www.shadowserver.org

ailleurs, que ces revenus sont directement proportionnels à la fiabilité des réseaux zombies et à son rythme de croissance[83].

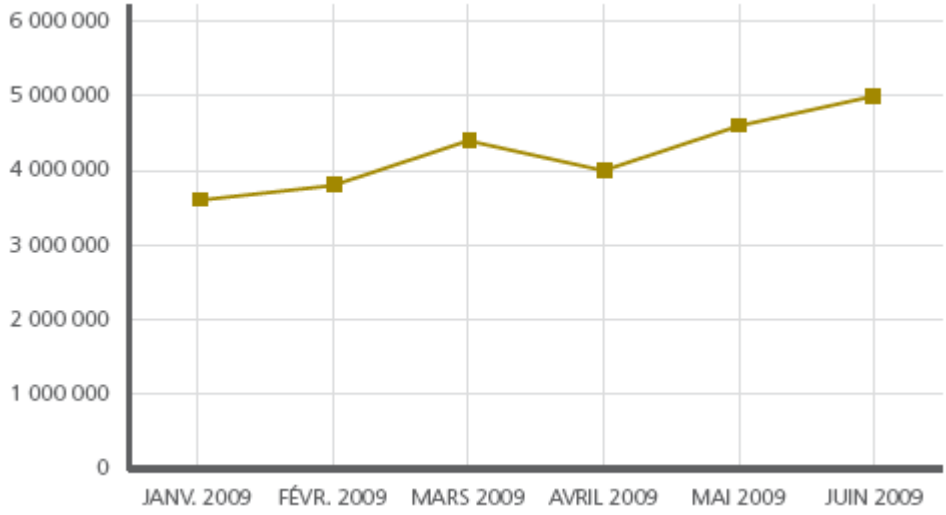

Figure 13 : L'évolution du nombre de PC zombies durant le 1er semestre 2009[84]

Les *botnets* sont considérés même par certains analystes comme un phénomène géopolitique. Il est important donc, d'examiner la production des ordinateurs zombies par pays. Cette production peut être évaluée à partir de la provenance des pourriels détectés[85]. A eux seuls, les Etats-Unis sont responsables d'environ 2,1 millions de nouveaux zombies durant le deuxième trimestre de 2009. Soit une augmentation de 33 % par rapport au premier trimestre de la même année, passant ainsi devant la Chine. Le Brésil, la Russie et l'Allemagne sont respectivement en troisième, quatrième et cinquième positions du classement.

2ème trimestre 2009	
Pays	%
Etats-Unis	15,7

[83] Yury Namestnikov « Économie des réseaux de PC zombies », Kaspersky Lab http://www.kaspersky.com/fr/reading_room?chapter=200463607

[84] Rapport de l'éditeur McAfee sur le paysage des menaces : 2éme trimestre 2009 http://www.3dcommunication.fr/pdf/Threat%20report%20Q2%202009.pdf

[85] Le nombre de pourriels en provenance d'un pays par rapport à la quantité globale de pourriels détectés donne une indication du nombre de machines zombies d'un pays par rapport à l'ensemble des machines connectées sur le réseau.

Chine	9,3
Brésil	8,2
Russie	5,6
Allemagne	5,3
Italie	4,0
République de Corée	3,8
Inde	3,2
Royaume Uni	3,0
Espagne	2,6
TOTAL	**60,7**

Figure 14 : Les principaux pays responsables de la création des zombies[86]

Qualifiés d'armées de zombies par les analystes du domaine, les *botnets* offrent à ceux qui les contrôlent une force de frappe inégalée. Ils sont à la base d'une économie sous terraine en pleine croissance. En effet, grâce notamment aux attaques par déni de service distribué, à la collecte d'informations confidentielles, à la diffusion de courrier indésirable, *au phishing*, et au téléchargement de logiciels publicitaires et d'applications malveillantes, les *botnets* assurent des gains importants à ceux qui les commandent[87]. Ainsi, certains cyberdélinquants se sont spécialisés dans la « levée » d'armées de « zombies », qu'ils peuvent ensuite louer à des tiers peu scrupuleux. La création de réseaux de zombies en vue de les vendre ou de le louer est une pratique qui est devenue courante dans l'univers *Underground.* Le prix d'un *botnet* varie entre 5 et 1 000 dollars américains en fonction de la diffusion du bot, de sa détection par les logiciels antivirus, des instructions qu'il prend en charge, etc[88].

Ce sont les spammeurs qui apprécient le plus les réseaux zombies en raison notamment de la vitesse et l'ampleur de la diffusion que procurent ces réseaux. Ils leur permettent d'envoyer des millions de messages en très peu de temps. En 2008, le top 11 des *botnets*

[86] « Rapport de l'éditeur McAfee sur le paysage des menaces : 2éme trimestre 2009 »
http://www.3dcommunication.fr/pdf/Threat%20report%20Q2%202009.pdf

[87] « Les réseaux de PC zombies rapportent des millions de dollars aux cybercriminels », Kaspersky Lab
http://www.kaspersky.com/fr/news?id=207217176

[88] Idem

était capable d'envoyer plus de 100 milliards de messages *spam* chaque jour dans le monde[89]. En 2008, les spammeurs ont empoché environ 780 millions de dollars[90].

Figure 15 : L'ampleur du phénomène du SPAM

Compte tenu du caractère rentable des activités cybercriminelles liées à l'utilisation des *botnets*, il faut s'attendre à ce que les cybercriminels accélèrent le processus de développement des technologies propres aux réseaux de zombies. Ces derniers resteront donc, l'un des principaux problèmes de délinquance électronique auquel devra faire face les organisations et les Etats dans les années à venir. Seule une collaboration étroite entre les éditeurs de logiciels antiviraux, les fournisseurs d'accès Internet et les autorités judiciaires est de nature à freiner le développement rapide des *botnets*.

1.5.2 Le Keylogger

Un *keylogger* (en français, enregistreur de frappe) est un logiciel[91] ou un matériel[92] qui enregistre les frappes clavier à l'insu de l'utilisateur. Le recours à un tel outil permet potentiellement de récupérer par exemples, des numéros de cartes bancaires, des mots de passe de banques en ligne ou de *Webmail*. Certains *Keyloggers* sont capables d'enregistrer les *URL* visités, les courriers électroniques consultés ou envoyés, les fichiers ouverts, voir de

[89] Joe Stewart, SecureWorks, RSA Conference http://www.clubic.com/actualite-135320-pc-robots-100-spam.html

[90] Yury Namestnikov « Économie des réseaux de PC zombies », Kaspersky Lab http://www.kaspersky.com/fr/reading_room?chapter=200463607

[91] Il s'agit d'un processus furtif (inclus dans un autre processus ou portant un nom ressemblant fortement au nom d'un processus système) écrivant les informations captées dans un fichier caché.

[92] Il s'agit d'un dispositif intercalé entre le port clavier de l'ordinateur et le clavier.

créer une vidéo retraçant toute l'activité de l'ordinateur.

Très sollicités dans le cadre d'opérations d'espionnage économique et politique, les *keyloggers* ne sont pourtant pas toujours détectés par les antivirus. Ce n'est donc pas évident pour les utilisateurs de les remarquer. Notons, cependant qu'à la différence des autres types de programmes malveillants, le *keylogger* ne présente aucun danger pour le système. Toutefois, il peut être très dangereux pour l'utilisateur.

Lancés directement au démarrage de la machine hôte, les *keyloggers* enregistrent au fur et à mesure tout ce qui est frappé sur le clavier. Si la machine cible ne dispose pas d'une connexion internet, le *keylogger* enverra discrètement, à une adresse mail ou à un serveur internet, un fichier, généralement crypté, contenant tous les renseignements collectés. Le mode opératoire des *keyloggers* est identique, même s'il existe une multitude de *keyloggers* différents. Ils sont installés directement par le pirate sur la machine visée, si l'ordinateur n'a pas de connexion internet permettant une installation à distance via un cheval de Troie[93].

Les *keyloggers* figurent désormais parmi les principales formes de cybercriminalité. Ils ont d'ailleurs détrôné l'hameçonnage en tant que méthode privilégiée pour le vol d'informations confidentielles[94]. En effet, tandis que dans le cas de l'hameçonnage, l'utilisateur attentif peut se protéger en ignorant les messages les plus suspects, il ne peut pas agir de la sorte contre les *keyloggers* et il devra absolument compter sur l'aide de dispositifs de protection spécialisés.

A noter que les fonctionnalités des *keyloggers* ont évolué avec l'avènement des « claviers virtuels», censés se protéger contre les *keyloggers*. En effet, il existe des *keyloggers* dont la fonctionnalité ne se limite plus à la capture des frappes clavier, mais surveillent aussi les clics de la souris et réalisent des captures d'écran.

1.5.3 Le Rootkit

Un *rootkit* (en français, kit racine) est un programme ou un ensemble de programmes permettant à un tiers d'automatiser la dissimulation et l'effacement des traces sur une machine. L'intérêt, c'est de pouvoir maintenir – dans le temps – un accès frauduleux à un

[93] « *Spyware* et sécurité Internet », http://coatmeur.fr/informatique/spyware.pdf

[94] « *Phishing* : la mode est aux *keyloggers* », http://www.itespresso.fr/phishing-la-mode-est-aux-keyloggers-13467.html

système informatique. Le terme *rootkit* était déjà utilisé il y a une douzaine d'années, désignant un kit de petits programmes permettant à un attaquant de maintenir son accès à un niveau « *root* » (ou administrateur) sur un système. Mais aujourd'hui, il va plus loin. En plus d'octroyer les privilèges administrateurs à l'attaquant, il est normalement indétectable sur un ordinateur. Pour y parvenir, il doit être nécessairement discret. En effet, les opérateurs systèmes soupçonnant une intrusion peuvent recourir à une investigation pour rechercher un programme malveillant ou une activité inhabituelle et ainsi compromettre l'action du pirate. D'où l'intérêt pour le pirate d'opérer au niveau noyau afin de pouvoir aisément modifier les fonctions utilisées par tous les logiciels, y compris les outils de sécurité. A partir de ce moment, un *rootkit* peut empêcher un outil de sécurité de s'exécuter directement en lui masquant des informations[95]. Rien à voir donc avec un virus ou ver de nouvelle génération. Un « *rootkit* » ne se réplique pas.

La plupart des techniques utilisées par un *rootkit* ont pour objectif de masquer des fichiers et des répertoires. On peut aussi trouver d'autres fonctionnalités permettant, par exemple, de capturer des paquets de données sur le réseau ou bien de masquer l'émission de certaines informations. Le plus souvent, c'est l'imbrication de ces fonctionnalités qui feront des *rootkits* une menace non négligeable.

2. L'ordinateur comme facilitateur d'actes cybercriminels

Un acte cybercriminel peut être aussi l'incarnation nouvelle d'une opération criminelle classique avec la seule différence, l'utilisation d'un ordinateur comme facilitateur. Parmi les actes de délinquance électronique les plus recensés dans le cyberespace, nous retenons l'escroquerie, la fraude à la carte bancaire, le blanchiment de l'argent, le cyberterrorisme et la pédophilie sur l'internet.

2.1 L'escroquerie

L'escroquerie n'est pas un phénomène nouveau. Il est aussi ancien que l'Homme. Cependant, depuis que l'internet est accessible au grand public, et en raison notamment de l'anonymat que procurent généralement les actes d'escroquerie perpétrés sur le cyberespace, ce phénomène ne cesse de croître. Certains types d'actes d'escroqueries se pratiquent même plus aisément sur l'internet que dans la vie réelle. Il en résulte qu'aujourd'hui tout le monde se retrouve menacé par l'e-arnaque. Qui n'a jamais reçu un

[95] Loïc Falletta, « *Rootkits* : La menace ultime », MAGSECURS, N°21

SMS ou un courrier électronique type « Vous avez gagné 1 million de dollars », ou « Vous êtes l'heureux gagnant du jeu *Coca Cola* » ou encore « Vous avez gagné une bourse d'études de la fondation *Bill Gates* ».

Facilités notamment par l'utilisation du *SPAM,* les cyberescrocs recourent de plus en plus vers les techniques d'ingénierie sociale pour duper les âmes crédules. La plus courante est certainement la « fraude nigérienne », surnommée aussi le *Scam* 419[96], qui consiste à jouer sur la cupidité de la victime pour la convaincre de transférer une somme importante en espérant en recevoir davantage en retour. Tantôt le cyberescroc fait appel à « l'humanité » de sa cible en lui annonçant qu'il se voit provisoirement privée d'importantes ressources. Tantôt, il lui promet de gagner de l'argent facilement. Tous les moyens sont bons pour prendre au piège la victime. Prenons l'exemple de la manipulation frauduleuse du cours d'un titre en bourse. La technique consiste, pour le cyberescroc à investir, en bourse, sur les titres de sociétés n'ayant aucune valeur. Par un envoi massif de courriels, il recommande l'achat de ces actions. A force de *spam*, de plus en plus de personnes investissent, ce qui donne de la valeur à l'action. En effet, plus la demande augmente, plus le cours de la bourse s'envole. Le cyberescroc revend ses actions quand elles ont atteint un niveau conséquent, et ne donne plus de nouvelles aux victimes. Au bout d'un moment, celles-ci commencent à paniquer et revendent leurs actions qui n'ont plus alors de valeur. L'attaquant, lui, pendant ce temps est déjà passé à sa nouvelle arnaque[97].

Au Maroc, le phénomène de l'escroquerie sur l'internet gagne du terrain comme le témoigne les nombreux cas rapportés dont voici quelques exemples :

- ✓ Janvier 2007 : La Direction Générale de la Sûreté Nationale (DGSN), et après avoir été informée d'une opération d'escroquerie sur l'internet ciblant les marocains souhaitant émigrer au Canada, a appelé à la vigilance lorsqu'il s'agit d'utiliser l'internet pour la transmission des demandes d'émigration. En effet, une femme non identifiée qui prétend être la nièce de l'ambassadeur du Canada à Abidjan arrive à faire croire aux victimes rencontrées sur le *Chat* de *Yahoo* qu'elle disposait du pouvoir de les aider à émigrer au Canada, à travers une intermédiation en vue de leur

[96] Appelée ainsi d'après le numéro de la section concernée du code pénal nigérien qui pénalise ce délit.

[97] « Les modèles économiques de la cybercriminalité à la loupe », GIROP
http://www.globalsecuritymag.fr/GIROP-les-modeles-economiques-de,20090314,7959

procurer les documents de séjour[98]. Pour y arriver, le candidat à l'émigration doit faire parvenir à l'adresse de l'ambassade canadienne à Abidjan, son passeport, une photocopie de la Carte d'Identité Nationale (CIN) et des photos d'identité et 533 Euros en faux frais de visa à envoyer au nom d'un certain John Lavry, au moyen de la société de transfert de fonds *Western Union*.

- ✓ Mai 2009 : Les éléments de la police judiciaire d'Essaouira en collaboration avec leurs homologues de Rabat ont dénoué les fils d'une affaire d'escroquerie par l'internet dont ont été victimes une quinzaine de femmes. L'enquête a été déclenchée lorsqu'une étudiante à Essaouira a déposé une plainte auprès de la police de la ville contre X pour piratage de données personnelles, des photos plus particulièrement, et extorsion sous menace. Le cyberescroc, originaire de Rabat et qui se faisait passer pour "un Emirati", promettait à ses victimes parmi les femmes rencontrées sur le Web un emploi dans un pays de la péninsule arabique et exigeait des photos personnelles. Une fois les photos reçues, le cyberescroc qui a eu à son actif, une quinzaine d'opérations identiques réclamait des sommes d'argent allant de 2 000 à 2 500 DH sous peine de diffusion des dites photos sur l'internet[99]. Un numéro de téléphone fourni à la police par la plaignante qui a reconnu avoir effectué au profit de l'escroc deux versements de 500 et 700 DH retirés auprès d'une agence *Wafacash* à Salé, a permis de remonter à la personne recherchée.

2.2 La fraude à la carte bancaire

Le phénomène de fraude à la carte bancaire est en évolution constante. Certes l'avènement de l'internet grand public a favorisé l'utilisation frauduleuse des coordonnées bancaires sur les sites marchands. Mais la fraude à la carte bancaire sur le web n'est rien en comparaison avec la fraude offline. En effet, le paiement par carte bancaire sur l'internet reste globalement un phénomène mineur par rapport au total des opérations réalisées par cartes physiquement. L'internet est rarement le lieu d'origine de la compromission des informations bancaires de l'acheteur. Selon une étude réalisée par *FIA-NET*[100], les données dérobées le

[98] « Maroc : la DGSN met en garde contre une escroquerie par Internet »
http://www.fmaroc.com/news+article.storyid+68.htm

[99] « Essaouira: dénouement d'une affaire d'escroquerie par internet »
http://biladi.ma/1012982-essaouira-denouement-d-une-affaire-d-escroquerie-par-internet.htm

[100] FIA-NET est un prestataire de service dont le métier est d'assurer un climat de confiance entre les acheteurs et vendeurs sur le web.

sont le plus souvent dans le monde physique et l'internet est avant tout un lieu d'utilisation de ces informations bancaires[101] comme le démontre les exemples suivants :

- Mars 2002, les gendarmes français ont réussi le démantèlement d'un réseau international de falsification de cartes. Le système utilisé était ingénieux, les malfrats de véritables stratèges. Il s'agissait de caméras fixées sur les pompes à essence automatiques de stations- service. Elles permettaient d'espionner à distance les codes secrets des clients : 143 automobilistes avaient été piégés pour un préjudice global estimé à 260 000 Euros[102].
- Juillet 2007, le chef présumé d'une bande organisée de piratage de cartes bancaires a été arrêté par les officiers de la police judiciaire de Toulouse. L'homme en question, était recherché par la police depuis quatre ans. Il était à la tête d'un réseau de pirates qui se servaient des outils dits *skimmers*[103] pour détourner de l'argent via des distributeurs de billets[104].
- Juillet 2007 : Un réseau international de contrefaçon de cartes bancaires a été démantelé. Ses membres pirataient des données bancaires en Asie avant de les recopier sur des cartes vierges en France. Les enquêteurs ont découvert un véritable arsenal lors des perquisitions: cinq ordinateurs, trois encodeurs, deux machines à embosser (qui impriment les numéros en relief de la carte) ou encore 1 200 cartes vierges et 14 déjà contrefaites. Le préjudice s'élève à plusieurs centaines de milliers d'euros[105].
- Juillet 2009 : Vingt-quatre personnes ont été arrêtées lors d'une opération policière visant à démanteler un réseau international de fraude à la carte bancaire actif dans plusieurs pays européens. Le réseau est suspecté d'avoir copié au moins 15.000 cartes de paiement dans l'Union Européenne, pour plus de 35.000 transactions frauduleuses d'un total d'environ 6,5 millions d'euros[106].

---

[101] FIA-NET « La fraude à la carte bancaire : le livre blanc 2008 » http://static.fia-net.com/__docs/livre_blanc_juin-2008.pdf

[102] http://marches.lefigaro.fr/news/societes.html?OFFSET=1&ID_NEWS=132400235&LANG=f

[103] Ce matériel électronique est capable de lire la bande magnétique d'une carte bancaire afin d'en extraire les informations. Celles-ci permettent ensuite de cloner, à l'identique, la carte usurpée sur une carte vierge.

[104] http://www.01net.com/editorial/354916/un-important-reseau-de-pirates-de-cartes-bancaires-demantele/

[105] http://www.lexpress.fr/actualite/societe/carte-bleue-un-reseau-de-piratage_demantele_465800.html

[106] http://www.7sur7.be/7s7/fr/1505/Monde/article/detail/951732/2009/07/31/Fraude-a-lacarte-bancaire-24-personnes-arretees-en-Europe.dhtml

Le Maroc n'échappe pas au phénomène de fraude à la carte bancaire. En effet, le nombre de cartes bancaires contrefaites au Maroc est passé de 1.694 cartes en 2000 à plus de 6.000 en 2008. Soit le triple. En parallèle, le montant des sommes détournées connaît lui aussi une hausse vertigineuse. De 4,4 millions de dirhams en 2000, ce montant est passé à 20 millions en 2008[107]. Une telle croissance s'explique notamment par l'engouement que suscite l'utilisation de la carte bancaire. Selon le Centre Monétique Interbancaire[108] (CMI), les opérations par cartes bancaires, marocaines et étrangères, au Maroc ont atteint au terme de l'année 2009 : 138 millions d'opérations pour un montant global de 119 milliards de DH. Ce montant est en progression de 16,3% par rapport à l'année précédente. Cet engouement n'est pas sans risque comme le rappelle les exemples suivants :

- 2005 : La gendarmerie royale a arrêté 7 personnes soupçonnées d'avoir détourné 4,6 millions de DH en copiant des cartes bancaires à l'aide de matériel informatique[109].
- 2008 : Deux employés d'un centre d'appel basé à Casablanca, ont été interpellés par les agents de la brigade centrale de police. Ils ont détourné d'importantes sommes d'argent en utilisant les données de porteur de cartes (nom de titulaire de carte, *PAN*[110], date d'expiration, etc…) qu'ils enregistraient lors des conversations téléphoniques avec les clients français et transmettaient par la suite à une complice basée en France qui se chargeait d'acheter des biens sur l'internet et de les revendre après. L'affaire a été portée à la connaissance de la brigade centrale de police par France Télécom. L'opérateur français avait en effet réclamé aux autorités marocaines d'enquêter sur les détournements dont ont été victimes une dizaine de ses clients[111].
- 2009 : Un réseau international spécialisé dans la falsification de cartes bancaires a été démantelé par la police de Casablanca. L'arrestation a eu lieu suite une alerte lancée auprès de la police par le responsable d'un hôtel où avait l'habitude de séjourner l'un des membres du groupe, et ce après avoir découvert, caché dans les gaines, un matériel électronique composé notamment d'un encodeur qui sert à falsifier les cartes bancaires et de plusieurs caméras. Ainsi, 1.400 cartes falsifiées ont été saisies. Le procédé est le même. Insérer une minuscule caméra et un appareil

[107] « Attention, cartes bancaires piratées », Maroc Hebdo
http://www.marochebdo.press.ma/MHinternet/Archives_844/html_844/attentioin.html

[108] http://www.cmi.co.ma

[109] « Piratage: Attention à vos cartes bancaires », l'Economiste
http://www.leconomiste.com/print_article.html?a=65366

[110] Primary Account Number (PAN) est le numéro qui est composé des 16 chiffres qui figure sur la carte bancaire.

[111] http://www.bladi.net/arnaque-centres-appel-maroc.html

type *skimmer* dans des guichets automatiques des quartiers aisés de la métropole économique[112].

Devant la professionnalisation accrue des malfaiteurs, il devient de plus en plus difficile de repérer la fraude. Partant de ce constat, les autorités et organismes compétents doivent se doter des outils de détection et des moyens nécessaires pour lutter efficacement contre ce fléau.

2.3 Le blanchiment d'argent

Le blanchiment d'argent est le processus consistant à dissimuler la source de l'argent ou des biens tirés d'activités criminelles. Une grande variété d'activités illégales est motivée par le profit, notamment le trafic de stupéfiants, la contrebande, la fraude, l'extorsion de fonds, la corruption et la cybercriminalité. L'enjeu financier est important - quelque 500 milliards à un billion de dollars américains dans le monde entier chaque année[113].

Sur l'internet, en raison notamment de la multiplication des banques en ligne, des casinos virtuels, des sites de paris en ligne et des possibilités de placements boursiers en ligne, les possibilités de blanchiment d'argent sont illimitées. Ainsi, transférer des capitaux sur le web est devenu une activité fleurissante. Les intermédiaires recrutés sont qualifiés de «mules[114]» et peuvent gagner une somme d'argent considérable, en toute illégalité. Avec ces modes opératoires, les activités cybercriminelles demeurent incontrôlables et les poursuites en justice se révèlent parfois impossibles[115]. En outre, compte tenue de l'implication de la planète toute entière dans la lutte contre le financement du terrorisme international, sous l'impulsion des Etats-Unis, l'argent sale provenant des activités criminelles ne peut plus circuler librement, même dans les paradis fiscaux[116]. Par conséquent, les diverses mafias se sont logiquement tournées vers la Toile pour l'activité de blanchiment de l'argent.

---

[112] « Attention, cartes bancaires piratées », Maroc Hebdo
http://www.marochebdo.press.ma/MHinternet/Archives_844/html_844/attentioin.html

[113] Source : Centre d'analyse des opérations et déclarations financières au Canada (CANAFE)
http://www.canafe-fintrac.gc.ca/intro-fra.asp

[114] Une « mule » est quelqu'un qui sert d'intermédiaire pour blanchir de l'argent, provenant d'escroqueries commises sur Internet ou d'autres pratiques frauduleuses.

[115] Solange Ghernaouti-Hélie « La cybercriminalité : Le visible et l'invisible », collection le savoir suisse, Edition 2009, Page 101

[116] http://cybercriminalite.wordpress.com/2008/11/30/internet-jeux-en-ligne-blanchiment-dargent-un-trio-devastateur

De ce phénomène se dégage deux principales tendances. Il s'agit du recours de plus en plus croissant vers les casinos en ligne et l'emploi de plus en plus facile des mules.

2.3.1 Les casinos en ligne

Le recours aux jeux de hasard en ligne demeure une tendance sérieuse en matière de blanchiment d'argent. Les casinos en ligne sont devenus les terrains de prédilection des organisations mafieuses modernes constate le Groupe d'Action Financière[117] (GAFI). Ils permettent aux cybercriminels de placer en toute impunité leur argent sale, et d'encaisser en retour les gains de jeu officiels. La création de tels sites se fait en toute illégalité. Ceux-ci sont qualifiés de « sauvages », très mobiles puisqu'ils changent constamment de pays et de serveur, afin de brouiller les pistes. Selon une récente étude de *McAfee*, plus 87 % des sites de jeux de hasard proposés sur l'internet réalisent une activité clandestine (sans licence)[118]. L'absence de cadre juridique permet à quiconque d'enregistrer un site web dans l'anonymat puis de facturer les clients via un compte bancaire anonyme dans un paradis fiscal ou un système monétaire virtuel.

Au Maroc, les jeux de hasard et d'argent font l'objet d'une réglementation très stricte. Ce qui permet de contrôler étroitement les conditions d'enregistrement et d'exploitation de ces activités. De ce point de vue, la situation des casinos virtuels est doublement illégale[119]. D'abord, parce qu'ils ne peuvent être crées que dans certaines villes du royaume. Ensuite, le transfert de devises ne peut être opéré dans un tel contexte.

2.3.2 Les mules

A l'origine le mot « mule » est utilisé dans le jargon du trafic de stupéfiant pour désigner toute personne chargée de faire transiter des produits illicites au travers de frontières. L'économie sous terraine de la cybercriminalité possède aussi ses propres mules. Il s'agit des

---

[117] Le Groupe d'Action financière (GAFI) est un organisme intergouvernemental visant à développer et promouvoir des politiques nationales et internationales afin de lutter contre le blanchiment de capitaux et le financement du terrorisme. http://www.fatf-gafi.org/pages/0,3417,fr_32250379_32235720_33631745_1_1_1_1,00.html

[118] François Paget « Fraude financière et opérations bancaires en ligne : menaces et contre-mesures », McAfee® Avert® Labs
http://www.mcafee.com/us/local_content/reports/6168rpt_fraud_0409_fr.pdf

[119] Bouchaïb Rmail, « Criminalité informatique ou liée aux nouvelles technologies de l'information et de la communication », Edition Somagram, page 101

individus recrutés via l'internet pour servir d'intermédiaires afin de récupérer les fonds illicitement.

En contrepartie des opérations de transferts de fonds dont elle aura la charge, la mule reçoit à titre de commission entre 5 et 10% du montant transféré. Les fonds en question sont retirés par la mule sous forme de liquide après les avoir reçus sur son propre compte bancaire et renvoyés par la suite aux cybercriminels à l'aide de services de transfert d'argent tels que *Webmoney, E-Gold, Western Union, MoneyGram, PayPal*, etc…

Le recrutement des mules s'effectue généralement via l'envoi de *spam*. Le destinataire se voit proposer de «devenir partenaire» d'une société respectable. De telles offres figurent aussi de plus en plus sur des sites de recherche d'emploi parfaitement légitimes. En novembre 2008, le site www.bobbear.co.uk consacré à la dénonciation des sites frauduleux impliqués dans le recrutement de mules, recensait 193 offres d'emploi en ligne consacrées au recrutement de mules[120].

Pour être éligible à l'offre, on demandera à la personne visée souvent de parler anglais, d'avoir environ deux heures à consacrer à cette activité par jour et, surtout, de disposer ou d'ouvrir un compte en banque pour effectuer des transactions. Si le destinataire de message manifeste son intérêt, il recevra un pseudo contrat qui va le lier à son nouvel employeur. Il sera contacté par la suite pour l'informer qu'une somme d'argent a été versée sur son compte et qu'il devra par la suite transférer souvent via *Webmoney, E-Gold, Western Union, Moneygram, ou PayPal*, à une personne bien déterminée qui se trouve souvent dans un autre pays. En agissant ainsi, la mule sans le savoir des fois, participe à une opération de brouillage de pistes qui permettra au cybercriminel de récupérer de l'argent blanchi. Remarquons par ailleurs, que de nombreuses personnes en quête d'argent facile en cette période de marasme économique[121] n'hésitent pas à se porter volontaires à tel point que certains experts n'hésitent pas à qualifier le travail de mule comme une profession à part entière[122].

---

[120] « Les dessous de l'hameçonnage : La mécanique expliquée », ZERO SPAM
http://www.isiq.ca/entreprise/publications/articles/articles_pdf/zerospam_fiche-dessous_hameconnage.08.pdf

[121] « Blanchiment d'argent : La cybercriminalité en plein recrutement ».
http://www.zataz.com/news/18426/blanchiment--argent-faux--emploi.html

[122] François Paget « Fraude financière et opérations bancaires en ligne : menaces et contre-mesures », McAfee® Avert® Labs

Pour mieux illustrer la mécanique derrière l'implication des mules, analysons à présent les deux scénarios suivants[123] :

Dans le 1er scénario, le commanditaire a pour objectif de collecter des fonds issus de comptes PayPal préalablement compromis.

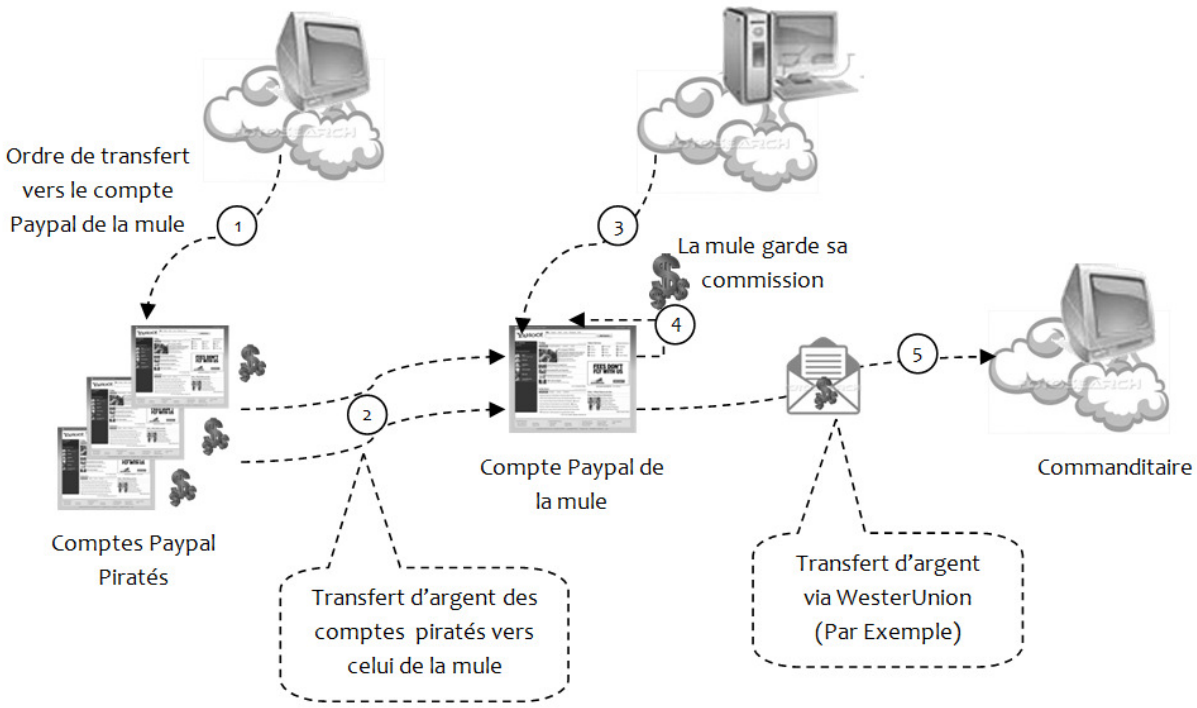

Figure 16 : Exemple de blanchiment d'argent via une mule[124]

1. Le commanditaire se connecte sur les comptes *PayPal* volés
2. Le commanditaire transfère l'argent depuis les comptes *PayPal* compromis vers celui de la mule.
3. La mule accède à son compte *PayPal*

---

http://www.mcafee.com/us/local_content/reports/6168rpt_fraud_0409_fr.pdf

[123] Source : Ces deux scénarios ainsi que les schémas correspondants ont été repris intégralement à partir du blog Sécurité de Orange Business Services. Article « Recrutement de "mules" : Petit cas d'espèce et schémas d'utilisation », Jean-François Audenard.
http://blogs.orange-business.com/securite/2009/03/recrutement-de-mules-petit-cas-despece-et-schemas-dutilisation.html

[124] Orange Business Services – Blog Sécurité – Jean-François Audenard http://blogs.orange-business.com/securite/

4. La mule provisionne son compte bancaire classique à partir de l'argent de son compte *PayPal* tout en gardant une commission prédéfinie.
5. Elle envoie un mandat (ici via *Western Union*) à l'adresse indiquée par le commanditaire.

L'étape finale passant d'un mode "électronique" à un mode "classique" (*PayPal* vers *Western Union*) peut être apparentée à une notion de "rupture de protocole". Cela rendra plus complexe la remontée éventuelle de la chaîne pour les forces de l'ordre.

Dans le deuxième scénario, le commanditaire souhaite recevoir des marchandises achetées avec des cartes bancaires volées.

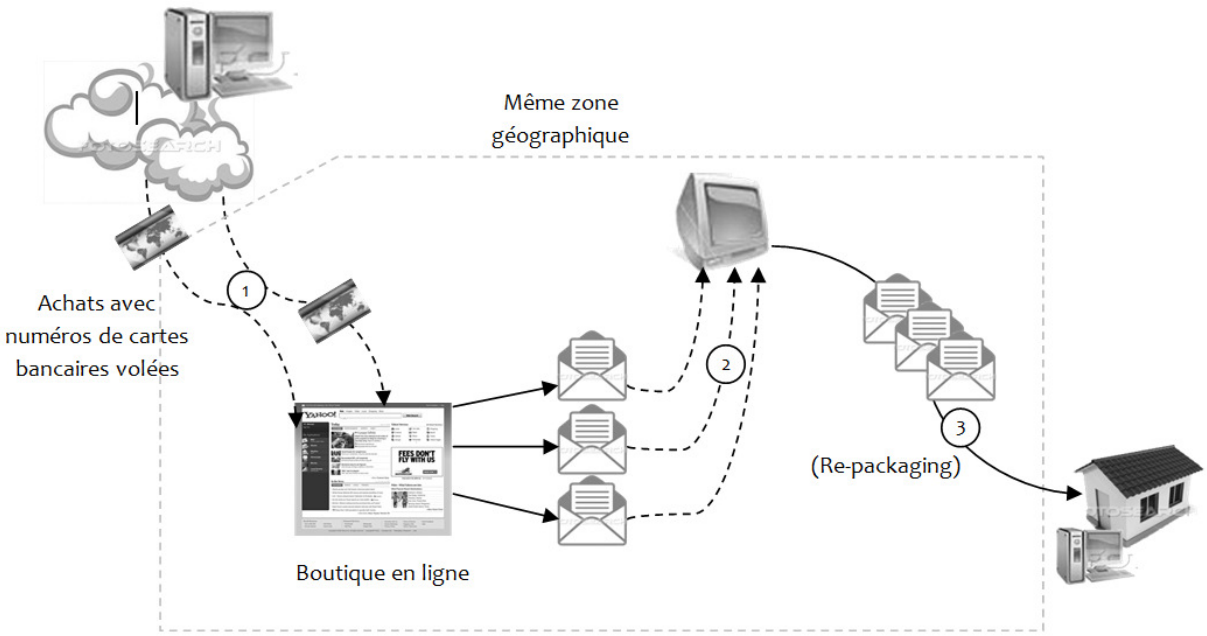

Figure 17 : Réexpédition de marchandises "douteuses" par une mule[125]

1. Le commanditaire achète des biens ou marchandises en utilisant des numéros de cartes bancaires volés. Les marchandises sont livrées à la mule. Typiquement, la livraison est faite à une mule résidant dans le même pays que celui des cartes bancaires, ce afin de réduire la détection éventuelle.
2. La mule effectue un éventuel regroupement des marchandises (ou un déballage/ré-emballage sous forme de cadeaux) et les envoie au commanditaire.
3. Les frais d'envoi sont typiquement payés à la mule via un transfert d'argent depuis un compte bancaire volé.

[125] Idem

Dans les deux schémas présentés, c'est la mule qui sera suspectée en priorité :

- ✓ C'est son compte *PayPal* vers lequel les sommes ont été versées depuis les comptes *PayPal* piratés
- ✓ C'est à son adresse qu'ont été livrées les marchandises achetées avec des cartes

Au Maroc, bien que nous disposions d'une réglementation stricte en matière de transfert de l'argent à l'étranger, nous assistons de plus en plus à un recrutement des mules comme le laisse entendre les nombreuses annonces de travail à domicile localisées sur les sites d'emplois marocains.
Autre l'appât du gain, le blanchiment d'argent sur l'internet peut être aussi motivée par une action de financement des groupes terroristes. Il s'agit d'une manifestation parmi tant d'autres du cyberterrorisme.

2.4 Le cyberterrorisme

Le cyberterrorisme est un terme controversé. Il peut être défini comme l'utilisation de l'information et du contrôle des systèmes d'information, par des groupes organisés ou par un individu, comme arme stratégique pour exercer des pressions et intimider l'adversaire[126]. Il peut s'agir de manipulation de l'information, de désinformation, d'infiltration de réseaux, de sabotage des infrastructures télécoms, de perturbation des services publics etc.

La vulnérabilité des infrastructures critiques d'un pays n'est plus à démontrer de nos jours. En effet, les secteurs comme le transport, les télécommunications, les services médicaux, l'eau, l'énergie et les services de l'administration recourent de plus en plus à une utilisation massive des technologies de l'information. L'importance de tels secteurs est telle qu'aujourd'hui, la dépendance vis-à-vis les technologies de l'information est très forte. L'indisponibilité d'un service public critique peut avoir un impact colossal sur le bon fonctionnement des activités d'un pays. Par exemple, la perturbation des services liés à une centrale des systèmes de production et de distribution d'électricité est de nature à porter atteinte à la sécurité publique en entraînant de la panique, en générant de la terreur et en mettant en danger les capacités de survie, voir en causant des pertes humaines. Par

[126] Provient de l'Office Québécois de la Langue Française (OQLF) http://www.olf.gouv.qc.ca/

conséquent, la prise de contrôle de ces infrastructures pourrait constituer un objectif privilégié du cyberterrorisme[127].

La cybercriminalité peut donc avoir une dimension terroriste. Selon un rapport de l'*Intelligence Advanced Research Projects Activity*[128] (IARPA), le cyberterrorisme peut se manifester à plusieurs niveaux. Il en a identifié cinq[129] :

1. **Les communications secrètes :** C'est l'un des aspects les plus visibles. Les terroristes utilisent le cyberespace comme outil de communication efficace pour, entre autres, y faire de la propagande et du renseignement, pour recruter, former, entraîner, rechercher des cibles, organiser, planifier des opérations et communiquer. L'internet, peu surveillé, offre potentiellement une formidable plateforme de communication aux groupes terroristes. En effet, le rapport des terroristes avec le cyberespace n'est pas anodin. L'exemple de l'attaque perpétrée par un Kamikaz dans un cyber café casablancais en mars 2007 est plein d'enseignement. Si le cyber n'était pas la cible de l'attaque, l'incident démontre à quel point le recours à l'internet est important pour la préparation des attaques terroristes[130].
2. **Entraînement**: Le caractère de plus en plus réel des mondes virtuels, ainsi que leur caractère modulable (la possibilité de créer des environnements spécifiques) permet aisément aux terroristes de simuler une attaque (avant de la mettre en œuvre dans le monde réel), et de développer de nouvelles stratégies. L'exemple de *Google Earth*[131] est édifiant. En effet, cet outil offre aux terroristes sans risque et en toute impunité toutes les informations et photos nécessaires pour identifier des cibles d'actions y compris pour les zones qualifiées comme sensibles. Les terroristes peuvent alors disposer de tout ce qui est nécessaire pour que leur action soit performante[132].

---

[127] Solange Ghernaouti-Hélie « La cybercriminalité : Le visible et l'invisible », collection le savoir suisse, Edition 2009, Page 88

[128] IARPA est une agence gouvernementale américaine spécialisée dans la très haute technologie de communication, équivalent de la DARPA militaire pour les services de renseignement

[129] http://lefrontasymetrique.blogspot.com/2008/04/terrorisme-et-cyberterrorisme-dans-les.html

[130] http://www.infosdumaroc.com/modules/news/articles-4181-internet-maroc-du-paradis-virtuel-a-l-enfer-terror.html

[131] Google Earth est un logiciel, propriété de la société Google, permettant une visualisation de la Terre avec un assemblage de photographies aériennes ou satellitaires.

[132] Solange Ghernaouti-Hélie « La cybercriminalité : Le visible et l'invisible », collection le savoir suisse, Edition 2009, Page 89

3. **Transfert/Blanchiment d'Argent**: Il est désormais possible pour des groupes terroristes de transférer des fonds de manière virtuelle et de les convertir ensuite, au besoin, en argent réel. L'argent est ainsi blanchi par l'intermédiaire de bureaux de change, de courtiers ou agents de change, des sociétés écrans, etc…
4. **Cyberattaques**: Jusqu'à une date récente, la cyberguerre était considérée comme étant une simple vision virtuelle sans conséquences réelles. Malheureusement quelques événements récents ont contredit cette vision. Plusieurs exemples significatifs ont marqué ces dernières années nos esprits. Il s'agit notamment de :

   - ✓ Mai 2007 : L'Estonie a été soumise à une cyber-attaque massive à la suite de la suppression d'un monument commémoratif de la seconde guerre mondiale. Malgré les spéculations que l'attaque avait été coordonnées par le gouvernement russe, le ministre de la défense de l'Estonie a admis qu'il n'avait aucune preuve liant les cyber-attaques aux autorités russes. La Russie a appelé « sans fondement » les accusations de son implication, et signalé que ni l'OTAN ni les experts de la commission européenne n'ont pu trouver des preuves de la participation officielle du gouvernement russe[133].
   - ✓ Octobre 2007 : Le site du président ukrainien Viktor Yushchenko a été attaqué. Un groupe de jeunes nationalistes russes, l'office eurasien *Youth Movement*, a revendiqué la responsabilité[134].
   - ✓ Août 2009 : De nombreux sites web géorgiens se sont trouvés paralysés, rendus inaccessibles par des attaques de type *DDoS*, ou bien défigurés, leurs pages modifiées par des hackers. Parmi les sites touchés on compte ainsi celui du président Mikhaïl Saakachvili, celui du ministère des affaires étrangères, du Parlement, du ministère de la défense, de la banque nationale de Géorgie, du portail d'information Georgia On-Line, du site rustavi2.com de la chaîne Georgian TV, de sosgeorgia.org (qui fait depuis défiler sur son site un bandeau pour informer les internautes qu'il fait l'objet d'attaques massives de la part des *hackers* russes), etc. L'exemple de la Géorgie est intéressant puisqu'il est le seul cas où les cyberattaques ont accompagné une « vraie » guerre[135].

[133] http://www.01net.com/editorial/350759/lestonie-denonce-les-cyber-attaques-terroristes-russes/

[134] http://www.ukrspravka.info/fr/3302.html

[135] http://www.ecrans.fr/La-Russie-mene-aussi-une-cyber,4861.html

- ✓ Juillet 2009 : Plusieurs cyber-attaques ont été lancées contre le Pentagone et la Maison Blanche aux Etats-Unis et des agences gouvernementales en Corée du Sud. Ces deux gouvernements ont accusé la Corée du Nord d'avoir lancée ces attaques[136].
- ✓ Janvier 2010 : Des *hackers* chinois ont lancé des attaques sophistiquées contre le géant américain Google. Cette attaque qui a été relayée par des complicités humaines au sein de Google, auraient procédé en deux vagues. La première qualifiée d'ultrasophistiquée s'en serait prise à des codes sources de logiciels Google. La seconde, travaillant de façon plus rustique par *phishing.* Cet incident, qui a ouvert le bal à une guerre froide numérique entre les deux pays, s'est terminé par un retrait de la société américaine Google du marché chinois[137].

Compte tenu de l'importance des conséquences de telles attaques, plusieurs pays n'ont pas hésité à mettre des mesures drastiques pour une surveillance et une protection plus serrées des réseaux internes et pour la création de leurs propres moyes de cyberdissuasion[138]. Voici quelques exemples de mesures prises en 2009.

- ✓ Avril 2009 : Le gouvernement britannique confirme son projet d'un système de pistage de 2 milliards de livres, aussi appelé *Interception Modernisation Programme* (IMP), pour explorer le trafic réseau à la recherche d'activités criminelles ou dangereuses[139].
- ✓ Juin 2009 : Les Etats-Unis annoncent la création de *l'US Cyber Command*, une structure militaire officielle dédiée à la défense contre les cyber-invasions et les attaques à l'encontre des réseaux informatiques ennemis[140].
- ✓ Juin 2009 : Le Royaume-Uni annonce son intention de former *l'Office for Cyber Security*, l'équivalent britannique de *l'US Cyber Command*, et refuse de nier qu'il attaque d'autres pays dans le cyberespace[141].

---

[136] http://www.20minutes.fr/article/337970/Monde-La-Maison-Blanche-et-le-Pentagone-victimes-d-une-cyber-attaque.php

[137] http://www.huyghe.fr/actu_750.htm

[138] « Rapport 2010 sur les menaces à la sécurité », SOPHOS http://www.sophos.fr/security/topic/security-report-2010.html

[139] http://www.theregister.co.uk/2009/04/27/imp_consultation156

[140] http://www.govexec.com/nextgov/0609/gates_cybercommand_memo.pdf

[141] http://www.sophos.com/blogs/gc/g/2009/06/26/uk-attack-countries-cyberspac

- ✓ Juillet 2009 : Un membre républicain du Congrès, aussi membre éminent du "*House Intelligence Committee*", incite le président Obama à prendre de solides cyber-mesures contre la Corée du Nord en représailles de son rôle supposé lors des cyber-attaques sur les Etats-Unis et la Corée du Sud[142].
- ✓ Novembre 2009 : l'Inde annonce des projets semblables à l'*IMP* britannique, suite à l'utilisation de la voix sur *IP* et *Google Earth* par des terroristes pour planifier et coordonner les attaques massives à Bombay[143]. Au début de l'année, l'Inde fait par ailleurs l'objet d'attaques de *spyware* au Ministère de l'Education, que beaucoup imputent à la Chine[144].
- ✓ Décembre 2009 : Le président américain Obama nomme Howard Schmidt responsable du Cyberspace[145].

5. **Guerre Informationnelle**: Les terroristes peuvent faire circuler leur propagande et recruter de nouveau membres dans un univers qui ressemble encore largement au "*wild west*", selon la *IARPA*.

Visé à plusieurs reprises par les attentats terroristes, le Maroc a entrepris plusieurs mesures dans le cadre de sa lutte antiterroriste dont la principale est la promulgation de la loi n° 03-03 relative à la lutte contre le terrorisme. Une loi qui réprime aussi le cyberterrorisme. Elle est claire à ce sujet et ne prête à aucune confusion. En effet, l'activité terroriste est appréhendée en combinant deux critères, à savoir l'existence d'un crime ou d'un délit de droit commun prévu par le code pénal, en l'espèce les infractions informatiques et d'autre part la relation de ces crimes ou délits avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur.

2.5 La pédophilie sur l'internet

L'internet en tant qu'environnement, à la fois appartenant à tout le monde et n'appartenant à personne, apporte une sécurité inédite aux réseaux pédophiles. En effet, grâce à la diffusion des technologies assurant l'anonymat, notamment le chiffrement des courriels et

[142] http://www.sophos.com/blogs/gc/g/2009/07/13/republican-urges-obama-launch-cyber-attack-north-korea

[143] http://www.theregister.co.uk/2009/11/27/imp_india/

[144] http://www.sophos.com/blogs/gc/g/2009/02/16/indian-government-computers-hit-spyware-attack

[145] http://www.washingtonpost.com/wp-dyn/content/article/2009/12/21/AR2009122103055.html162

l'utilisation du *proxy*[146], il est devenu extrêmement difficiles de surveiller les activités des réseaux pédophiles. La prolifération des contenus pédophiles sur l'internet est telle qu'en 2006, le nombre de sites contenant des images ou des vidéos de pornographie juvénile a dépassé 3000 sites web selon *Internet Watch Fondation*[147]. Bien que ce chiffre ait baissé en 2008 de 10%[148], les réseaux pédophiles continuent toujours à faire de l'internet une véritable zone de non-droit. Un havre de paix où s'échangent par centaines de milliers et en toute impunité les supports multimédias pédophiles[149]. Rappelons par ailleurs qu'avec le développement du haut débit, l'échange d'images pédophiles se transforme en échange de séquence vidéo. Le « *cam to cam* » est devenu un véritable phénomène de société. Un pédophile peut donc approcher ses futures victimes en toute quiétude, caché derrière son écran.

Selon un chiffre désormais largement diffusé, un mineur sur cinq a été confronté à des avances sexuelles sur l'internet[150]. Le Maroc n'échappe pas à ce phénomène. Il est de plus en plus visé par les réseaux pédophiles. En effet, selon les résultats d'une enquête réalisée par *Center for Media Freedom in the Middle East and North Africa* (*CMF-MENA*)[151] auprès de 106 enfants de la ville de Casablanca, plus des deux tiers des enfants interviewés auraient reçu des offres de voyages, des cadeaux ou des propositions de mariages via l'internet de la part d'inconnus. Ces dernières années ont été marquées par plusieurs affaires de pédophilie sur l'internet au Maroc. Nous citons notamment[152] :

- 2005 : Hervé Le Gloannec, un touriste français a été condamné par le tribunal de première instance de Marrakech à 4 ans de prison ferme. Il ne s'était pas contenté d'infliger des sévices sexuels sur des enfants à Marrakech, mais il s'était également adonné à l'exploitation de leur vertu à travers la production et la distribution de films pornographiques utilisant des enfants. Son ordinateur personnel regorgeait de 17.000

[146] Un serveur mandataire ou proxy (En anglais) est un serveur informatique qui a pour fonction de relayer des requêtes entre un poste client et un serveur.

[147] Un organisme de surveillance des activités pédopornographie sur le Web basé en Grande-Bretagne

[148] Guillaume Belfiore, « Pédopornographie : menace en baisse mais plus complexe » http://www.clubic.com/actualite-273492-cyber-pedo-pornographie.html

[149] Joël Rivière, « Criminalité et Internet, une arnaque à bon marché », dossier « Cybercriminalité, une guerre perdue ? » Documentation française. Hiver 2008-2009

[150] Agnès Leclair, « Les Ados auteurs de 90% des avances sexuelles sur Internet », Le Figaro http://www.lefigaro.fr/actualite-france/2009/01/21/01016-20090121ARTFIG00520-les-ados-auteurs-de-des-avances-sexuelles-sur-internet-.php

[151] Un centre de recherche sur les médias basé à Londres

[152] Source : CMF-MENA

photos et 140.000 enregistrements vidéo qu'il envoyait vers des sites pornographiques[153].

- 2005 : Un journaliste belge de l'hebdomadaire « Le Soir » prenait des photos pornographiques des jeunes filles d'Agadir et les publiait sur un site pornographique. Parmi ses victimes, il y avait des prises montrant des filles mineures.
- 2006 : Le directeur du théâtre Mogador à Paris a été condamné par le tribunal de première instance de Marrakech à quatre mois de prison avec sursis après avoir été pris en flagrant délit en train d'abuser sexuellement d'un mineur qu'il a rencontré sur l'internet selon les rapports de police.
- 2006 : Un touriste français a été condamné à 4 ans de prison après avoir été pris en flagrant délit, en train de prendre des photos d'enfants mineurs dans des positions sexuelles. Il possédait dans son appareil photo 117.000 photos pornographiques.

Cette liste est loin d'être exhaustive. De nombreux cas de pédopornographie sur l'internet au Maroc ne font pas l'objet d'investigation. Rares sont les victimes qui vont aller jusqu'à dénoncer en justice leurs agresseurs. Quoi qu'il en soit, les scandales cités nous montrent à quel point les crimes sexuels sur les mineurs marocains prennent de l'ampleur sur l'internet. Certains criminels considérés avant comme des pédophiles passifs ont fait le pas vers la pédophilie active. L'apparition notamment de sites de rencontre et de discussion, et leur réappropriation massive par les jeunes – en particulier les préadolescents – les a fortement encouragés à basculer vers la pédophilie active.

[153] L'association « Touche pas à mon enfant », Rapport annuel, 2008 téléchargeable à l'adresse suivante : http://www.touchepasamonenfant.com/Rapportannuel/tabid/210/Default.aspx

Conclusion du chapitre

La cybercriminalité peut se manifester de plusieurs façons. En effet, l'ordinateur peut non seulement être la cible et le moyen d'attaque mais aussi le facilitateur d'actes cybercriminels.

Appuyées de plus en plus sur les réseaux de zombies, qui resteront l'un des principaux problèmes auquel devra faire face les autorités de régulation de l'internet dans les années à venir, les attaques sont de plus en plus variées et difficiles à détecter.

De l'attaque virale à l'espionnage industriel, en passant par *le phishing, le carding*, le blanchiment d'argent et la pédopornographie en ligne, rien n'échappe au phénomène de la cybercriminalité. Seule l'imagination du cyberdélinquant demeure une limite sérieuse à l'expansion de la cybercriminalité.

La convergence de la criminalité classique vers une criminalité numérique est en passe de devenir la règle. Ainsi, les mafias voient de plus en plus dans la cybercriminalité une alternative qui présente des avantages sérieux par rapport à la criminalité dans le monde réel.

Chapitre 3 : L'écosystème de la cybercriminalité au Maroc

« Internet est le produit d'une combinaison unique
de stratégie militaire, de coopération scientifique
et d'innovation contestataire»
Manuel Castells

Chaque acte cybercriminel suppose l'interaction entre plusieurs acteurs aux aspirations diverses. Il ne peut être la résultante d'une action perpétrée par un seul individu. Mener à bien une opération cybercriminelle, ayant notamment comme objectif l'appât du gain, repose inévitablement sur une logique de spécialisation, de division de travail et de répartition des tâches. Une telle logique est nécessaire pour la formation d'un écosystème cybercriminel.

Etudier l'écosystème de la cybercriminalité est un exercice intellectuel difficile. En effet, l'univers *Underground,* qui est l'une de ses composantes majeures, est difficilement pénétrable. Ses acteurs agissent en parfaite discrétion et tirent profit de l'anonymat que leurs procurent les nombreux outils de cyberespace. En outre, de nombreuses organisations refusent de communiquer autour des actes cybercriminels dont elles font l'objet. Ces opérations échappent donc aux analyses et investigations permettant une meilleure compréhension de l'économie souterraine de la cybercriminalité.

Si les industriels de sécurité composés notamment des éditeurs de logiciels et de fournisseurs de services ne cessent de faire évoluer leurs produits et services – souvent avec l'aide du milieu universitaire – pour tenir compte des nouvelles menaces – les acteurs de l'univers *Underground* sont toujours à la recherche de nouvelles vulnérabilités permettant d'outrepasser les mesures de sécurité. Nous avons eu d'ailleurs souvent le sentiment que les industriels de sécurité se trouvent dépassés par les événements.

Au Maroc, l'écosystème de la cybercriminalité est dans un état embryonnaire. Il a en outre, ses propres spécificités. Par exemple, le cybercafé joue un rôle extrêmement important dans l'univers *Underground*. On ne peut donc le comparer à l'écosystème d'un pays comme la France, le Canada où les Etats-Unis dont la formation date de plusieurs années.

1. L'univers *Underground*

Contrairement à ce qu'anime souvent notre imaginaire collectif, le pirate n'est qu'un maillon de la longue chaîne constituant l'univers *Underground.* Ce dernier se compose d'une multitude d'acteurs aux aspirations différentes. Des logiques diverses animent l'univers *Underground*. Dés lors, la recherche d'une classification est presque impossible pour cerner le phénomène. Les frontières sont de plus en plus floues. *L'Ethical Hacker,* qui n'est autre qu'un *hacker* reconverti offrant ses services aux cabinets conseil dans le cadre notamment des missions de tests d'intrusion est une meilleure illustration de la complexité régissant l'univers de l'*Underground.* Les acteurs basculent facilement et souvent d'un coté à l'autre. Ce constat a même incité certains experts à identifier une nouvelle catégorie d'acteurs qualifiés de « cybercriminels de dimanche » pour désigner les adeptes des petites escroqueries numériques[154].

L'univers *Underground* a toujours laissé rêveur toute une génération d'adolescents en mal d'être. C'était une forme de rébellion et d'anticonformisme, par laquelle s'exprimait cette jeunesse. Ceux qui maitrisaient les techniques secrètes du monde du *hacking*, étaient sans équivoque les nouveaux maîtres. Incontestablement, les modèles étaient *Legion of Doom*[155], *Master of Deception* ou encore *Kevin Mitnick* alias *The Condor*, alors star montante de *l'Underground* américain et certainement d'autres chevaliers du côté obscur (*Marc Abene* alias *Phiber Optik*, *Kevin Poulsen* alias *Dark Dante*, *Vladimir Levin*)

A cette époque, internet n'était pas le moyen de communication sophistiqué que l'on connaît actuellement. Par conséquent, l'information était maîtrisée par une élite et il fallait beaucoup de compétences et d'ingéniosité pour contourner les systèmes de protection et de sécurité.

[154] Gaétan Pouliot, « Avec la crise, les cybercriminels du dimanche attaquent », http://www.rue89.com/2010/04/21/avec-la-crise-les-cybercriminels-du-dimanche-attaquent-148231?page=1

[155] http://en.wikipedia.org/wiki/Legion_of_Doom_%28hacking%29

1.1 Les acteurs de l'univers *Underground*

1.1.1 Le hacker

Le *Hacker* est utilisé pour désigner en informatique les programmeurs astucieux et débrouillards. Plus généralement, il désigne le possesseur d'une connaissance technique lui permettant de modifier un objet ou un mécanisme pour lui faire faire autre chose que ce qui était initialement prévu. Utilisé souvent à tort et à travers, il devient de plus en plus difficile de trier le bon grain de l'ivraie dans la masse exponentielle des informations sans cesse disponibles dans les différents médias sur le sujet.

Dans l'univers de la cybercriminalité, le *hacker* est souvent utilisé pour désigner un pirate informatique. De ce fait, il est souvent assimilé à l'auteur de la fraude informatique. Ce qui n'est pas toujours le cas. De nombreux *hackers* ont choisi la voie de « la sagesse » en évitant de déployer leurs compétences pour nuire. Nous parlons alors dans ce cas de « *white hat hackers* ». Le but recherché par cette catégorie de *hackers* est d'aider à l'amélioration des systèmes et technologies informatiques. De part leurs connaissances avancées dans divers domaines, ils découvrent souvent de nouvelles vulnérabilités à différents niveaux (réseau, système, application…), mais ces découvertes ne sont pas exploitées.

Dans sa signification largement adoptée par les médias et diffusée auprès du grand public, le terme fait surtout référence aux "*black hats*" ou chapeaux noirs.

1.1.2 Les black hat hackers

La communauté des *hackers* est représenté aussi par les « *black hat hackers* », plus couramment appelés pirates, c'est-à-dire des personnes s'introduisant dans les systèmes informatiques à des fins malveillantes. Ils peuvent détruire ou dérober des données, attaquer d'autres systèmes, ou effectuer tout autre acte nuisible. Rappelons par ailleurs que si à l'origine le *hacker* qui pénètre par effraction dans des systèmes ou des réseaux avait un objectif personnel, aujourd'hui derrière ces actes malveillants, il y a l'appât du gain.

Créateurs de virus, cyber-escrocs ou espions, leurs actions sont motivées par le profit, la destruction ou toute action qualifiée de néfaste. Cependant, tomber du côté obscur n'interdit pas de changer ultérieurement de profil pour devenir en quelque sorte un repenti. Celui-ci ne manque souvent pas d'intéresser les firmes spécialisées dans la sécurité. Une reconversion en tant que consultant est courante. *Kevin Mitnick* ou *Kevin Poulsen* sont deux exemples de pirates ayant rejoint le clan des *white hats*.

En réalité, cette distinction n'est bien évidemment pas aussi nette, dans la mesure où certains *white hat hackers* ont parfois été *black hat hackers* auparavant et parfois inversement. Les habitués des listes de diffusion et des forums voient souvent des sujets à propos de la différence qu'il convient de faire entre pirate et *hacker*.

1.1.3 Les « script kiddies »

Les « *script kiddies* » sont de jeunes utilisateurs du réseau utilisant des programmes trouvés sur l'internet, généralement de façon maladroite, pour vandaliser des systèmes informatiques afin de s'amuser. Souvent peu compétents, ils se contentent d'utiliser des outils d'exploitation automatique à la recherche souvent aléatoire de machines potentiellement vulnérables[156].

Malgré leur niveau de qualification faible, les *script kiddies* sont parfois une menace réelle pour la sécurité des systèmes. En effet, autre le fait qu'ils peuvent par incompétence altérer quelque chose sans le vouloir ou le savoir, d'une part les *script kiddies* sont très nombreux, et d'autre part ils sont souvent obstinés au point de passer parfois plusieurs jours à essayer toutes les combinaisons possibles d'un mot de passe, avec le risque d'y parvenir bien que souvent, c'est le *script kiddie* lui-même qui se fait infecter[157].

Il existe plusieurs types de *script kiddies,* mais ils sont généralement reniés par la plupart des communautés de pirates.

1.1.4 Les phreakers

Le mot anglais *phreaking* est obtenu par la contraction de *phone* et *freak*, le terme *freak* signifiant « marginal », ou personne appartenant à une contre-culture. Le pirate téléphonique est appelé un *phreaker*. La plupart des premiers pirates étaient des *phreakers*. Ces derniers se sont apparus avant l'invention de l'ordinateur et bien avant celle du réseau de l'internet.

Dans certains cas, le *phreaker* peut utiliser le réseau téléphonique d'une manière non prévue par l'opérateur afin d'accéder à des fonctions spéciales, principalement afin de ne pas payer la communication et de rester anonyme. Toutefois, les premiers *phreakers*, et un certain

---

[156] Christophe CASALEGNO, « Carnet de route d'un *Hacker* »,
http://www.christophe-casalegno.com/2007/01/30/hackers-crackers-consultants-securite-qui-sont-ils-vraiment/

[157] http://fr.wikipedia.org/wiki/Script_kiddie

nombre de *phreakers* actuels, sont des passionnés cherchant à effectuer une prouesse technique sans mauvaises intentions[158].

1.1.5 Les carders

Les *carders* s'attaquent principalement aux systèmes de cartes bancaires pour en comprendre le fonctionnement et en exploiter les failles. Le terme *carding* désigne le piratage de cartes bancaires. D'après une étude réalisée par *Actimize*, un spécialiste de la conformité dans le domaine du secteur financier, le *carding* devient un métier qui rapporte gros[159].

1.1.6 Les crackers

Un *cracker* - on trouve aussi parfois le terme de craqueur, casseur et déplombeur - est une sorte de pirate informatique spécialisé dans le cassage des protections dites de sécurité des logiciels, notamment les partagiciels (qui nécessitent des clés d'enregistrement). Un *crack* est ainsi un programme chargé de modifier le logiciel original afin d'en supprimer les protections. Un bon *cracker* écrira aussi ses propres programmes pour s'en servir comme outils dans son activité. Ces outils peuvent être génériques ou spécifiques au programme à « *cracker*[160] ».

Mener des opérations de *cracking* ne se limite pas à l'attaque ni à l'étude de logiciels, mais nécessite souvent des connaissances en cryptographie, domaine dans lequel leurs connaissances mathématiques et informatiques font de certains *crackers* d'excellents casseurs de code.

1.1.7 Les hacktivistes

Le *hacktivisme* est une contraction de *hacker* et activisme que l'on peut traduire en cybermilitantisme ou cyberrésistance. Un *hacktiviste* est donc un *hacker* mettant son talent au service de ses convictions idéologiques allant jusqu'à infiltrer les réseaux et organiser des opérations de piratages, de détournements de serveurs et remplacement de pages d'accueil par des tracts reflétant ses positions idéologiques. Ce sont des actions qui peuvent prendre la forme de désobéissance civile.

---

158 http://fr.wikipedia.org/wiki/Phreaking

159 http://www.actimize.com/index.aspx?page=news196

160 http://fr.wikipedia.org/wiki/Cracker_(d%C3%A9plombeur_de_logiciels)

Il existe plusieurs types d'*hacktivistes*; la plupart sont des personnes qui défendent leurs idées en défaçant des sites contraires à leur éthique. Ils peuvent aussi faire des *Google Bombings*[161] ou des chaînes de mails pour essayer de faire passer un message par la voix de la cyber-information.

1.2 Quelques mythes entourant l'univers *Underground*

L'univers *Underground* a fortement évolué dans le temps. Le profil de ses acteurs n'est plus le même. Leurs motivations encore moins. Quand nous analysons très finement les caractéristiques de cet univers, nous nous rendons compte que de nombreux mythes sont en train de tomber.

1.2.1 Le cyberdélinquant est-il un expert informatique ?

Dans l'imaginaire collectif, en raison notamment de la surmédiatisation dont bénéficie le phénomène de la délinquance numérique, le cyberdélinquant serait un expert informatique avec des compétences hors du commun. Cette affirmation n'est pas toujours vraie. En effet l'univers *Underground* est notamment composé par des *scripts kiddies* qui appliquent machinalement et méthodiquement les instructions que les experts de *reverse engineering* et en programmation ont mis en ligne. Ainsi, se réapproprient-ils les outils développés par les *hackers* pour les utiliser à des fins malveillantes[162].

Aujourd'hui, grâce notamment à la vulgarisation des modes opératoires des attaques, de nombreux tutoriels très pédagogiques et suffisamment explicites sont accessibles sur le web. Ils permettent ainsi aux profanes de perpétrer des attaques qui étaient jusqu'à une date récente réservées aux experts en informatique. Il en résulte qu'un cyberdélinquant n'a pas vraiment besoin d'une très bonne expertise en informatique pour se faire une place dans l'univers *Underground.* Il suffit d'être motivé.

1.2.2 Le cyberdélinquant est-il quelqu'un d'organisé ?

Contrairement à ce que nous pensons, le cyberdélinquant ne serait pas toujours quelqu'un qui agit d'une façon hasardeuse et désorganisée. La complexité des systèmes et réseaux informatiques est telle qu'aujourd'hui une personne à elle seule ne peut développer de

[161] Le bombardement Google (*Google bombing* en anglais) est une technique de référencement visant à influencer le classement d'une page dans les résultats du moteur de recherche Google.

[162] Franck Franchin et Rodolphe Monnet, « Le business de la cybercriminalité », Edition LAVOISIER, 2005

l'expertise dans tous les domaines informatiques. Le recours à d'autres acteurs de l'univers *Underground* est inévitable pour mener à bien une opération cybercriminelle. Dés lors, les compétences deviennent de plus en plus segmentées et ciblées. D'où la tendance vers la spécialisation et l'organisation de l'activité déviante dans le cyberespace. La création, la diffusion et l'utilisation des programmes malveillants sont réalisées par des groupes différents.

L'univers *Underground* est davantage organisé aujourd'hui en « réseau » d'opportunités, relations basées sur l'achat-vente de prestations et de données personnelles volées en échange de l'argent. Un tel réseau ne possède donc pas de hiérarchie fixe, et ne présente que des relations hiérarchiques ponctuelles et temporaires de « client-marchand » et/ou « prestataire-commanditaire »[163].

1.2.3 Le cyberdélinquant est-il un introverti ?

Ce mythe consiste à faire du cyberdélinquant un acteur isolé antisocial et qui ne trouve pas son compte dans l'interaction avec les autres. Ici encore, ce mythe est controversé par la réalité. Il n'est autre que la conséquence de l'image véhiculée par les médias. En effet, dans le système de valeurs qui régit l'univers *Underground,* la cohésion demeure une valeur très prisée. Elle est la base même de l'idée de l'équipe *Underground*. Ce qui exige une certaine ouverture d'esprit à l'égard des autres. En outre, les différentes techniques de récupération de l'information sensible, notamment la technique de l'ingénierie sociale, qui serviront de base d'attaques à posteriori, supposent des qualités personnelles autres que celles de l'introversion et de l'isolement. Par ailleurs, les acteurs de l'univers *Underground* tendent de plus en plus à se rassembler physiquement notamment lors des conférences internationales dédiées à leurs activités[164]. C'est le cas par exemple de *Defcon hacking conference*[165] qui se tient chaque année à Las Vegas ou encore de *Chaos Computer Club*[166] qui se tient en Allemagne.

---

[163] Idem

[164] « Hackers : quand les jeunes loups se rassemblent en meute organisée »
http://techno.branchez-vous.com/actualite/2009/07/hackers_quand_les_jeunes_loups.html

[165] http://www.defcon.org/

[166] Le Chaos Computer Club, que l'on désigne souvent par l'acronyme CCC, est l'une des organisations de hackers les plus influentes en Europe.

1.3 Les principales motivations des acteurs de l'univers *Underground*

Bien qu'ils appartiennent tous à une sous culture où la légitimité des normes violées est souvent remise en cause, les acteurs de l'univers *Underground* ne disposent pas du même référentiel idéologique. Par conséquent, les sources de motivation ne seront pas les mêmes d'un acteur à l'autre. En effet, si le *white hat hacker* est animé notamment par la curiosité intellectuelle en mettant à l'épreuve des technologies jusqu'à leurs limites afin de tendre vers un idéal plus performant, *le black hat hacker* trouve sa source de motivation dans la vengeance, l'intérêt de renommée et l'appât du gain financier.

1.3.1 La curiosité intellectuelle

La soif de la connaissance et le désir d'explorer de nouvelles compétences sont à l'origine de l'apparition du phénomène de *hacking*. L'intrusion sur les réseaux et le détournement des systèmes ne sont que l'incarnation de cette curiosité intellectuelle qui développe chez un certain nombre d'acteurs de l'univers *Underground*, notamment les *white hat hackers,* cette capacité à résister à toute épreuve. Cette caractéristique les conduit à consacrer énormément de temps et d'effort pour l'exploration des limites des systèmes ciblés.

Bien que, souvent la barrière de la légalité est vite franchie, l'objectif n'est pas en premier lieu l'illégalité. Il s'agirait plus de dépasser les limites, que ce soient celles imposées par la société ou celles que l'on se pose soi-même pour diverses raisons[167]. Cette recherche perpétuelle d'un idéal technologique sans failles est une valeur fondamentale dans l'univers de *hacking*. La curiosité intellectuelle justifie même pour de nombreux acteurs de l'univers *Underground* le passage à l'acte de déviance dans le cyberespace. Cette attitude renvoie souvent au célèbre texte du *Mentor* « la Conscience d'un *hacker* » daté de 1986 : "Nous recherchons la connaissance... et vous nous appelez criminels. Oui, je suis un criminel. Mon crime est celui de la curiosité. Je suis un *hacker,* et ceci est mon manifeste...[168]"

1.3.2 L'Ego

Une bonne partie de la motivation d'un *hacker* vient de son ego ou de la recherche d'une acceptation externe. Derrière cette motivation, il y a ce que les anthropologues appellent une culture du don. En effet, les *hackers* donnent pour partager mais aussi pour satisfaire leur égo et valoriser leurs créations. On obtient ainsi un statut ou une réputation et on arrive à

[167] Franck Franchin et Rodolphe Monnet, « Le business de la cybercriminalité », Edition LAVOISIER, 2005

[168] Observatoire d'informatique libre québécois. http://oilq.org/fr/node/5247

satisfaire son ego, non pas en dominant les autres ou en possédant des choses que les autres désirent, mais en faisant des dons : de son temps, de sa créativité, du résultat de ses compétences. Ainsi, lorsqu'un *hacker* distribue son code source, il attend un retour de la part de ses pairs et espère asseoir sa réputation. Par ses contributions, il cherche à étendre sa renommée et à satisfaire son ego.

Ces dernières années, cette motivation basée sur l'ego tend à disparaître derrière des motivations purement financières.

1.3.3 L'idéologie

L'adhésion à des thèses idéologiques et/ou politiques fondées sur la recherche d'intérêts affectifs ou symboliques oriente aussi les actions de certains acteurs de l'univers *Underground*. Elle sert souvent de prétexte pour perpétrer des actions de déviance dans le cyberespace[169]. L'un des exemples marquants à ce jour reste celui des *Anonymous*[170]. En effet, en 2008, le groupe s'est fait connaître notamment en lançant la guerre contre l'église de scientologie. Ainsi, ils ont réussi à organiser des dizaines de manifestations simultanées regroupant plusieurs centaines de personnes dans le monde entier. Par ailleurs, ils ont piraté de nombreux sites de la secte en usant du savoir-faire de leurs membres, *hackers* pour la plupart. Plus récemment le groupe a constitué avec les membres de « *The pirate bay* », le groupe "*Anonymous Iran*", un mouvement d'opposition au régime iranien après la réélection de Mahmoud Ahmadinejad.

Au Maroc, de nombreux actes déviants dans le cyberespace, motivées par des considérations religieuses, idéologiques et politiques ont été recensés ces dernières années. Voici quelques exemples :

- ✓ Juin 2006 : En signe de protestation contre la guerre menée par l'armée israélienne à Gaza, un groupe de *hackers* marocains appelé « *Team Evil* » a lancé une attaque d'envergure pour le défacement des sites web israéliens. Ainsi, plus de 850 sites ont été défacés pendant quelques heures. Sur les sites piratés, le groupe a laissé le message suivant : « site piraté par le groupe arabe 'Team Evil'. Tant que vous tuerez

[169] Franck Franchin et Rodolphe Monnet, « Le business de la cybercriminalité », Edition LAVOISIER, 2005

[170] Groupe de web-activistes, aux méthodes parfois contestées, sans pour autant tomber dans l'illégalité, ils militent pour une totale liberté d'expression sur internet.

des Palestiniens nous tuerons vos serveurs »[171]. L'attaque était d'une telle médiatisation que certains experts commencent à parler de *Webtifada*.

- ✓ Avril 2009 : Le site web de l'association dénommée « Kif Kif » regroupant les homosexuels marocains a été défacé par un *hacker* marocain du nom « ibn Al Walid ». Sur la page d'accueil, le *hacker* a diffusé quelques versets du coran incitant au meurtre des homosexuels, ainsi qu'une image de pendaison collective.

Ces attaques montrent bien que le *hacktivisme* marocain est une réalité avec laquelle il faudra désormais se composer. Le cyberespace devient ainsi une extension virtuelle d'affrontement religieux, idéologique et politique.

1.3.4 L'argent

Si à l'origine les acteurs de l'univers *Underground* trouvaient leurs motivations dans l'égo, la curiosité intellectuelle, la recherche de l'estime et de la reconnaissance et le *hacktivisme*, aujourd'hui, il semblerait que les actes de déviance dans le cyberespace sont de plus en plus orientés vers l'appât du gain. Il s'agit d'un phénomène récent qui commence à prendre de l'ampleur. Ainsi, les opérations ayant comme finalité la recherche du profit sont désormais monnaie courante. Le développement des phénomènes d'extorsions par déni de service distribué (*DDoS*) et des arnaques bancaires avec le *phishing* est une illustration parfaite de la monétisation des actes cybercriminels. D'après une étude réalisée en 2008 par le *Web Hacking Incidents Database*[172], les motivations des pirates restent la recherche du profit, même si dans 24% des cas l'attaque a été menée dans le but de défacer un site[173]. Ce n'est pas par hasard qu'aujourd'hui la plupart des attaques sont orientées vers la perspective de récupérations de données critiques. Selon *Symantec*, 24% des demandes des « clients » des pirates porteraient en effet sur des informations relatives à des comptes bancaires. Les cybercriminels s'en servent pour obtenir des emprunts, se procurer des traitements médicaux ou pharmaceutiques, voire même voler des titres immobiliers. Le rapport de

[171] Rachid Jankari, « Des hackers marocains immobilisent le web israélien » Juin 2006 http://www.protection-palestine.org/spip.php?article2952

[172] http://www.xiom.com/whid

[173] http://www.journaldunet.com/solutions/securite/actualite/30-d-attaques-par-injection-sql-en-2008/l-interet-financier-avant-tout.shtml

l'éditeur décrit une véritable économie planétaire du *cybercrime*. Ces activités frauduleuses pourraient générer sept milliards de dollars de revenus par an[174].

Il en résulte, qu'aujourd'hui la cybercriminalité exerce une attractivité telle que de nombreux acteurs de l'univers *Underground* n'hésitent pas à abandonner les simples opérations dont la motivation est l'égo, la curiosité intellectuelle, la recherche de l'estime ou le *hacktivisme* pour se diriger vers une véritable monétisation de leurs actes.

Témoignage sur l'*Underground* marocain

L'existence d'un mythique *Underground* marocain n'a été révélée au public que vers la fin des années 90. Cette décennie rimait cyniquement avec la première attaque web dite de "*defacement*". L'annonce a fait l'effet d'une bombe puisqu'il s'agissait du serveur d'une institution publique. Le Maroc tenait ici son premier chevalier de l'*Underground* un certain *Netoperat*. Le mode opératoire fût simple : un cybercafé alors fief des bidouilleurs et autres récalcitrants numériques, une connexion internet et un réseau marocain fragile et faillible à tous les niveaux.

Je me souviens qu'à cette période j'avais réalisé un audit de sécurité sur le réseau marocain par simple curiosité. Le résultat était ahurissant. La composante sécurité n'était pas à l'ordre du jour. Mon rapport, envoyé dans la foulée à plusieurs institutions publiques et privées, est resté sans réponse. Aucune suite n'a été donnée à mes recommandations. Affaire classée et sujet tabou. Les piratages se sont par ailleurs accentués dans la plus grande impunité.

Le destin très particulièrement impressionnant d'un *hacker* marocain a attiré toute mon attention. Au fait, il s'agissait de l'unique *hacker* ayant des compétences hors normes et donc capable de s'introduire même sur les réseaux téléphoniques (*phreaking*).

Il avait su tirer profit de ses compétences pour gagner le respect et la confiance de ses acolytes américains et européens. Il fût le premier *hacker* marocain à se rendre à des manifestations sur le *hacking*.

Ce *hacker* marocain était le « mentor » d'une poignée triée sur le volet de quelques pirates

[174] Rapport de l'éditeur Symantec sur l'économie souterraine, Novembre 2008 http://www.symantec.com/fr/fr/business/theme.jsp?themeid=threatreport

informatiques qui allaient faire trembler les sites informatiques des plus grandes entreprises dans le monde.

Face à l'absence totale de lois contre la délinquance informatique, les attaques se sont renforcées plaçant le Maroc dans la liste des pays à haut risque. Les fondements et les bases même de l'éthique « *Hacker* » ont été transgressés et la montée fulgurante des « script kiddies » a poussé le « mentor » des *hackers* marocain à se retirer définitivement de la scène du *hacking*. Plusieurs de ses disciples ont fait de même. L'esprit *Underground* marocain est bel et bien terminé. Aujourd'hui approchant la quarantaine, le « mentor » mène une vie paisible en compagnie de sa femme et de ses enfants quelque part en Europe. Il continue à exercer son métier de consultant en sécurité informatique dans une multinationale.

2. Les éditeurs, constructeurs, intégrateurs, distributeurs, cabinets conseils, hébergeurs et les cybercafés.

2.1 Les éditeurs et les constructeurs

Le marché mondial des solutions de sécurité est un marché qui évolue très vite. Avec un taux de croissance estimé en 2008 à 18%[175] qui s'explique notamment par le regain de l'investissement des PME en la matière, mais également par les obligations légales auxquelles sont soumises de nombreuses organisations, le marché des solutions de sécurité devrait atteindre en 2009 selon *Gartner* 14,5 milliards de dollars[176]. Ce marché met en scène plusieurs acteurs et peut être découpé en trois domaines à la valeur ajoutée croissante :

- ✓ La sécurité opérationnelle (antivirus, firewall, encryptage de données)
- ✓ La sécurité transactionnelle (authentification PKI, biométrie, smartcard)
- ✓ La sécurité administrative (contrôle d'accès au réseau, scanning de mail, gestion d'intrusions ...).

[175] « Le marché mondial des logiciels de sécurité a le vent en poupe », Gartner http://www.itespresso.fr/le-marche-mondial-des-logiciels-de-securite-a-le-vent-en-poupe-31525.html

[176] Idem

Gartner note également l'importante activité de croissance externe menée par des acteurs d'envergure du marché de la sécurité *IT* en 2008, aboutissant ainsi à un "haut niveau de consolidation dans ce secteur", à travers l'acquisition notamment de *Secure Computing* et de *Solidcore* par *McAfee*, et les rachats par *Sophos* d'*Ultimaco* et de *MessageLabs* par *Symantec*[177].

Au Maroc, une poignée de constructeurs et éditeurs de solutions de sécurité informatique dont les ventes sont en majorité tirées par les besoins des opérateurs télécoms et du secteur de la banque-finance, se partagent ainsi cette niche de marché. *Cisco, Blue Coat Systems, Websense, Kaspersky, Symantec, McAfee, Trend Micro, Juniper Networks, Checkpoint* en sont les principaux protagonistes. Le Maroc reste un pur consommateur des solutions de sécurité. En effet, si le domaine de la monétique est représenté par des acteurs marocains présents à l'international, tels que *HPS, S2M et M2M,* il n'existe aujourd'hui aucun acteur marocain opérant dans le développement des solutions de sécurité si on excepte quelques projets qui rentrent dans le cadre de *l'offshoring.* Face à cette situation, il est extrêmement urgent pour le gouvernement marocain d'encourager la naissance d'une industrie locale non seulement pour pouvoir générer de l'emploi hautement qualifié, mais surtout pour ne pas laisser la sécurité d'institutions critiques entre les mains des étrangers.

2.2 Les intégrateurs et les distributeurs

Pour adresser le marché marocain, les différents constructeurs et éditeurs de solutions de sécurité s'appuient sur des distributeurs et/ou des intégrateurs locaux, qui revendent leurs solutions de sécurité clés en main aux clients finaux, opérateurs télécoms, banques, organismes financiers, mais aussi administrations et industrie[178]. Il s'agit généralement des sociétés à capitaux locaux ou étrangers qui offrent les services d'intégration de solutions de sécurité chez les clients finaux. *CBI, IB Maroc, Intelcom,* sont quelques exemples d'intégrateurs de solutions de sécurité. Sur le volet de distribution, *Config, Exclusive Networks, Logix Maroc, Feeder Informatique* et *Afina* sont les principaux acteurs de distribution de solutions de sécurité sur le marché marocain.

Rappelons par ailleurs, que les clients marocains ont tendance, sur des sujets pointus de sécurité, de recourir directement aux intégrateurs étrangers. Ceci s'explique notamment par

[177] Idem

[178] Sylvaine LUCKX « Le marché de la sécurité informatique en Afrique dominé par les américains », Mag Securs, 2009 ? http://www.mag-securs.com/spip.php?article14567

l'absence des références locales et le manque de compétences en la matière. Ainsi, par exemple les projets liés à la mise en place de solutions de gestion des identités, des sites de repli et à la mise en place des solutions de gestion des risques opérationnels et de lutte contre le blanchiment d'argent sont souvent pris en charge par des acteurs étrangers.

2.3 Les cabinets conseil

Si l'intégration des solutions de sécurité est plus ou moins bien prise en charge par un certain nombre d'acteurs marocains, les missions de conseil en sécurité sont généralement confiées aux prestataires étrangers. Ainsi par exemple toutes les missions de mise en place de plan de continuité d'activités chez les banques marocaines ont été confiées aux acteurs étrangers notamment français ayant plus de retour d'expérience en la matière. C'est le cas aussi pour les projets liés à la conformité aux normes et standards internationaux tels que *PCI DSS*, *Bâle II* et *SOX* qui ont été pris en charge dans la majorité des cas par des prestataires étrangers tels que *Devoteam, Capgemini, Accenture, Symantec et BT Net2S*.

De l'analyse des risques jusqu'aux audits de sécurité en passant par la mise en place des politiques et des référentiels de sécurité tels que *ISO 27001*, l'offre des prestataires marocains reste très timide. Ceci s'explique notamment par le manque et la volatilité des ressources certifiées en la matière. Toutefois, nous assistons aujourd'hui à l'émergence d'acteurs locaux qui n'ont rien à envier à leurs homologues étrangers. Ainsi, des sociétés comme *Dataprotect ou Netpeas sont* de plus en plus présentes sur le marché des audits de sécurité, des tests d'intrusion et de l'accompagnement à la certification *PCI DSS.*

2.4 Les hébergeurs

Toute opération cybercriminelle s'appuie, à un moment ou à un autre, sur une plateforme d'hébergement. Le choix d'un mode d'hébergement va être déterminant dans le succès ou l'échec d'un acte cybercriminel. Le recours aux hébergeurs dits « *bulletproof* » ou « par-balles » figure parmi les solutions les plus envisageables. Ce mode d'hébergement a favorisé l'émergence de véritables paradis cybercriminels dans lesquels un malfaiteur peut héberger des serveurs et des contenus illicites en toute impunité.

2.4.1 Le recours aux hébergeurs dits bulletproof

Les hébergeurs *bulletproof* offrent des services d'hébergement classique, tout en garantissant à leurs clients un anonymat total et une qualité de service maximale. La

professionnalisation dont bénéficie cette pratique a incité de nombreux cybercriminels à abandonner le recours aux serveurs piratés de façon opportune au profit d'un véritable marché de location de machines dédiées. Des sociétés commerciales proposent désormais des services d'hébergement dévoués au *spamming,* au lancement des compagnes de *phishing*, au stockage des codes malicieux et des données volées, et à l'utilisation des serveurs de commande de *botnets.* Ces sociétés garantissent à leur client la continuité du service même quand elles reçoivent des plaintes officielles. Les mieux organisées disposent même de leur propre infrastructure d'hébergement. Elles sont gérées comme de véritables entreprises, disposant souvent d'une existence légale, de leur propre *datacenter*, et d'un site web assurant la promotion de leurs services. Parmi les organisations qui ont le plus fait parler d'elles, nous retenons *Russian Business Network (RBN)*[179]*.* Cette organisation est devenue tellement puissante que certains rumeurs laissent même entendre qu'elle entretienne des relations étroites avec le gouvernement russe[180].

Avec un million de sites, plusieurs millions d'adresses *IP* disponibles et quatre millions de visiteurs par mois, *RBN* disposait d'une activité très lucrative[181]. Toutefois, les articles fréquents dans la presse sur la possible implication de *RBN* dans tous les incidents criminels survenus sur l'internet ont poussé les propriétaires inconnus de *RBN* à scinder leur activité et à créer plusieurs sociétés d'hébergement autonomes à travers le monde, depuis Singapour jusqu'à l'Ukraine et à réaliser leurs activités de manière un peu plus discrète avec la complicité souvent des autres hébergeurs. C'est le cas de la société *SecureHosting*[182]basée au *Bahamas* qui a été suspectée d'avoir soutenu *RBN* en hébergeant certains de leurs serveurs. Le site web de cette société *offshore* annonce la couleur dans leurs conditions d'utilisation: « L'internet n'appartient à personne. Ainsi, nous ne pouvons pas nous permettre de surveiller ou de censurer l'internet et nous ne le ferons pas. Nous ne pouvons pas assumer la responsabilité pour des activités de nos clients, qu'il s'agisse de publication d'un contenu offensant ou illégal »[183].

---

[179] La revue MISC, « Dossier spécial cybercriminalité », Janvier 2009.

[180] François PAGET « Fraude financière et opérations bancaires en ligne : menaces et contre-mesures », McAfee Avert Labs
http://www.mcafee.com/us/local_content/reports/6168rpt_fraud_0409_fr.pdf

[181] VeriSign, « *Uncovering Online Fraud Rings: The Russian Business Network* » (Les réseaux de fraudes en ligne dévoilés : le réseau russe *Russian Business Network*), séminaire web. *http://www.verisign.com*

[182] http://www.securehost.com

[183] L'actu Sécu « Le coté obscure de l'Internet », Janvier 2008
http://www.xmcopartners.com/actu-secu/XMCO-ActuSecu-Janvier2008.pdf

Avec la disparition de *RBN*, les soupçons se sont rapidement tournés vers trois fournisseurs d'accès Internet : d'abord *Abdallah Internet Hizmetleri*[184] (Turquie) et ensuite *Atrivo*[185] et *EstDomains*[186] (Etats-Unis).

2.5 Le cybercafé

Selon l'Agence Nationale de Réglementation des Télécommunications (ANRT), le recours au cybercafé représente un taux d'utilisation de 84% quand il s'agit de connexion internet hors domicile au Maroc[187]. Il demeure donc un lieu hautement sollicité par les internautes marocains. Bien que les demandes de création de cybercafés n'aient pas cessé de baisser ces dernières années en raison notamment des offres *ADSL* et *3G* qui continuent à séduire de plus en plus d'internautes[188], le cybercafé continue de jouer un rôle important dans le paysage de l'internet au Maroc. Pour les acteurs de l'univers *Underground*, il constitue un lieu privilégié, en raison de l'anonymat qu'il procure, pour naviguer, échanger et mettre en œuvre des actions déviantes dans le *cyberespace*. Ainsi, le cybercafé s'est retrouvé à maintes reprises à l'une de l'actualité au Maroc. C'est le cas par exemple de Farid Essebar qui a participé à la création et à la diffusion du vers *Zotob*[189] en opérant à partir d'un cybercafé basé à Rabat et du Kamikaze qui a perpétré un attentat à l'explosif dans un cybercafé situé à Casablanca lui servant d'un lieu d'échanges et de communications avec les réseaux terroristes[190].

Compte tenu du rôle que peut jouer le cybercafé, qui rappelons-le a été longtemps considéré comme une zone de non droit, dans l'univers de la cybercriminalité, plusieurs pays ont

---

[184] *The Shadowserver Foundation* « *RBN 'Rizing': Abdallah Internet Hizmetleri (AIH)* »
http://digitalninjitsu.com/downloads/RBN_Rizing.pdf

[185] Jart Armin « *Atrivo - Cyber Crime USA* »
http://hostexploit.com/downloads/Atrivo%20white%20paper%20090308ad.pdf

[186] Washington Post, « *EstDomains: A Sordid History and a Storied CEO* »
http://voices.washingtonpost.com/securityfix/2008/09/estdomains_a_sordid_history_an.html

[187] « Le marché des Technologies de l'information : Enquête 2008», ANRT
http://www.anrt.ma/fr/admin/download/upload/file_fr1680.pdf

[188] « Les cybercafés dans la tourmente », La vie économique 11/05/2007
http://www.lavieeco.com/economie/2544-les-cybercafes-dans-la-tourmente.html

[189] « Sophos : Les auteurs du ver Zotob condamnés à des peines de prison » Mag Securs, Septembre 2006
http://www.mag-securs.com/spip.php?article5743

[190] Nadia Lamlili et Abdellatif El Azizi, « Terrorisme. Le retour de la peur », Tel Quel
http://www.telquel-online.com/265/couverture_265_1.shtml

adopté des lois permettant de mieux surveiller les activités déviantes dans ces lieux. Ainsi, par exemple en France, la loi anti-terrorisme de 2006 oblige les cybercafés à conserver à la disposition des autorités judiciaires les données de connexion pendant un an[191]. Il a été même question de faire étendre cette mesure vers les bornes d'accès *Wifi*, aux éditeurs de messagerie électronique et aux points d'accès dans les lieux publics[192].

3. Les centres de recherche et de formation

3.1 La recherche

Par définition, l'industrie de la sécurité de l'information est liée à la recherche et au développement. Si aujourd'hui, les géants de l'industrie arrivent à percer à l'international, c'est tout simplement parce qu'ils injectent une somme colossale dans la recherche et le développement. L'innovation dans ce domaine est une exigence pour survivre. En effet, si à l'origine la sécurité des grands systèmes d'information (architecture centralisée) n'était pas un enjeu important puisqu'ils fonctionnaient dans des environnements fermés, aujourd'hui, en raison notamment de l'ouverture des systèmes (architecture distribuée), la sécurité de l'information a pris de l'importance. Elle a déplacé la sécurité vers l'utilisateur final. Quiconque utilise un micro-ordinateur et a accès à l'internet est devenu vulnérable aux virus, aux *spam* et à toutes les formes d'intrusion mal intentionnées. C'est pour répondre à cette nouvelle demande en sécurité que l'industrie de la sécurité est en passe d'injecter des sommes importantes en recherche et développement.

Autre la recherche et le développement dans le domaine de la sécurité de l'information engagée par les industriels, les universités et les armées s'y intéressent aussi de plus prés. D'ailleurs de nombreuses entreprises « *Start-Up* » ont vu le jour en tant que «*Spin-off*[193] » dans le milieu universitaire et de l'armée. Le rôle joué par l'université dans l'innovation n'est plus à démonter. Aux Etats-Unis par exemple, plus de 70% de tous les brevets sont basés sur des résultats universitaires[194].

---

[191] Michèle Alliot-Marie, « Se donner les moyens de faire face au défi de la cybercriminalité », Problèmes économiques et sociaux, L a délinquance électronique, Octobre 2008, N°953.

[192] Idem

[193] Par société spin-off, on entend une entreprise créée en aval d'un service universitaire pour assurer la valorisation industrielle ou commerciale de l'expertise ou de résultats de recherche disponibles au sein de l'Université.

[194] Source *: National Science Foundation (NSF)* http://www.nsf.gov/

Au Maroc, l'université est complètement déconnectée de la recherche scientifique à vocation industrielle. Une étude récente, coordonnée par le sociologue Mohamed Cherkaoui précise que plus de 55% des professeurs marocains n'ont jamais publié une seule ligne de leur carrière[195].

Pour pouvoir avancer sur le volet de la recherche à vocation industrielle, il faudra certainement se donner les moyens nécessaires à son développement, et surtout, il faudra que le secteur productif rime avec le secteur éducatif pour donner lieu à un véritable partenariat public-privé en la matière. Autrement, le Maroc continuera à être un pur consommateur des avancées technologiques dans le domaine de la sécurité de l'information.

3.2 La formation

3.2.1 L'enseignement académique

Nombreuses sont les organisations marocaines qui estiment que le manque de personnels qualifiés est un sérieux obstacle au renforcement de la sécurité de leurs SI. Certaines n'hésitent pas à aller chercher des compétences de l'autre coté de la Méditerranée. Cette pratique est justifiée notamment par le manque de formations supérieures dédiées à la sécurité. Les universités et les écoles des ingénieurs marocaines proposent au mieux quelques cours qui se limitent souvent à des introductions à la sécurité. L'offre de formation académique en sécurité est très pauvre comparativement à d'autres pays. Les candidats qui souhaitent développer des connaissances en matière de sécurité se voient contraints de postuler pour les universités et écoles étrangères notamment françaises. Face à ce manque d'intérêt par les écoles d'ingénieurs et les universités marocaines, quelques écoles privées proposent depuis peu, pour combler le vide, des Mastères en sécurité SI. Rappelons enfin que l'Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes (ENSIAS) a enrichi récemment son programme de formation pour y inclure désormais une option de sécurité des systèmes d'information[196].

3.2.2 Les certifications en sécurité

Au cours des dernières années, le métier de la sécurité a subi un mouvement de professionnalisation sans précédent. Des barrières à l'entrée sont de plus en plus exigées

[195] « Grande enquête. Le silence des intellectuels » tel Quel, Octobre 2009 http://www.telquel-online.com/393/couverture_393.shtml

[196] http://www.ensias.ma/

pour pouvoir exercer dans le domaine de la sécurité SI. Ainsi, par exemple pour mener des audits de sécurité de conformité à la norme *PCI DSS (Payment Card Industry Data Security Standard)*, il faut se doter d'une certification *PCI QSA (Payment Card Industry Qualified Security Assesor)*. Pour pouvoir exercer le métier de l'audit de SI dans des organismes publiques aux Etats-Unis, il faudra être certifié *CISA* (*Certified Information System Auditor*).

La professionnalisation du secteur de la sécurité SI a fait en sorte qu'aujourd'hui, les certifications en matière de la sécurité SI sont de plus en plus exigées et valorisées par le marché de l'emploi. Ainsi, dans de nombreux appels d'offres publiques, ces certifications sont exigées pour s'assurer de la bonne prestation.

Il existe actuellement de nombreuses certifications en matière de la sécurité. Nous retenons à titre d'exemple la liste suivante :

Certifications	Exigences	Organisme certificateur
CISA (Certified Information System Auditor)	✓ 5 ans d'expériences en audit SI. ✓ Examen écrit de 4 heures. ✓ Présentation du dossier.	ISACA http://www.isaca.org
CISM (Certified Information Security Manager)	✓ 5 années d'expérience dans les domaines du management de la sécurité. ✓ Examen écrit de 4 heures ✓ Présentation du dossier.	ISACA http://www.isaca.org
Lead Auditor ISO 27001	✓ Formation de 5 jours en ISO 27001 ✓ Examen écrit	LSTI http://www.lsti-certification.fr/ IRCA http://www.irca.org
CEH (Certified Ethical Hacker)	✓ Formation de 5 jours sur les différents modules CEH ✓ Examen écrit ✓ 2 ans d'expérience en matière de sécurité.	EC-COUNCIL http://www.eccouncil.org
PCI QSA (Payment Card Industry Qualified Security Assesor)	✓ Formation de 3 jours en PCI DSS ✓ Etre certifié CISA ou CISSP ✓ Réussir un examen de 4 heures ✓ Justifier d'une expérience de 5 ans en audit de sécurité	PCI Security Standards Council https://www.pcisecuritystandards.org
CISSP (Certified Information System Security Professional)	✓ Justifier de 4 ans de pratique de la sécurité des SI ✓ Examen écrit de 4 heures	ISC2 http://www.isc2.org

Autres les certifications métier, ils existent de nombreuses certifications produits. A titre d'exemples, les technologies comme *Cisco, Juniper, Checkpoint, RSA, PGP, Kaspersky,*

McAfee ou *Symantec* proposent des certifications liées à leurs solutions de sécurité afin de pouvoir valoriser la prestation d'intégration de ces solutions chez les clients.

4. Les organes institutionnels d'investigation, de répression et de veille

La lutte contre le phénomène de la cybercriminalité doit inévitablement déboucher sur la mise en place d'institutions étatiques. En effet, il appartient à l'Etat de droit de garantir la sécurité dans le cyberespace et d'établir la confiance numérique, seuls éléments capables de favoriser le développement des nouvelles économies basées sur la dématérialisation des relations et des échanges.

Il faut non seulement agir dans le sens de la répression, encore faut-il mieux comprendre le phénomène de la cybercriminalité en se dotant de structures adéquates ayant pour mission l'investigation et la veille.

4.1 L'investigation et la répression

Pour pouvoir apporter de bonnes réponses au phénomène de la cybercriminalité, il est extrêmement important pour l'Etat d'avoir une connaissance précise du phénomène. Cela suppose non seulement le recours à des outils statistiques fiables mais surtout une collaboration étroite entre les différentes organisations publiques et privées impliquées dans la lutte contre la cybercriminalité. En effet, l'investigation en matière de la cybercriminalité nécessite un travail d'ensemble. La police et la gendarmerie en sont les acteurs essentiels certes, mais ils ne sont pas les seuls. Les fournisseurs d'accès à l'internet et les cybercafés par exemple sont des acteurs qu'il faudra faire impliquer dans le travail d'investigation à travers une démarche de coopération structurée.

Mettre en place une approche structurée d'investigation et de répression en matière de cybercriminalité implique le recours à des organisations dédiées. De nombreux pays avancés en la matière ont mis en place des structures dédiées. C'est le cas par exemple de la France qui dispose aujourd'hui de nombreuses structures chargées de mener le travail d'investigation et de la répression en matière de la cybercriminalité. Le tableau ci-dessous regroupe les structures françaises impliquées dans ce travail[197].

[197] Source : le Club de la sécurité de l'information français, http://www.clusif.fr

Organisme	Mission	Territorialité	Domaine de compétences
La Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information (BEFTI)	BEFTI est un service opérationnel qui dépend de la Direction Régionale de la Police Judiciaire de Paris. Sa mission est triple : ✓ Elle est spécialisée dans les enquêtes en milieu informatique. ✓ Elle assiste tous les services enquêteurs qui la sollicitent dès lors qu'ils sont confrontés au numérique. ✓ Elle assure une mission de formation et de sensibilisation à la sécurité auprès des autres services de Police, des entreprises et diverses institutions.	La B.E.F.T.I est compétente sur Paris et les trois départements limitrophes (92, 93 et 94). Toutefois avec l'accord des Autorités Judiciaires, cette compétence peut être étendue à l'ensemble du territoire national.	La B.E.F.T.I. intervient principalement dans les affaires portant atteinte aux systèmes de communication (piratage informatique) mais également dans certains délits spécifiques (contrefaçon de logiciels ou de bases de données, infraction aux fichiers nominatifs, fraudes téléphoniques ou aux chaînes à péage...). D'une manière générale, elle n'enquête pas sur les infractions traditionnelles véhiculées par les réseaux, hormis le cas où le mode opératoire est particulièrement technique ou inédit

Organisme	Mission	Territorialité	Domaine de compétences
La Direction Centrale du Renseignement Intérieur (DCRI)	La DCRI est un service de renseignement de sécurité disposant de pouvoirs de police judiciaire spécialisée. Le décret n°2008-609 du 27 juin 2008 (publié au journal officiel du 28 juin 2008) définit les missions et l'organisation de la direction centrale du renseignement intérieur (DCRI), grand service de renseignement intérieur unique qui marque la disparition de la DST (direction de la surveillance du territoire) et des RG (Renseignements généraux). La DCRI a compétence pour rechercher et prévenir, sur le territoire de la République française, les activités inspirées, engagées ou soutenues par des puissances étrangères et de nature à menacer la sécurité du pays, et plus généralement, pour lutter contre ces activités. A ce titre, la DCRI exerce une mission se rapportant à la défense.	La Direction Centrale du Renseignement Intérieur est compétente sur tout le territoire national.	Concrètement, les missions de la DCRI sont traditionnellement de trois types : contre-espionnage, contre-terrorisme, protection du patrimoine économique et scientifique. De nouvelles menaces de niveau stratégique apparaissent et sont d'ores et déjà prises en compte, telles que la prolifération des armes nucléaires, bactériologiques, chimiques et balistiques ou la grande criminalité organisée

Organisme	Mission	Territorialité	Domaine de compétences
La gendarmerie nationale	La gendarmerie nationale est une des deux forces de police françaises. Elle dépend pour son administration du ministère de la défense et pour emploi du ministère de l'intérieur. Les enquêtes judiciaires sont menées sous le contrôle du ministère de la justice.	Les unités de gendarmerie nationale sont implantées sur l'ensemble du territoire français, en métropole et outre-mer. La gendarmerie est chargée de la sécurité publique en dehors des grandes villes, ce qui représente environ 95% du territoire national et 50% de la population.	Les personnels de la gendarmerie sont juridiquement compétents pour traiter de toute infraction, et notamment de toute atteinte à un système de traitement automatisé de données. Des enquêteurs spécialisés en technologies numériques (150 NTECH au 1er mai 2007) sont implantés sur l'ensemble du territoire. La gendarmerie participe aux activités de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de la DCPJ de la police nationale. C'est une des modalités de l'échange permanent d'information entre les deux institutions dans ce domaine.

Organisme	Mission	Territorialité	Domaine de compétences
L'Office Centrale de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC)	L'OCLCTIC est une structure nationale, à vocation interministérielle et opérationnelle, compétente dans le domaine des infractions aux technologies de l'information et de la communication. Outre sa vocation opérationnelle, l'O.C.L.C.T.I.C. intègre d'autres missions relatives à l'animation, à la coordination, l'assistance technique, la centralisation et la diffusion de l'information dans le domaine de la cybercriminalité. L'O.C.L.C.T.I.C. assure également la gestion des échanges internationaux (Interpol, Europol et G8H24) en tant que point de contact unique national dans son domaine d'activité.	L'O.C.L.C.T.I.C. est compétent sur l'ensemble du territoire national. La Direction Centrale de la Police Judiciaire dispose également sur l'ensemble de ses services territoriaux (Directions interrégionales et régionales de Police Judiciaire) d'un réseau d'Enquêteurs Spécialisés en Criminalité Informatique compétents pour diligenter des enquêtes dans leur ressort de compétence géographique.	L'OCLCTIC intervient sur des affaires d'envergure nationale et internationale dans le cadre d'enquêtes liées aux technologies de l'information et de la communication (ex : intrusion, entrave ou altération de systèmes informatiques, de contrefaçon de cartes de paiement, atteintes aux personnes et aux biens).

L'importance de ces structures en matière de collectes d'information sur le paysage cybercriminel est de taille. Cependant, leurs démarches se heurtent à une limite bien réelle. Il s'agit, du nombre de victimes qui ne se font pas connaître. Ce « chiffre noir » demeure important car de nombreuses victimes ne se font pas connaître, soit parce qu'elles n'ont pas pris conscience du préjudice subi, soit parce qu'elles craignent que la dénonciation auprès des services de police ou de gendarmerie ait des effets négatifs sur leur image (cas des entreprises victimes de piratage de leurs réseaux)[198].

Consciente des nouvelles menaces liées au cyberespace au Maroc, la Direction Générale de la Sûreté Nationale (DGSN) a mis en place une cellule de lutte contre la cybercriminalité. Cette nouvelle brigade au Maroc est « une police en charge de traquer les comportements et les agissements illicites sur les réseaux informatiques[199] ». Composée d'une dizaine d'experts dédiés, c'est à cette dernière cellule qu'on doit notamment la localisation et l'arrestation de Farid Essebar, jeune Marocain soupçonné d'avoir été derrière l'attaque "virale" contre plusieurs compagnies américaines[200].

L'existence d'une telle cellule est de nature à améliorer le travail d'investigation en matière cybercriminelle. Cependant, le Maroc ne dispose pas de structure dédiée à l'alerte et à l'assistance sur l'internet.

4.2 La veille et le signalement

Pour pouvoir veiller sur les contenus véhiculés par le cyberespace et détecter ceux que la loi interdit afin de déférer leurs auteurs devant la justice, les forces de l'ordre optent pour une double approche. La veille et le signalement.

4.2.1 La veille

La veille est un travail d'initiative qui a pour but de rechercher de manière proactive les infractions en surveillant l'espace public par les « patrouilles du Net ». C'est une forme de recherche de renseignements utiles à de futures enquêtes. La veille s'accompagne d'une liberté d'action et de réaction de l'enquêteur qui peut sélectionner les éléments qui méritent

[198] Solange Ghernaouti-Hélie, « La cybercriminalité : Le visible et l'invisible », collection le savoir suisse, Edition 2009

[199] Rabya Khallok, « Cybercriminalité : comment contrer le piratage informatique », http://www.jeunesdumaroc.com/article1027.html

[200] http://www.bladi.net/forum/50106-enquete-coeur-cyberpolice/

d'être travaillés, exploités. C'est une approche ciblée[201].

En France, cette veille est assurée notamment par les services de la police et de la gendarmerie. Plusieurs pôles de compétences sont impliqués dans ce travail. Il s'agit notamment du[202] :

- ✓ Pôle de veille de la police nationale qui est chargé de la veille des contenus à connotation raciste, antisémite ou xénophobe, de ceux liés au terrorisme et de ceux relatifs au piratage informatique ;
- ✓ Pôle de la gendarmerie nationale qui, quant à lui, est chargé de la veille des contenus pédopornographiques; des liens fonctionnels sont établis avec le Centre national d'analyse des images pédopornographiques et avec la base des sites pédopornographiques tenue par l'OCLCTIC.

Au Maroc, la veille en matière de cybercriminalité n'est pas assurée par un service dédié.

4.2.2 Le signalement

Le signalement émane d'une tierce personne, physique ou morale et s'impose à l'enquêteur qui doit, systématiquement, le vérifier, l'exploiter, dans une finalité judiciaire[203]. En France, le signalement est assuré par une plateforme située au sein de l'OCLCTIC. Lancée en 2008, la plate-forme de signalement, qui est accessible au public[204], a vu en début d'année 2009 son champ d'action s'étendre à l'ensemble des délits avec comme vecteur l'internet (escroqueries en ligne, la fraude en ligne, le cyberterrorisme...) et plus uniquement la corruption et la pédophilie en ligne[205].

Composée d'une équipe mixte de policiers et gendarmes, cette plateforme est considérée comme un point d'entrée national, unique et clairement identifié pour tout signalement des cyberdélits. A l'échelle européenne, un dispositif commun de signalement a été mis en place. Il s'agit d'une plateforme européenne de signalement qui est hébergée par *Europol*[206]. Le Maroc, partenaire européen de référence, a été choisi avec trois autres pays extra-européens

[201] Thierry Breton, « Chantier sur la lutte contre la cybercriminalité », rapport présenté au Ministre d'intérieur français en 2005. http://www.ladocumentationfrancaise.fr/rapports-publics/054000263/index.shtml

[202] Idem, Page 12

[203] Idem, Page 13

[204] https://www.internet-signalement.gouv.fr/

[205] Didier Duval, « PHAROS, la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements », La criminalité numérique, Cahier de la sécurité n°06, page 91.

[206] Christian Aghroum, «L'Europe, un atout pour la France dans la lutte contre la cybercriminalité», La criminalité numérique, Cahier de la sécurité n°06, page 95.

(Canada, Japon, et Sénégal) pour faire partie des collaborateurs autour de cette plateforme[207].

5. Les acteurs institutionnels internationaux

Malgré un consensus presque universel sur le fait que la cybercriminalité est une question transnationale qui exige une réponse coordonnée de la part de tous les pays, les prémices de la coopération internationale, qu'il convient de saluer, se heurtent pour autant à de nombreuses limites. D'une part, le dialogue et la coordination au niveau international ne se sont pas traduits par des actions concrètes. Il y a bien des initiatives diverses mais elles sont encore trop éparses ou indépendantes les unes des autres pour qu'il en émane réellement une cohérence dans la politique de lutte contre la cybercriminalité. Il en résulte que beaucoup d'Etats ont des législations différentes au point que les criminels profitent de ces failles juridiques[208]. En effet, des attaques lancées par une personne dans un pays ou une juridiction donnée peuvent affecter des personnes dans plusieurs autres pays et une communication par email envoyée à une personne se trouvant pourtant dans le même pays peut générer en un autre endroit des preuves sous forme électronique, les données pouvant être transmises dans plusieurs pays via les serveurs. Les failles aussi bien pénales que procédurales limitent donc les actions de répression compte tenu du caractère transnational des crimes et délits. D'autre part, il est compréhensible que des pays ayant des niveaux de développement, des priorités et des problèmes différents aient des avis différents sur des questions de portée mondiale comme les cybermenaces ou l'inadéquation des solutions de cybersécurité. C'est la raison pour laquelle de nombreuses organisations et institutions internationales se sont emparées du sujet afin de coordonner la lutte contre la cybercriminalité au niveau international. Nous citons par exemple :

- ✓ Les Nations-Unies
- ✓ L'Organisation de Coopération et de Développement Economiques (OCDE)
- ✓ L'Union Internationale des Télécommunications (UIT)
- ✓ Interpol
- ✓ Le conseil de l'Europe
- ✓ Europol

[207] http://lecourrier.vnagency.com.vn/PrintView.asp?id=42915

[208] Franck Franchin et Rodolphe Monnet, « Le business de la cybercriminalité », Edition LAVOISIER, 2005

Rappelons par ailleurs qu'une convention sur la cybercriminalité a été ratifiée par plusieurs pays. Négocié en étroite collaboration avec les Etats-Unis, le Canada, le Japon et l'Afrique du Sud, le projet de convention sur la cybercriminalité, premier traité destiné à lutter contre les infractions pénales commises sur les réseaux informatiques, a été adopté par le Conseil de l'Europe en 2001.

Conscient de la nécessité d'une coopération internationale pour mieux lutter contre la cybercriminalité, le Maroc a signé des mémorandums d'entente avec plusieurs pays. Il s'agit notamment d'un mémorandum d'entente portant sur la coopération dans le domaine de la cybersécurité, en particulier l'aspect relatif à la formation et au développement des compétences, avec la Malaisie et d'un mémorandum d'entente avec la Corée du Sud portant sur la coopération en matière d'e-gouvernement et de la cybersécurité.

Conclusion du chapitre

A l'instar de plusieurs pays, la formation de l'écosystème de la cybercriminalité au Maroc date depuis peu de temps. Ce n'est qu'à partir du moment où l'internet est devenu accessible pour le grand public que nous avons commencé à entendre parler de la criminalité liée aux technologies de l'information. Par ailleurs, l'univers *Underground* marocain a plusieurs années d'avance par rapport à l'univers répressif, qui rappelons-le, est représenté par peu d'institutions et dispose de peu de moyens. C'est sous la pression de nos partenaires étrangers et dans le cadre de la lutte contre le terrorisme qu'un certain nombre d'acteurs représentant les pouvoirs publics se sont emparés du phénomène de la cybercriminalité pour mieux structurer la lutte. Aujourd'hui, plusieurs institutions clés intervenant dans l'investigation, la veille et la répression sont en cours de mise en place dans le cadre de la stratégie « Maroc Numeric 2013 ».

Chapitre 4 : L'arsenal juridique face à la cybercriminalité au Maroc

« Ce qu'on appelle liberté, dans le langage politique,
c'est le droit de faire des lois,
c'est-à-dire d'enchaîner la liberté »
Auguste Vermorel

Face au phénomène de la cybercriminalité, les ripostes juridiques nationales sont différentes d'un pays à l'autre. Ceci s'explique notamment par l'émergence de deux courants ayant deux conceptions différentes du phénomène. Le premier estime qu'il n'y a pas lieu de distinguer entre l'information stockée sur les supports traditionnels et celle qui est automatisée. Par conséquent, la cybercriminalité ne justifie pas de nouvelles mesures législatives[209]. Le deuxième courant considère la cybercriminalité comme étant un phénomène spécifique. De nouvelles mesures sont donc nécessaires. Les ripostes juridiques marocaines s'inscrivent dans cette deuxième perspective. Cette démarche a abouti à l'adoption de trois textes législatifs :

- La loi n°07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données;
- La loi n°53-05 relative à l'échange électronique de données juridiques;
- La loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Signalons par ailleurs, comme cela est de coutume, en particulier lorsqu'il s'agit de domaines liés aux nouvelles technologies, les rédacteurs de ces lois se sont contentés de reproduire presque littéralement les dispositions de la loi française. Il s'agit notamment des lois suivantes :

- ✓ La loi n°2004-801 du 6 août 2004, qui modifie la loi du 06 janvier 1978 relative à l'informatique, aux fichiers et libertés ;

[209] Mohamed Chawki, « Combattre la cybercriminalité », page 120.

- ✓ La loi du 5 janvier 1988 dite Loi Godfrain ;
- ✓ La loi n°2000-230 du 13 Mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

Certes, ces textes permettront au Maroc de mettre à niveau son arsenal juridique, mais à l'état actuel, nous ne pouvons pas dire que nous disposons de tous les textes permettant de réprimer la cybercriminalité avec ses multiples visages. Ils nous arrivent d'ailleurs souvent de nous rabattre sur les infractions de droit commun telles que l'escroquerie, le faux et usage de faux pour incriminer des infractions comme la fraude à la carte bancaire commise sur l'internet par exemple.

1. La loi n°07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données

Jusqu'à octobre 2003, le phénomène de la cybercriminalité au Maroc n'a fait l'objet d'aucune disposition législative visant à le réprimer. Il s'agissait encore d'un phénomène mal connu et marginal. Par conséquent, l'arsenal juridique marocain disposait de lacunes sérieuses empêchant la répression des infractions liées à la criminalité informatique. De nombreuses dispositions du code pénal se révèlent parfaitement inadaptées aux spécificités du phénomène[210]. Face à cette situation, le législateur marocain se trouvait contraint d'enrichir le code pénal par des dispositions susceptibles de s'appliquer aux infractions commises par voie informatique ou électronique. C'est ainsi que la loi n°07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données a vu le jour en 2003.

Reproduite à partir de la loi française du 5 janvier 1988 dite loi Godfrain, la loi n°07-03 constitue un texte fondateur pour la mise à niveau de l'arsenal juridique marocain afin de tenir compte des infractions imputables à la criminalité informatique. Elle traite les atteintes aux systèmes de traitement automatisé des données (STAD) et réprime pénalement de nombreux comportements. Les intrusions ainsi que les atteintes aux systèmes de traitement

[210] Mohamed Diyaâ Toumlilt, « Le commerce électronique au Maroc : Aspects juridiques » Les éditions Maghrébines.

automatisé des données demeurent les plus importantes incriminations contenues dans cette loi[211].

1.1 Les intrusions

La loi n°07-03 permet de sanctionner toutes les intrusions non autorisées dans un système de traitement automatisé de données. Elle fait la distinction entre l'accès et le maintien frauduleux dans un STAD. En effet, deux types d'accès illicites peuvent être envisagés[212] :

- L'accès dans l'espace, qui consiste à pénétrer par effraction dans un système informatique (accès frauduleux) ;
- L'accès dans le temps, qui s'agit du fait d'outrepasser une autorisation d'accès donnée pour un temps déterminé (maintien frauduleux).

Les sanctions prévues varient selon que l'intrusion a eu ou non une incidence sur le système en cause.

1.1.1 L'accès frauduleux dans un STAD

Parmi les actes réprimés dans la loi n°07-03, on trouve en premier lieu l'accès frauduleux. Cette infraction résulte de l'article 607-3 du code pénal qui dispose dans sa rédaction de 2003 : « le fait d'accéder, frauduleusement, dans tout ou partie d'un système de traitement automatisé des données est puni d'un mois à trois mois d'emprisonnement et de 2.000 à 10.000 dirhams ou de l'une de ces deux peines seulement ». Dès lors que le maintien ou l'accès frauduleux entraîne une altération du système, la loi marocaine prévoit un doublement de la peine. En effet, l'article 607-3, al. 3 du Code pénal dispose « La peine est portée au double lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le STAD, soit une altération du fonctionnement de ce système ».

L'accès au STAD peut se faire[213] :

- Depuis l'extérieur du système : ainsi, un pirate qui pénètre dans un ordinateur connecté à l'internet tombe sous le coup de la loi.
- Depuis l'intérieur du système : un salarié qui, depuis son poste, pénètre dans une zone du réseau de l'entreprise à laquelle il n'a pas le droit d'accéder pourra être poursuivi.

---

[211] Idem, Page 213

[212] Mohamed Chawki, « Combattre la cybercriminalité », Page 123

[213] Droit et Internet « Interviews de spécialistes » 2005
http://epi.univ-paris1.fr/82341344/0/fiche___actualite/&RH=epi-287&RF=epi-287

L'accès est sanctionné uniquement s'il est frauduleux. Il convient ainsi, de préciser que l'accès frauduleux à un STAD, tel qu'il a été précisé par la jurisprudence française[214], est constitué « dès lors qu'une personne, non habilitée, pénètre dans ce système tout en sachant être dépourvue d'autorisation, peu importe le mobile[215] ». Ce qui recouvre un grand nombre d'hypothèses. Dans cette perspective, la Cour d'appel de Paris a considéré dans un arrêt du 5 avril 1994 que « l'accès frauduleux, au sens de la loi, vise tous les modes de pénétration irréguliers[216] d'un système de traitement automatisé de données, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication[217] ».

Toutefois, dans un arrêt du 4 décembre 1992, la Cour d'appel de Paris a écarté les délits d'accès et de maintien dans un système de traitement automatisé de données informatiques en constatant que l'appropriation d'un code d'accès avait pu être le résultat d'une erreur de manipulation sur les fichiers, cette circonstance excluant le caractère intentionnel exigé par la loi. Ainsi, une intrusion accidentelle ne peut être incriminée, encore faut-il ne pas se maintenir dans le STAD accidentellement atteint[218]. Mais, il reste à savoir si la présence d'un dispositif de sécurité est une condition de l'incrimination pénale ?

Si certains pays comme la Norvège et les Pays-Bas considèrent qu'un dispositif de sécurité est nécessaire pour punir l'accès ou l'interception illicite de données[219], la loi marocaine à l'instar de la loi française, n'a pas apporté de précision concernant la nécessité ou l'indifférence de la présence de dispositifs de sécurité pour la constitution du délit d'accès et de maintien frauduleux. En France, le législateur n'a pas voulu reprendre cette obligation pourtant proposée par le député Godfrain dés 1988, ni dans la loi sur les infractions informatiques, ni lors de la réforme du Code pénal. Cette volonté a été affirmée par la cour d'appel de Paris en 1994 qui a déclaré : « Il n'est pas nécessaire pour que l'infraction existe,

---

[214] Etant donné que la loi marocaine n'est que la reproduction de la loi française, il s'avère important d'analyser les précisions apportées par la jurisprudence française par rapport à la notion de l'accès.

[215] Maitre Delphine Bastien, « Accès frauduleux dans un système de traitement automatisé de données », décembre 2008 http://avocats.fr/space/delphine.bastien/content/_AA84FB96-8CD4-4860-9DF6-C9EFA2729809

[216] Par pénétration irrégulière, il est entendu toute intrusion non autorisée par le maître du système.

[217] CA. Paris, [5 avril 1994], (Les Petites Affiches), [5 juillet 1995] n°80, p.13. obs Alvarez.

[218] Mireille Cahen, « Intrusion dans un Système Informatique » http://www.murielle-cahen.com/publications/p_intrusions.asp

[219] Mohamed Chawki, « Combattre la cybercriminalité », page 135

que l'accès soit limité par un dispositif de protection, mais qu'il suffise que le maître du système ait manifesté l'intention de restreindre l'accès aux seuls personnes autorisées[220] ».

1.1.2 Le maintien frauduleux dans un STAD

La loi marocaine incrimine également le maintien frauduleux dans un système de traitement automatisé de données. L'article 607-3 du code pénal marocain dispose : « Est passible de la même peine toute personne qui se maintient dans tout ou partie d'un système de traitement automatisé de données auquel elle a accédé par erreur et alors qu'elle n'en a pas le droit ». La jurisprudence française précise que l'incrimination concerne le maintien frauduleux ou irrégulier dans un système de traitement automatisé de données de la part de celui qui y est entré par inadvertance ou de la part de celui qui, y ayant régulièrement pénétré, se serait maintenu frauduleusement[221]. C'est sur ce fondement que la cour d'appel de Paris a condamné en 1994 les fondateurs de sociétés télématiques, les gérants de centres serveurs et les informaticiens à leur service. Ils essayaient de se maintenir dans des services télématiques au mépris de la volonté des titulaires et alors que ceux-ci tentaient d'évincer les intrus par divers moyens de surveillance[222].

Quant à l'élément intentionnel de cette infraction, la doctrine et la jurisprudence s'accordent à admettre que l'adverbe "frauduleusement" n'est pas le dol général de l'attitude volontaire, ni le dol très spécial de l'intention de nuire, mais la conscience chez le délinquant que l'accès ou le maintien ne lui était pas autorisé. Cette précision vise le cas du fraudeur habilité à accéder à une partie non autorisée d'un système de traitement automatisé de données, s'y maintient en connaissance de cause, et au cas du fraudeur qui ayant eu par hasard accès à un système fermé, s'y maintient volontairement tout en sachant qu'il n'y a pas de droit[223]. Dans ce cadre, la cour d'appel de Toulouse dans un arrêt a précisé que le maintien pendant 45 minutes caractérisait l'aspect frauduleux de ce dernier[224]. Il s'agissait en l'espèce d'un informaticien qui, après son licenciement, avait conservé le code d'accès au système de son

[220] CA. Paris : (IR), [5/04/1994] p.130

[221] Cours d'appel de Paris. Jugement de 5 avril 1994 précité.

[222] CA. Paris, [5 avril 1994], (Paris, D.IR.), [1994] p.130.

[223] Mohamed Chawki, « Combattre la cybercriminalité », page 150

[224] CA Toulouse 21 janvier 1999, Juris-Data n°040054.

ancien employeur, y avait accédé puis s'y était maintenu, causant même des dommages justifiant une incrimination plus grave[225].
En clair, relèvent de la qualification pénale toutes les intrusions intentionnelles irrégulières (accès frauduleux), mais aussi régulières si elles dépassent l'autorisation donnée (maintien frauduleux).

1.2 Les atteintes

Les atteintes au STAD ont tendance à devenir de plus en plus fréquentes de nos jours, que le but soit le simple vandalisme ou bien encore, de façon plus élaborée, un but économique (vol ou altération de données dans le but d'en retirer de l'argent). Le législateur marocain a prévu des incriminations de ces délits dans le cadre de la loi n°07-03.

1.2.1 Les atteintes au fonctionnement d'un STAD

L'atteinte au fonctionnement d'un STAD peut être constitué de manières très diverses, par tout comportement ou toute action qui va entraîner temporairement ou de manière permanente une gêne dans le fonctionnement du système, une dégradation du système voire le rendre totalement inutilisable. L'article 607-5 du Code pénal, inséré en vertu de la loi n°07-03, dispose que « Le fait d'entraver ou de fausser intentionnellement le fonctionnement d'un système de traitement automatisé des données est puni d'un an à trois ans d'emprisonnement et de 10.000 à 200.000 dirhams d'amende ou de l'une de ces deux peines seulement ».

A la lecture de l'article 607-5, il ressort que l'élément matériel d'une atteinte portée à un STAD lui-même et non pas à ses données peut provenir de l'entrave ou du faussement de ce dernier. L'exemple le plus connu de ce délit est l'attaque par déni de service[226]. Au-delà de ces attaques sophistiquées, la jurisprudence française a retenu que le fait pour un employé de changer les mots de passes d'accès à un système dans le but de la rendre inutilisable pouvait l'exposer aux peines prévues pour l'entrave, à contrario si le refus de communiquer

[225] Mohamed Diyaâ Toumlilt « Le commerce électronique au Maroc : Aspects juridiques » Les éditions Maghrébines, Page 215

[226] La Cour d'appel de Paris a considéré l'envoi automatique de messages et l'utilisation de programmes simulant la connexion de multiple Minitel à un centre serveur, perturbant ainsi les performances du système et entraînant un ralentissement de la capacité des serveurs, comme étant constitutif du délit d'entrave au fonctionnement d'un STAD.

les mots de passe n'empêche pas le bon fonctionnement du système le délit n'est pas constitué[227].

Alors que l'entrave a pour finalité de perturber le fonctionnement du système, le faussement pour sa part consiste à faire produire au système un résultat différent de celui qui était attendu. Il peut suffire de bloquer l'appel d'un programme, d'un fichier ou encore d'altérer l'un des éléments du système. Le plus courant étant le cas d'une attaque virale classique.

Bien évidemment, pour que l'atteinte au fonctionnement d'un STAD soit retenue, l'auteur doit avoir conscience que ses actes vont dégrader les performances d'un système voire le rendre inopérant. Ainsi, lorsqu'un individu pénètre dans un système informatique sans rien faire d'autre, nous parlerons alors d'accès et de maintien frauduleux et non de l'entrave.

1.2.2 Les atteintes aux données

L'article 607-6 du code pénal dispose que « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de détériorer ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni d'un an à trois ans d'emprisonnement et de 10.000 à 200.000 dirhams d'amende ou de l'une de ces deux peines seulement ».

En réalité, toute manipulation de données, qu'il s'agisse de les introduire, de les supprimer, de les modifier ou de les maquiller, provoque, en toutes circonstances, une altération du système. Le fait de modifier les tables d'une base de données, de déréférencer l'adresse d'un serveur Web dans les moteurs de recherche, ou encore, de défacer un site web pour y insérer une image indécente, constituent autant d'atteintes visées par le texte.

Si dans le cadre de la législation française, le délit n'est constitué que si les atteintes sont réalisées avec une intention délictueuse et hors de l'usage autorisé, il convient d'observer à propos de cet élément intentionnel une des rares dispositions que le législateur marocain n'a pas « empruntée » à la loi Godfrain. Il s'agit en l'occurrence de l'exigence que l'atteinte soit commise « aux mépris des droits d'autrui »[228].

---

[227] Cours d'appel de Poitiers le 20/01/1998 (Gazette du Palais 14-15 Janvier 2000, p37).

[228] Mohamed Diyaâ Toumlilt, « Le commerce électronique au Maroc : Aspects juridiques » Les éditions Maghrébines, P. 226

Enfin, il convient de signaler que pour tous ces délits, que ce soit pour les intrusions (accès et atteinte frauduleux au STAD) et pour les atteintes (atteintes au fonctionnement et atteintes aux données d'un STAD), la tentative est punie des mêmes peines. En effet, l'article 607-8 du code pénal dispose « La tentative des délits prévus par les articles 607-3 à 607-7 ci-dessus et par l'article 607-10 ci-après est punie des mêmes peines que le délit lui-même ».

2. La loi 53-05 relative à l'échange électronique de données juridiques

L'utilisation de plus en plus croissante des nouvelles technologies d'information et de communication ainsi que l'obsolescence du droit marocain de la preuve – puisqu'avant le 30 novembre 2007[229], le seul support ayant la force probante était le papier – ont justifié la réforme du cadre juridique de la preuve.

Cette réforme a pour objet de fixer le régime applicable aux données juridiques échangées par voie électronique, à l'équivalence des documents établis sur papier et sur support électronique et à la signature électronique. Elle détermine également le cadre juridique applicable aux opérations effectuées par les prestataires de services de certification électronique, ainsi que les règles à respecter par ces derniers et les titulaires des certificats électroniques délivrés. En outre, la loi institue une autorité nationale d'agrément et de surveillance de la certification.

2.1 La preuve

La loi n°53-05 comporte deux volets particulièrement novateurs en matière de preuve. Il s'agit de la redéfinition de la preuve littérale et la consécration de la force probante de l'écrit électronique.

2.1.1 La redéfinition de la preuve littérale

Traditionnellement, l'écrit avait fini par se confondre avec son support papier. Pourtant, le dictionnaire définit l'écriture comme « une représentation de la parole et de la pensée par des signes », sans qu'il soit fait référence à un quelconque support papier[230]. La loi n°53-05

[229] La date de promulgation de la loi n°53-05 relative à l'échange électronique des données juridiques

[230] Valérie Sedallian, « Preuve et Signature électronique »,
http://www.juriscom.net/chr/2/fr20000509.htm#_ftn11

relative à l'échange électronique de données juridiques a mis fin à cette confusion en prenant soin de modifier la formulation de l'article 417, alinéa 2 du Dahir des Obligations et Contrats (D.O.C). La preuve littérale ne s'identifie plus au papier, ne dépend ni de son support matériel, ni de ses modalités de transmission. L'article 417, alinéa 2 dispose que la preuve littérale peut également résulter « de tous autres signes ou symboles dotés d'une signification intelligible quels que soient leur support et leurs modalités de transmission ». Le législateur affirme donc l'équivalence entre le papier et l'électronique. Cela a constitué une avancée fondamentale du droit de la preuve. La définition respecte ainsi le principe de neutralité technologique[231]. La seule condition posée réside dans le fait que le message doit être intelligible, c'est-à-dire qu'il s'agisse d'une information destinée à être communiquée et comprise[232].

2.1.2 La consécration de la force probante de l'écrit électronique

La redéfinition de la preuve littérale n'est pas le seul apport de la nouvelle loi, la consécration de la force probante de l'écrit électronique est aussi l'un des volets particulièrement novateurs de la loi n°53-05. En effet, cette loi confère la même force probante à l'écrit électronique que l'écrit sous forme papier, à condition qu'il permette à la personne dont il émane d'être dûment identifiée et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. L'article 417-1 dispose que « l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse dûment être identifiée à la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».

2.2 La signature électronique

Dans le but de faciliter l'utilisation des signatures électroniques, de contribuer à leur reconnaissance juridique et d'instituer un cadre juridique pour les services de certification, la loi n°53-05 reconnaît la validité juridique de la signature électronique dés lors qu'elle remplira certaines conditions. Cette reconnaissance constitue une avancée importante pour la promotion du commerce électronique. Elle en est même son fondement de base.

---

[231] Eric Caprioli, « Le juge et la preuve électronique », *Juriscom.net*, 10 janvier 2000, http://www.juriscom.net.

[232] Mohamed Diyaâ Toumlilt, « Le commerce électronique au Maroc : Aspects juridiques » Les éditions Maghrébines, P.445

2.2.1 La reconnaissance juridique de la signature électronique

Le texte de la loi n°53-05 non seulement reconnaît juridiquement la signature électronique, mais il va encore plus loin en consacrant la validité de la signature électronique en l'absence de toute convention préalable. Cependant, la signature électronique ne peut être qualifiée de valide tant qu'elle ne remplisse pas certaines conditions. En effet, l'article 417-2, dispose que lorsque la signature est électronique, « il convient d'utiliser un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ».

Dans l'absolu, la signature remplit deux fonctions juridiques de base. Il s'agit de l'identification de l'auteur et de la manifestation de sa volonté d'approbation du contenu de l'acte. Il va de même pour la signature électronique. L'article précité exige que le procédé d'identification soit d'une part, fiable et d'autre part, il doit garantir le lien de la signature électronique avec l'acte, lien qui en effet indispensable pour que la signature électronique joue pleinement sa fonction d'approbation du contenu de l'acte[233].

La fiabilité de ce procédé est présumée, jusqu'à preuve de contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, conformément à la législation et la réglementation en vigueur en la matière. L'article 417-3 dispose que « la fiabilité d'un procédé de signature électronique est présumée, jusqu'à preuve de contraire, lorsque ce procédé met en œuvre une signature électronique sécurisée ».

Pour qu'elle puisse être qualifiée de « sécurisée », la signature électronique doit remplir les conditions suivantes[234] :

- ✓ Elle doit être propre au signataire ;
- ✓ Elle doit être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- ✓ Elle doit garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure dudit acte soit détectable ;
- ✓ Elle doit être produite par un dispositif de création de signature électronique, attestée par un certificat de conformité ;

[233] Mohamed Diyaâ Toumlilt, « Le commerce électronique au Maroc : Aspects juridiques » Les éditions Maghrébines, P. 448

[234] Ces conditions sont prévues par l'article 6 de la loi n°53-05

- ✓ Les données de vérification de la signature électronique sécurisée doivent être mentionnées dans le certificat électronique sécurisé prévu à l'article 10 de la présente loi ».

Les caractéristiques du dispositif sécurisé de création de signature électronique auquel la loi fait allusion sont précisées au niveau de l'article 8 de la loi précitée qui dispose que « Le dispositif de création de signature électronique consiste en un matériel et/ou un logiciel destiné(s) à mettre en application les données de création de signature électronique, comportant les éléments distinctifs caractérisant le signataire, tels que la clé cryptographique privée, utilisée par lui pour créer une signature électronique ». Ce dispositif doit en outre, conformément à l'article 9, satisfaire aux exigences ci-après :

1. Garantir par des moyens techniques et des procédures appropriées que les données de création de signature électronique :
   a) Ne peuvent être établies plus d'une fois et que leur confidentialité est assurée ;
   b) Ne peuvent être trouvées par déduction et que la signature électronique est protégée contre toute falsification ;
   c) Peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers.
2. N'entraîner aucune altération ou modification du contenu de l'acte à signer et ne pas faire obstacle à ce que le signataire en ait une connaissance exacte avant de le signer.

Toujours dans le même ordre d'idées, et conformément aux dispositions de l'article 11 de la loi, le certificat de conformité ne pourra être considéré comme sécurisé que s'il est délivré par un prestataire de services de certification électronique agréé par l'autorité nationale d'agrément et de surveillance de la certification électronique, à condition toutefois qu'il comporte un certain nombre de mentions informatives énumérées au paragraphe 2 du dit article.

2.2.2 Les prestataires de services de certification

Pour que le recours à la signature électronique offre une sécurité juridique, des tiers de confiance doivent être mis en place. Il s'agit d'un organisme public ou privé, qui émet des certificats électroniques. Le certificat est un registre informatique revêtu d'une signature électronique qui identifie l'émetteur du certificat, identifie le souscripteur et donne sa clé publique. On peut le comparer à une carte d'identité électronique qui serait émise par un tiers indépendant et neutre. La signature électronique correspondant à un certificat est considérée appartenir à la personne mentionnée dans le certificat. C'est dans cette

perspective, que la loi n°53-05 a institué, en vertu de l'article 15, l'autorité nationale d'agrément et de surveillance de la certification électronique. Cette dernière a pour mission :

- ✓ De proposer au gouvernement les normes du système d'agrément et de prendre les mesures nécessaires à sa mise en œuvre ;
- ✓ D'agréer les prestataires de services de certification électronique et de contrôler leurs activités.

Pour exercer les activités liées à la certification électronique, il faut obligatoirement être agréé par l'Autorité Nationale d'Agrément et de Surveillance de la Certification Electronique. Pour y parvenir, le demandeur de l'agrément doit, en vertu de l'article 21 de la loi précitée, être constitué sous forme de société ayant son siège social sur le territoire du Royaume et :

1. Remplir des conditions techniques garantissant :
    a) La fiabilité des services de certification électronique qu'il fournit, notamment la sécurité technique et cryptographique des fonctions qu'assurent les systèmes et les moyens cryptographiques qu'il propose ;
    b) La confidentialité des données de création de signature électronique qu'il fournit au signataire ;
    c) La disponibilité d'un personnel ayant les qualifications nécessaires à la fourniture de services de certification électronique ;
    d) La possibilité, pour la personne à qui le certificat électronique a été délivré, de révoquer, sans délai et avec certitude, ce certificat ;
    e) La détermination, avec précision, de la date et l'heure de délivrance et de révocation d'un certificat électronique ;
    f) L'existence d'un système de sécurité propre à prévenir la falsification des certificats électroniques et à s'assurer que les données de création de la signature électronique correspondent aux données de sa vérification lorsque sont fournies à la fois des données de création et des données de vérification de la signature électronique.
2. Etre en mesure de conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique, sous réserve que les systèmes de conservation des certificats électronique garantissent que :
    a) L'introduction et la modification des données sont réservées aux seules personnes autorisées à cet effet par le prestataire ;

b) L'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;

c) Toute modification de nature à compromettre la sécurité du système peut être détectée ;

3. S'engager à :

3.1 Vérifier, d'une part, l'identité de la personne à laquelle un certificat électronique est délivré, en exigeant d'elle la présentation d'un document officiel d'identité pour s'assurer que la personne à la capacité légale de s'engager, d'autre part, la qualité dont cette personne se prévaut et conserver les caractéristiques et références des documents présentés pour justifier de cette identité et de cette qualité ;

3.2 S'assurer au moment de la délivrance du certificat électronique :

a) Que les informations qu'il contient sont exactes ;

b) Que le signataire qui y est identifié détient les données de création de signature électronique correspondant aux données de vérification de signature électronique contenues dans le certificat ;

3.2.1 Informer, par écrit, la personne demandant la délivrance d'un certificat électronique préalablement à la conclusion d'un contrat de prestation de services de certification électronique :

a) Des modalités et des conditions d'utilisation du certificat ;

b) Des modalités de contestation et de règlement des litiges ;

3.3 Fournir aux personnes qui se fondent sur un certificat électronique les éléments de l'information prévue au point précédent qui leur sont utiles ;

3.4 Informer les titulaires du certificat sécurisé au moins soixante (60) jours avant la date d'expiration de la validité de leur certificat, de l'échéance de celui-ci et les inviter à le renouveler ou à demander sa révocation ;

3.5 Souscrire une assurance afin de couvrir les dommages résultant de leurs fautes professionnelles ;

3.6 Révoquer un certificat électronique, lorsque :

a) Il s'avère qu'il a été délivré sur la base d'informations erronées ou falsifiées, que les informations contenues dans ledit certificat ne sont plus

conformes à la réalité ou que la confidentialité des données afférentes à la création de signature a été violée ;

b) Les autorités judiciaires lui enjoignent d'informer immédiatement les titulaires des certificats sécurisés délivrés par lui de leur non conformité aux dispositions de la présente loi et des textes pris pour son application.

3. La loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

Inspirée de la célèbre loi française Informatique et Libertés, la loi n° 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel a été publiée au Bulletin Officiel n° 5744 du 18 Juin 2009, après avoir été promulguée par le Décret n° 2-09-165, en date du 21 mai 2009. Elle introduit, pour la première fois, dans le paysage juridique marocain, un ensemble de dispositions légales harmonisées avec le droit européen et, notamment, avec la Directive Communautaire n° 95/46.

La loi prévoit, des clauses relatives aux objectifs, champ d'application et au référentiel du concept de protection des données personnelles, des dispositions portant sur les conditions du traitement de cette catégorie de données, les droits de la personne concernée et obligations du responsable du traitement, et la création d'une commission de contrôle de la protection de cette catégorie de données.

3.1 La nature des données à protéger

La loi n° 09-08 s'applique au traitement des données à caractère personnel, sous quelque forme que ce soit relatives à une personne physique identifiée ou identifiable[235]. Le nom, prénom, adresse, courriel, photographie d'identité, numéro d'identification, empreintes digitales constituent par exemple des données à caractère personnel. Dans cette optique peut-on considérer une adresse *IP* comme une donnée à caractère personnel et par

[235] « Est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques de son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale » Article premier de la loi n°09-08

conséquent tombe sous la protection de la loi n°09-08. Compte tenu du fait que la loi marocaine n'est qu'une reproduction de la loi française, il apparaît opportun d'apporter les précisions émises par la jurisprudence française concernant l'adresse *IP*. Ainsi, la cour d'appel de Paris a estimé que, contrairement à la position de la CNIL, le relevé de l'adresse *IP* qui est une série de chiffres qui entre dans le constat de la matérialité de l'infraction et non dans l'identification de son auteur, ne constitue en rien une donnée indirectement nominative.

Le traitement qui fait l'objet de la protection des données à caractère personnel concerne toute opération ou tout ensemble d'opérations portant sur des données à caractère personnel réalisés ou non par le biais de procédés automatisés. Il s'agit notamment de la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. Rappelons, par ailleurs, qu'une seule de ces opérations suffit à constituer un traitement de données à caractère personnel qui sera soumis aux dispositions de la loi n°09-08. Le simple fait de collecter les données, sans même les communiquer ou les diffuser, suffit à caractériser un traitement[236].

Il convient de souligner par ailleurs que les implications de cette nouvelle loi concernent non seulement les entreprises et les citoyens établis sur le territoire marocain mais aussi toutes les entreprises étrangères qui entretiennent des relations d'affaires avec leurs homologues marocaines ou qui échangent des données avec leurs filiales ou leurs maisons mères marocaines, tout en utilisant des moyens situés sur le territoire marocain. Toutefois, le champ d'application de cette loi exclut les données relatives à l'exercice d'activités personnelles ou ménagères, celles obtenues au service de la Défense nationale et de la Sûreté intérieure et extérieure de l'Etat, ou encore celles obtenue dans le cadre du traitement effectué en application d'une législation particulière.

3.2 Les droits de la personne concernée

Chaque traitement de données à caractère personnel, ou son transfert à des tiers, nécessite en principe, pour être effectué, le consentement indubitable de la personne concernée par ledit traitement ou ledit transfert. Toutefois, ledit consentement n'est pas requis dans

[236] Myriam Quemener, Joël Ferry, « Cybercriminalité : Défi mondial » Edition Economica 2009, Page 106

certains cas, notamment pour le respect d'une obligation légale, la sauvegarde d'intérêts vitaux ou l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique[237].
Les personnes physiques disposent au titre des articles 5 et suivants de la loi précitée de quatre types de droits.

3.2.1 Le droit à l'information

Ce droit de regard sur ses propres données personnelles vise aussi bien la collecte des informations que leur utilisation. Ce droit d'être informé est essentiel car il conditionne l'exercice des autres droits tels que le droit d'accès ou le droit d'opposition. Ainsi, Toute personne sollicitée en vue d'une collecte de ses données personnelles, doit être préalablement informée par le responsable du traitement de celles-ci ou son représentant d'un certain nombre d'éléments dont principalement les finalités du traitement auquel les données sont destinées.

3.2.2 Le droit d'accès

Autre le droit à l'information, la loi précitée donne le droit à la personne concernée d'être au courant de la compilation de ses données et d'y avoir accès pour s'assurer de leur véracité et si elles font l'objet d'un usage sain. L'accès peut se faire à intervalles raisonnables sans qu'il y ait d'entrave à ce droit, c'est-à-dire sans que la procédure d'accès soit trop lourde.

3.2.3 Le droit de rectification

Le droit de rectification constitue un complément essentiel du droit d'accès. En effet, les personnes concernées peuvent obtenir l'actualisation, la rectification, l'effacement ou le verrouillage des données personnelles collectées, notamment du fait du caractère inexact ou incomplet des informations.

3.2.4 Le droit d'opposition

Enfin, pour autant qu'elle justifie de motifs légitimes, la personne concernée pourra s'opposer au traitement des données la concernant. Ainsi toute personne peut refuser, sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection, en particulier commerciale.

[237] « La nouvelle loi sur la protection des données des personnes physiques » Newsletter de Garrigues Maroc, N°7, Avril-Mai-Juin 2009.

3.3 Les obligations du responsable du traitement

La loi n°09-08 définit le responsable du traitement comme « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires, le responsable du traitement doit être indiqué dans la loi d'organisation et de fonctionnement ou dans le statut de l'entité légalement ou statutairement compétente pour traiter les données à caractère personnel en cause »[238].
Selon la nature des informations collectées, le traitement va nécessiter soit une autorisation préalable, soit une déclaration préalable de la part de la Commission de contrôle de la protection des données à caractère personnel. Le responsable de traitement est tenu en outre par des obligations de confidentialité et de sécurité des traitements et de secret professionnel.

3.3.1 Déclaration préalable

Tout traitement de données personnelles doit donner lieu à une déclaration préalable auprès de la commission nationale sauf si la loi en dispose autrement conformément à l'article 18. Ainsi constitue bien une collecte de données à caractère personnel devant donner lieu à une déclaration le fait d'identifier des adresses électroniques et de les utiliser, même sans les enregistrer dans un fichier, pour adresser à leurs titulaires des messages électroniques[239]. La déclaration préalable comporte l'engagement que le traitement sera effectué conformément aux dispositions de loi. La dite déclaration a pour objet de permettre à la commission nationale d'exercer les compétences qui lui sont dévolues et de contrôler le respect des dispositions de la loi. Le défaut de déclaration est sanctionné par l'article 52 de la loi précitée.

Le principe de finalité constitue un élément majeur « les données sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ». Dés lors un traitement de données à caractère personnel est créé pour atteindre un objectif et ne pas servir à d'autres fins. Ainsi, la SNCF en France qui avait déclaré comme finalité du fichier Socrate la délivrance de titres de

[238] Loi n°09-08, Chapitre premier : Dispositions générales, Article premier.

[239] Myriam Quémener, Joël Ferry, « Cybercriminalité : Défi mondial » Edition Economica 2009, Page 106

transport a commis un détournement de finalité en utilisant ses fonctionnalités pour vérifier l'activité d'un personnel[240].

3.3.2 Autorisation préalable

L'autorisation préalable devra être obtenue par le responsable du traitement lorsque ledit traitement porte sur des données dites « sensibles ». Par données sensibles, il est entendu conformément à l'alinéa 3 de l'article premier « *données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale de la personne concernée ou qui sont relatives à sa santé y compris ses données génétiques* ». En outre, doivent être soumises à autorisation préalable les données utilisées à d'autres fins que celles pour lesquelles elles ont été collectées, les données relatives aux infractions, condamnations ou mesures de sûreté, de même que les données comportant le numéro de la carte d'identité nationale de la personne concernée. Rappelons cependant, que conformément à l'alinéa 1 de l'article 12, des exemptions de déclaration sont parfois possibles pour les associations ou tout autre groupement à but non lucratif et à caractère religieux, philosophique, politique, syndical, culturel ou sportif. Tout comme pour la déclaration préalable, le défaut de l'autorisation préalable est sanctionné par l'article 52 de la loi précitée.

3.3.3 Obligation de confidentialité et de sécurité des traitements et de secret professionnel

Autre l'obligation de procéder à une déclaration préalable ou à une autorisation préalable, selon les cas, le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Cette obligation relève de l'article 23 de la loi n°09-08 et son défaut est sanctionné. Il peut être assuré au moyen d'une sécurisation des transferts, des accès par des mots de passe sur les postes, par l'attribution de niveau d'habilitation ou de profils d'accès variant avec le niveau des utilisateurs. Mais la sécurité n'est jamais totale et doit être adaptée à l'état de l'art et à l'importance des données à protéger.

Notons enfin que des sanctions allant de simples amendes à des peines d'emprisonnement ont été mises en place pour assurer le respect des nouvelles dispositions.

[240] Myriam Quémener, Joël Ferry, « Cybercriminalité : Défi mondial » Edition Economica 2009, Page 107

Conclusion du chapitre

Conscient des dangers de la cybercriminalité, le Maroc a encadré aux quatre vents son cyberespace. En effet, la loi n°07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données, la loi n°53-05 relative à l'échange électronique de données juridiques et la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel constituent une étape importante dans la mise à niveau de notre arsenal juridique. Certes, elles ont pu poser les premières bases d'une lutte contre la cybercriminalité mais désormais le défi se situe au niveau de l'applicabilité de ces textes de lois. Pour le relever, l'Etat doit créer plus de passerelles entre l'univers informatique et celui des juristes comprenant aussi bien des avocats, des magistrats que des policiers et des gendarmes.

Chapitre 5 : Vers la confiance numérique au Maroc

« L'Homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique »
Albert Einstein

Il appartient à l'Etat d'établir la confiance numérique et de garantir la sécurité dans le cyberespace. Certes, la tâche est plus ardue qu'il n'y paraît puisqu'il est difficile de contrôler humainement et techniquement un internet sans frontière[241]. Cependant, de nombreuses initiatives dans plusieurs pays ont eu l'impact dissuasif souhaité. Les mesures prises varient selon les pays et les cultures locales. En effet, si par exemple les Etats-Unis inscrivent leur politique de répression contre la cybercriminalité dans le cadre de la protection des intérêts vitaux de la nation américaine, en France, la lutte s'inscrit dans une perspective de protection des libertés individuelles et de droits de l'Homme[242].

Au Maroc, à défaut d'un texte fondateur décrivant la stratégie tout comme la vision globale à mettre en place pour sécuriser le cyberespace marocain, nos politiques ont entrepris différentes actions à plus ou moins grande échelle. Parmi ces initiatives, le programme « Confiance Numérique » qui rentre dans le cadre de la stratégie « Maroc Numeric 2013[243] », est incontestablement la feuille de route la mieux élaborée à l'heure où nous écrivons ces lignes. C'est la raison pour laquelle nous avons jugé nécessaire de présenter les différents axes de cette feuille de route tout en essayant de l'enrichir davantage à la lumière des meilleures pratiques en la matière.

[241] Frank Franchin et Rodolphe Monnet, « Le business de la cybercriminalité », Edition LAVOISIER, 2005

[242] La loi « Informatique et Libertés » qui date de 1978 en est le meilleure exemple.

[243] Maroc Numeric 2013 « Stratégie Nationale pour la Société de l'Information et de l'Economie Numérique » http://www.mcinet.gov.ma/mciweb/MarocNumeric2013/MarocNumeric2013.pdf

1. L'Etat de l'art des tentatives étatiques pour garantir la confiance numérique

De nombreux pays sont en train de mobiliser leurs forces vives pour combattre le phénomène de la cybercriminalité. Différentes initiatives nationales sont à remarquer même si leurs niveaux de mise en œuvre varient d'un pays à l'autre. Il y a un réel retour d'expérience à faire partager. Le plus avancé dans ce domaine est incontestablement les Etats-Unis. Mais plusieurs autres pays tels que le France et le Canada par exemple ne cessent de faire évoluer leur arsenal répressif afin de mieux cerner le phénomène. Les pays émergents ne sont pas épargnés par cette lutte. Sous couvert de la coopération internationale et compte tenu de l'importance des enjeux politiques et économiques, ces pays sont souvent contraints de s'aligner sur les standards internationaux pour éviter qu'ils deviennent des paradis cybercriminels.

1.1 L'exemple des Etats-Unis

Parue en 2003 et impulsée par l'administration *Bush*, la stratégie de sécurisation du cyberespace américain est prise en charge par le *Department of Homeland Security (DHS)*. La lutte s'inscrit donc dans une vision globale de sécurité. Elle se fonde sur un corpus juridique global qui a donné lieu à de nombreux résultats concrets. En effet, depuis les événements du 11 septembre 2001, de nouvelles lois qui servent de fondement à la sécurisation des infrastructures critiques se sont apparues. Le *Patriot Act*[244] a été le premier texte à impulser un tel mouvement. Cette loi qualifie par exemple toute activité de *hacking* visant les sites web gouvernementaux ou d'autres systèmes connectés au réseau de l'internet d'actes terroristes[245]. Toujours dans la même perspective, le *Cyber Security*

[244] Le USA PATRIOT Act (qui signifie : *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* ou en français : *Loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme*) est une loi anti-terroriste qui a été votée par le Congrès des États-Unis et signée par George W. Bush le 26 octobre 2001. L'un des axes centraux de ce long texte (132 pages) est d'effacer la distinction juridique entre les enquêtes effectuées par les services de renseignement extérieur et les agences fédérales responsables des enquêtes criminelles (FBI) dès lors qu'elles impliquent des terroristes étrangers. Elle a créé aussi les statuts de combattant ennemi et combattant illégal, qui permettent au gouvernement des États-Unis de détenir sans limite et sans inculpation toute personne soupçonnée de projet terroriste. Source : http://fr.wikipedia.org/wiki/USA_PATRIOT_Act

[245] Frank Franchin et Rodolphe Monnet « Le business de la cybercriminalité », Edition LAVOISIER, 2005, Page 56

Enhancement Act (CSEA) adopté dans le cadre de la loi *Homeland Security Act,* vise à fixer des normes minimales de sécurité pour les entreprises exploitant une part de l'infrastructure critique des Etats-Unis et imposerait également des normes officielles pour les professionnels de la sécurité informatique[246]. Ce principe de *Net Guard* a renforcé les pouvoirs des autorités compétentes. Par ailleurs, le législateur américain est intervenu pour protéger la propriété des données, des applications ainsi que des infrastructures des internautes en édictant le *Computer Fraud and Abuse Act (CFAA)* ainsi que le *Digital Millenium Copyright (DMCA)*[247].

L'application concrète de cet arsenal juridique regroupant aussi d'autres textes qui s'inscrivent dans la même perspective tels que par exemple *Theft Penalty Enhancement Act* qui se penche sur le vol des identités sur l'internet, a eu d'importantes retombées. Ainsi, en 2004 une large opération de démantèlement menée par les services secrets américains, appelée "Opération Firewall", a dévoilé au public les premières informations sur le marché noir en ligne et qui se cache derrière ce marché. Plusieurs membres principaux et chefs de *ShadowCrew*, une communauté en ligne de cybercriminels, étaient arrêtés pour appartenir à une économie clandestine où l'usurpation d'identité et l'échange de biens volés étaient monnaie courante[248]. En 2010, une opération menée conjointement entre le *FBI* et les autorités espagnoles a permis le démantèlement d'un groupe de cybercriminels derrière le plus important réseau d'ordinateurs zombies. Nommé *Mariposa* (Papillon en espagnol), ce *botnet* qui a infecté plusieurs millions d'ordinateurs dans plusieurs pays, s'était spécialisé notamment dans la récupération des données confidentielles (numéros de cartes de crédit, codes d'accès à des sites bancaires)[249].

En 2010, un nouveau pas a été franchi dans la lutte contre la cybercriminalité. En effet, pour mieux protéger le cyberespace, le président Obama a nommé un coordinateur gouvernemental pour les questions de cybersécurité. Howard Schmidt, un ancien *Microsoft*, a été désigné pour coordonner, au sein de l'ensemble du gouvernement américain, les dispositifs de lutte contre les cyber-menaces. Cette nomination est intervenue après la

---

[246] Nicolas Guillaume « Cyber-guerre : les Etats-Unis seraient vulnérables », ITespresso.fr http://www.itespresso.fr/cyber-guerre-les-etats-unis-seraient-vulnerables-33881.html

[247] Frank Franchin et Rodolphe Monnet « Le business de la cybercriminalité », Edition LAVOISIER, 2005, Page 56

[248] « Le marché noir de la cybercriminalité », Symantec http://www.symantec.com/fr/fr/norton/cybercrime/blackmarket.jsp

[249] Reynald Fléchaux « Coup de filet en Espagne pour démanteler Mariposa, un botnet géant » http://www.lemagit.fr/article/securite-espagne-police-hackers-conficker-botnet/5750/1/coup-filet-espagne-pour-demanteler-mariposa-botnet-geant/

publication d'un rapport remis au Congrès américain indiquant explicitement que la Chine a élaboré des techniques si sophistiquées d'espionnage informatique qu'il pouvait pénétrer dans les réseaux américains les plus sensibles pour y dérober des informations confidentielles[250].

1.2 L'exemple de la France

La France a pris conscience du phénomène de la cybercriminalité, il y a plusieurs années. Pour la police et la gendarmerie, la cybercriminalité représente la nouvelle forme de criminalité du XXIe siècle. De nombreux organes d'investigation, de répression et de veille ont été mis en place. Que ce soit la brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI), la cellule informatique de l'institut de recherche criminelle de la gendarmerie nationale (IRCGN), l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) ou bien le CERTA comme structure d'alertes et d'assistance sur l'internet, les moyens mis en place sont multiples[251].

Parallèlement à cette réponse institutionnelle, la France a renforcé son paysage législatif en se dotant des lois qui répriment la cybercriminalité dans ses multiples visages. En effet, depuis la loi Informatique et libertés (1978), la législation française a pris en compte la problématique de la cybercriminalité avec la loi du 5 janvier 1988, dite « loi Godfrain », la loi du 15 novembre 2001 relative à la sécurité quotidienne, la loi du 18 mars 2003 pour la sécurité intérieure, la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, la loi du 21 juin 2004 pour la confiance dans l'économie numérique et la loi du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle. Cet important dispositif législatif est complété par plusieurs textes réglementaires.

2. La confiance numérique au Maroc

En Octobre 2009, Ahmed Réda CHAMI, le Ministre de l'Industrie, du Commerce et des Nouvelles Technologies a présenté devant Sa Majesté le Roi Mohammed VI, la stratégie

[250] http://technaute.cyberpresse.ca/nouvelles/internet/200811/21/01-802908-etats-unis-alerte-au-cyber-espionnage-chinois.php

[251] Thierry Breton, « Chantier sur la lutte contre la cybercriminalité », rapport présenté au Ministre d'intérieur français en 2005. http://www.ladocumentationfrancaise.fr/rapports-publics/054000263/index.shtml

nationale pour la société de l'information et l'économie numérique. Intitulée « Maroc Numeric 2013 », cette stratégie s'articule autour de quatre priorités stratégiques[252]:

1. Rendre accessible aux citoyens l'Internet Haut Débit et favoriser l'accès aux échanges et à la connaissance.
2. Rapprocher l'administration des besoins de l'usager en termes d'efficacité, de qualité et de transparence à travers un ambitieux programme d'e-gouvernement.
3. Inciter à l'informatisation des Petites et Moyennes Entreprises pour accroître leur productivité.
4. Développer la filière locale TI en soutenant la création et la croissance des acteurs locaux ainsi qu'en favorisant l'émergence de pôles d'excellence à fort potentiel à l'export.

Pour rendre opérationnelles ces orientations stratégiques, deux mesures d'accompagnement ont été identifiées. Il s'agit du développement du capital humain et de l'instauration de la confiance numérique. Sans ces deux mesures, une stratégie aussi ambitieuse soit-elle est vouée à l'échec. En effet, le Maroc ne produit pas assez de compétences en nouvelles technologies de l'information et de communication. L'objectif de 10 000 ingénieurs informaticiens vers l'horizon 2010 est loin d'être atteint. En outre, on ne peut parler du développement du commerce électronique sans un réel climat de confiance numérique. Les acteurs économiques ont besoin d'être rassurés sur le volet sécurité pour qu'ils puissent se lancer dans l'économie numérique. La stratégie nationale de confiance numérique repose sur trois initiatives clés.

- ✓ Initiative 1 : Mettre à niveau et renforcer le cadre législatif ;
- ✓ Initiative 2 : Mettre en place les structures organisationnelles appropriées ;
- ✓ Initiative 3 : Promouvoir et sensibiliser les acteurs de la société à la sécurité des systèmes d'information.

2.1 Le renforcement du cadre législatif

Que ce soit la loi n°07-03 complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données, la loi n°53-05 relative à l'échange électronique de données juridiques ou la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, le Maroc

[252] Source : Maroc Numeric 2013 « Stratégie Nationale pour la Société de l'Information et de l'Economie Numérique »
http://www.mcinet.gov.ma/mciweb/MarocNumeric2013/MarocNumeric2013.pdf

est en train de réaliser un effort certain pour mettre à niveau son arsenal législatif. Toutefois, le manque de jurisprudence ainsi que de définitions communes entre le technicien et le magistrat sont autant de limites à la mise en place d'une réelle politique judiciaire de répression de la cybercriminalité.

2.1.1 Protéger les personnes physiques à l'égard des traitements de données à caractère personnel

Ayant vu le jour sous la pression des acteurs de *l'offshoring,* notamment les centres d'appels délocalisés dont l'activité nécessitait un traitement rigoureux des données à caractère personnel, la loi n° 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel vise la protection de l'identité, des droits et des libertés individuelles et collectives ainsi que de la vie privée, contre toutes les atteintes susceptibles de les affecter par l'usage de l'informatique. Notons par ailleurs que le décret d'application de la loi a été publié au Bulletin Officiel N° 5744 dans son édition du 18 juin 2009. Ledit décret a fixé notamment les conditions et modalités de désignation des membres de la Commission Nationale, ses règles de fonctionnement et ses pouvoirs d'investigation, ainsi que les conditions de transfert des données à caractère personnel vers un pays étranger.

Des sanctions allant de simples amendes à des peines d'emprisonnement ont été mises en place pour assurer le respect des nouvelles dispositions[253].

2.1.2 Favoriser la dématérialisation des transactions électroniques

La dématérialisation des transactions électroniques n'est plus un luxe. Il s'agit désormais d'une contrainte qui s'impose de plus en plus aux opérateurs économiques marocains sous notamment la pression d'une concurrence féroce imposant la rationalisation des coûts et la réingénierie des processus d'affaires. Partant de ce constat, il était évident d'accompagner sur le plan juridique ce développement. C'est dans cette perspective que la loi n°53-05 relative à l'échange électronique de données juridiques a vu le jour. Cette réforme se justifie par plusieurs constats : tout d'abord la sécurité juridique est devenue nécessaire pour favoriser les échanges dans la société de l'information actuelle, puis l'obsolescence du D.O.C

[253] Voir chapitre 4 « Arsenal juridique face à la cybercriminalité au Maroc », Paragraphe 3 pour plus de détails à ce sujet.

en matière de preuve puisque avant la loi 53-05, le seul support ayant la force probante était le papier[254].

En consacrant la valeur probante de l'écrit sous forme électronique, d'une part, et en introduisant la signature électronique dans notre droit, d'autre part, la loi est saluée comme constituant une avancée fondamentale du droit de la preuve. En outre, le décret tant attendu pour l'application des articles 13, 14, 15, 21 et 23 de ladite loi est sorti dans le bulletin officiel en date de 21 mai 2009. Ceci a permis d'apporter de nombreuses réponses aux différentes questions techniques relatives au cryptage et à la signature électronique.

Toujours dans la même perspective et pour permettre une réelle application sur le terrain de la loi n°53-05, plusieurs arrêtés ont été publiés. Il s'agit de :

- ✓ Arrêté du ministre de l'industrie, du commerce et des nouvelles technologies n°151-10 du 22 mars 2010 fixant la forme de la déclaration préalable d'importation, d'exportation, de fourniture, d'exploitation ou d'utilisation de moyens ou de prestations de cryptographie et le contenu du dossier l'accompagnant ;
- ✓ Arrêté du ministre de l'industrie, du commerce et des nouvelles Technologies n°152-10 du 22 mars 2010 fixant la forme et le contenu de la demande d'autorisation préalable d'importation, d'exportation, de fourniture, d'exploitation ou d'utilisation de moyens ou de prestations de cryptographie et du dossier l'accompagnant ;
- ✓ Arrêté du ministre de l'industrie, du commerce et des nouvelles technologies n°153-10 du 22 mars 2010 relatif à l'agrément des personnes ne disposant pas de l'agrément de prestataires de services de certification électronique et qui entendent fournir des prestations de cryptographie soumises à autorisation ;
- ✓ Arrêté du ministre de l'industrie, du commerce et des nouvelles technologies n°154-10 du 22 mars 2010 fixant la forme de la demande d'agrément de prestataire de services de certification électronique et portant approbation du modèle de cahier des charges l'accompagnant.

2.1.3 Soutenir le développement du commerce électronique

Selon le Centre Monétique Interbancaire, le montant total des paiements effectués sur internet par carte bancaire auprès des sites marchands a atteint presque 53 millions de DH au premier trimestre de l'année 2010. Autrement dit, le e-commerce au Royaume a

[254] Voir chapitre 4 « Arsenal juridique face à la cybercriminalité au Maroc », Paragraphe 2 pour plus de détails à ce sujet.

enregistré une progression de 25% par rapport au 4ème trimestre 2009 et environ la moitié du montant réalisé en 2009 (107 millions de DH)[255]. Cet engouement pour le commerce électronique s'explique par plusieurs facteurs. D'abord, la mise à niveau de l'arsenal juridique marocain par la promulgation de loi n°53-05 et la loi n°09-08 qui sont des textes fondateurs en matière d'échange électronique de données juridiques et de protection des personnes physiques à l'égard des traitements des données à caractère personnel. Ensuite, par la possibilité, rendue effective par les banques marocaines en 2008, d'effectuer des paiements en ligne par des cartes marocaines. Rappelons par ailleurs, que la diversité des services et produits proposés en ligne a fortement contribué à cette croissance.

Cette croissance, qui certes demeure importante, est en deçà de chiffre d'affaires potentiel à aller chercher. La principale cause de « ce manque à gagner » demeure le manque de confiance dans le paiement en ligne. En effet, plusieurs études montrent que le développement du commerce électronique ne se fera que si l'on arrive à gagner la confiance du consommateur. Dans cette perspective, et à travers le programme « confiance numérique », le gouvernement marocain envisage d'élaborer les textes législatifs et réglementaires nécessaires à la protection des consommateurs pour la vente en ligne.

En clarifiant les conditions de l'achat en ligne et en renforçant les droits du cyberconsommateur, les textes envisagés doivent offrir une sécurité juridique déterminante au profit de l'acheteur en ligne. Il s'agira de couvrir notamment les aspects suivants :

1. *La sécurité lors de la formation du contrat :* Les textes envisagés doivent imposer une certaine transparence de la part du cybervendeur à l'égard du cyberacheteur (obligation de préciser son identité, les prix, les taxes, les frais de livraison). L'idée, c'est de pouvoir obliger le cybervendeur à ce qu'il fasse en sorte que toutes les informations relatives à la transaction soient claires et non ambiguës.
2. *La sécurité quant à l'exécution de la prestation :* Les futurs textes doivent instaurer une responsabilité de plein droit du cybercommerçant à l'égard du cyberconsommateur. Le cybervendeur est présumé responsable de plein droit de l'inexécution ou de la mauvaise exécution de la prestation, quand bien même celle-ci serait due à un intermédiaire de la chaîne de contrat et à charge pour lui de se retourner contre cet intermédiaire.

[255] Rachid Jankari, « E-commerce au Maroc : croissance de 180 % en 2010 ! » http://zawaya.magharebia.com/fr/zawaya/opinion/212

3. *La sécurité lors du paiement de la transaction :* Autre le recours à des moyens cryptographiques pour la sécurisation du paiement en ligne, qui est rendu possible grâce à la loi 53-05 et son décret d'application, les futurs textes doivent préciser les responsabilités des différentes parties en cas d'utilisation frauduleuse d'une carte bancaire pour réaliser un paiement en ligne.

2.2 Mise en place des structures organisationnelles appropriées

Les ripostes juridiques en matière de lutte contre la cybercriminalité, aussi exhaustives soient-elles, seront insuffisantes si elles ne sont pas accompagnées par la mise en place d'institutions chargées notamment de la répression, d'investigation et de veille en matière de cybercriminalité. Dans cette perspective, le programme « confiance numérique » a eu le mérite de prévoir la mise en place des organismes suivants :

- ✓ Le Comité de la Sécurité des Systèmes d'Information (SSI) ;
- ✓ L'organisme ma-CERT ;
- ✓ L'organisme de tiers de confiance ;
- ✓ La commission Nationale de Protection des Données Personnelles (CNDP) ;
- ✓ Les sites de *back-up.*

2.2.1 Mettre en place le Comité de la Sécurité des Systèmes d'Information

Conformément à l'article 9 de décret n°2-08-444 du 25 joumada I 1430 (21 mai 2009) instituant le conseil national des technologies de l'information et de l'économie numérique dispose que « Le Conseil national peut créer en son sein tous autres comités spécialisés qu'il estime nécessaires à l'accomplissement de ses missions ». A cet effet, il est prévu dans le cadre du « Maroc Numeric 2013 » de mettre en place un comité de la sécurité des systèmes d'information. Il aura notamment comme mission, l'élaboration de la politique relative à la protection des infrastructures critiques du Royaume.

Cette initiative, bien que louable, reste insuffisante. En effet, par définition un comité ne propose que des actions ponctuelles. Or, pour pouvoir piloter la confiance numérique, il faut un travail structurel. Pour y parvenir, de nombreux pays ont mis en place des Agences Nationales de Sécurité des Systèmes d'Information (ANSSI). C'est le cas par exemple de la France, du Canada mais aussi de la Tunisie.

Prenons l'exemple du pays le plus proche de nous culturellement et économiquement. Créée en 2004 sur la base de la loi n°2004-5, l'Agence Nationale de la Sécurité Informatique[256] en Tunisie, a pour mission d'effectuer le contrôle général des systèmes informatiques et des réseaux relevant des divers organismes publics et privés tunisiens. Elle est notamment chargée des missions suivantes :

- ✓ Veiller à l'exécution des orientations nationales et de la stratégie générale en matière de sécurité des systèmes informatiques et des réseaux ;
- ✓ Suivre l'exécution des plans et des programmes relatifs à la sécurité informatique dans le secteur public, à l'exception des applications particulières à la défense et à la sécurité nationale, et assurer la coordination entre les intervenants dans ce domaine ;
- ✓ Assurer la veille technologique dans le domaine de la sécurité informatique ;
- ✓ Etablir des normes spécifiques à la sécurité informatique, élaborer des guides techniques et procéder à leur publication ;
- ✓ Œuvrer à encourager le développement de solutions nationales dans le domaine de la sécurité informatique et à les promouvoir conformément aux priorités et aux programmes qui seront fixés par l'agence ;
- ✓ Participer à la consolidation de la formation et du recyclage dans le domaine de la sécurité informatique ;
- ✓ Veiller à l'exécution des réglementations relatives à l'obligation de l'audit périodique de la sécurité des systèmes informatiques et des réseaux.

2.2.2 Mettre en place le ma-CERT

Pour assurer une meilleure veille en matière de sécurité et coordonner ainsi les réponses aux incidents liés à la sécurité des systèmes d'information (ma-CERT) au niveau national, un centre dédié sera mis en place dans les prochains mois. Il aura pour mission de :

- ✓ Répondre aux incidents de sécurité, de coordonner les réponses aux incidents au niveau national et de proposer divers services portant sur le traitement de ces incidents,
- ✓ Analyser les vulnérabilités et la restauration des systèmes attaqués.

Au lancement du centre ma-CERT, plusieurs services dits « de base » seront proposés. Il s'agit notamment de :

- ✓ Services de base « réactifs »

[256] http://www.ansi.tn/

- Alertes et avertissements
- Gestion des incidents

✓ Services de base « proactifs »

- Annonces
- Veille technologique
- Audits ou évaluation de la sécurité
- Service de détection des intrusions
- Diffusion d'informations relatives à la sécurité

✓ Gestion de la qualité et de la sécurité

- Conseil en matière de sécurité
- Sensibilisation
- Formation

Pour rendre opérationnels ces services, un appel d'offre pour l'assistance à la mise en place du centre ma-CERT a été lancé en juillet 2009 par le Département de la Poste, des Télécommunications et des Nouvelles Technologies (DEPTI)[257].

Au niveau du cahier des charges relatif à l'appel d'offres précité, on trouve notamment les principaux services attendus. Il s'agit notamment de[258]:

✓ *Service d'alertes et d'avertissements :* Ce service aura pour mission de diffuser des informations décrivant une attaque, une vulnérabilité de sécurité, une alerte d'intrusion, un virus informatique ou un canular, et à recommander des mesures à court terme pour remédier aux problèmes qui en découlent. Un bulletin d'alerte, d'avertissement ou de sécurité sera envoyé par la suite aux parties prenantes dont les systèmes sont affectés, afin de les prévenir et de leur donner des conseils pour protéger leurs systèmes ou pour les restaurer s'ils ont été affectés.

✓ *Service de réponse aux incidents :* La gestion des incidents constitue le service de base de ma-CERT. Il vise à répondre aux incidents de sécurité affectant ses parties prenantes en assurant une assistance téléphonique, email ou fax aux victimes d'une attaque en vue de circonscrire l'incident.

[257] http://www.technologies.gov.ma/test_offre.aspx?id=1431

[258] Source : Appel d'offre n°02/2009 relatif à « Assistance à la mise en place du Centre National de Gestion et de Traitement des Incidents de Sécurité Informatique : "Computer Emergency Response Team of Morocco (ma-CERT) »

- ✓ *Activités de veille technologique :* Cette activité consistera à produire mensuellement une lettre d'information présentant les tendances, les nouvelles menaces, les dernières technologies de protection et les principales solutions.

Autre ces services, des prestations complémentaires seront prises en charge par ma-CERT. Il s'agit notamment de :

- ✓ L'analyse des incidents
- ✓ La réalisation de l'expertise post-incident
- ✓ La coordination de la réponse aux incidents
- ✓ La coordination internationale au sein des réseaux des CERTs
- ✓ La conduite de missions de revue de configuration
- ✓ La conduite de missions d'examen de bonnes pratiques
- ✓ La conduite de missions de tests d'intrusion
- ✓ L'adhésion au réseau FIRST

Précisons par ailleurs, que le centre ne disposera pas d'une plateforme de signalement qui permettra aux internautes marocains de signaler les sites illicites tels que les sites pédopornographiques, les sites d'incitations à la haine et aux injures raciales, au terrorisme et de déclarer les incidents cybercriminels à l'image de ce qui se fait par exemple en France. Ce dispositif, qui permettra d'élucider les délits et les orienter vers les services de polices, de gendarmerie et des douanes et éventuellement vers Interpol, sera pris en charge en partie par le portail de la sécurité des systèmes d'information proposé par le DEPTI[259].

Le portail, qui constituera un support de communication à destination des internautes mal informés des risques liés à la cybercriminalité, contiendra les éléments suivants[260] :

- ✓ A propos de la sécurité des systèmes d'information au Maroc
  - o Politique nationale
  - o Cadre juridique
- ✓ Services
  - o Services de base « réactifs »
    - ▪ Déclaration d'incidents

[259] Source : http://www.technologies.gov.ma/test_offre.aspx?id=1431

[260] D'après le Cahier des Prescriptions Spéciales (CPS) relatif à l'appel d'offre n°05/2009 relatif à « L'élaboration du contenu du portail de la sécurité des systèmes d'information SSI ».
http://www.technologies.gov.ma/Fiche_pdf/appel_offre/2009/Cps_App_Off5-2009.pdf

        - Alertes et avertissements
        - Gestion des incidents
        - Gestion des vulnérabilités
    - Service de base « proactifs »
        - Annonces
        - Veille technologique
    - Gestion de la qualité et de la sécurité
        - Conseil en matière de sécurité
        - Sensibilisation
        - Formation
- ✓ Outils & ressources
    - Protection
    - Diagnostic
    - Contrôle parental
    - Glossaire
    - Conseils et mesures
    - Guide de meilleures pratiques
    - Module d'autoformation
- ✓ Rapports et publications
    - Rapports d'incidents
    - Rapports de vulnérabilités
    - Lettres d'informations
- ✓ Partenaires
    - CERTA
    - ENISA
    - UIT
    - IMPACT
    - OIC-CERT
    - MalaysiaCert
    - CERT-TCC
    - FIRST
- ✓ Contact
    - Demande d'aide
    - Envoi de commentaires
- ✓ Agenda des événements

- ✓ Liens utiles

Des informations sur les méthodes de protection de l'infrastructure informatique ainsi que sur les modes opératoires les plus couramment employés par les fraudeurs pourraient aussi être diffusées sur ce portail.

2.2.3 Mettre en place un tiers de confiance

Conformément à la loi n°53-05 et à son décret d'application, et afin de mettre en pratique les différentes dispositions relatives à la délivrance de certificats électroniques, Poste Maroc a été choisi pour jouer le rôle de tiers de confiance. Le but, c'est d'offrir aux échanges électroniques une garantie de fiabilité, d'authentification et d'intégrité des données et ceci par l'émission et la délivrance de certificats électroniques. Ainsi, d'ici 2013, il est prévu dans le cadre du « Maroc Numeric 2013 », de délivrer 60 000 certificats électroniques.

2.2.4 Mettre en place la commission nationale de la protection des données personnelles

Pour veiller, au respect de ses différentes dispositions, la loi 09-08 a institué la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel. Chargée de veiller à la mise en œuvre des dispositions de la loi, la commission nationale est un organe doté de prérogatives et de larges pouvoirs d'investigation, de contrôle et d'intervention. Ses membres sont nommés par Sa Majesté le Roi afin de garantir leur autonomie et leur impartialité vis-à-vis des différentes parties prenantes.

Rappelons par ailleurs qu'un décret d'application de la loi 09-08 a été publié au Bulletin Officiel N° 5744 dans son édition du 18 juin 2009. Ledit décret a fixé notamment les conditions et modalités de désignation des membres de la Commission Nationale, ses règles de fonctionnement et ses pouvoirs d'investigation, ainsi que les conditions de transfert des données à caractère personnel vers un pays étranger.

2.2.5 Développer des sites de back-up

Les infrastructures critiques sont constituées de l'ensemble des grands réseaux indispensables au bon fonctionnement d'un pays. Leur sécurisation est donc, par nature, un enjeu majeur. En effet, il est de plus en plus difficile d'accepter des pannes généralisées sur

ces réseaux. Les conséquences d'un tel accident sont dramatiques à la fois socialement et économiquement. Par exemple, les technologies de l'information et de la communication sont de plus en plus utilisées pour la conduite des réseaux électriques. Réciproquement, les réseaux informatiques et de télécommunications ne peuvent fonctionner que grâce à la disponibilité de l'énergie électrique, même si dans bien des cas des pannes de courtes durées sont tolérées du fait de l'usage d'alimentations sans interruptions. Cet accroissement des dépendances entre les infrastructures amène à l'apparition de nouvelles vulnérabilités qu'il s'agit d'identifier. C'est la raison pour laquelle, il est extrêmement important pour un pays d'envisager les différents scénarios lui permettant d'assurer la continuité des services critiques. Le Maroc, n'y échappe pas. C'est dans cette perspective, que le développement des sites de secours a été identifié comme chantier dans le cadre de la stratégie « Maroc Numeric 2013 ». L'intérêt, c'est de pouvoir faire face à une éventualité d'interruption d'un service critique en ayant recours à des *datacenters bunkérisés.*

Si l'Etat a clairement un rôle à jouer dans ce domaine, il ne faut pas pour autant écarter de cette initiative l'industrie informatique et celle des télécommunications. Riches d'expérience et de savoir-faire, ces acteurs doivent pouvoir s'inscrire dans cette démarche afin de mutualiser les efforts et les ressources.

2.3 Promotion d'une culture de sécurité

L'être humain est le maillon faible de la chaîne de la sécurité. De nombreuses techniques cybercriminelles s'appuient sur ce constat. De ce fait, quelques soient les mesures de sécurité mises en place, elles n'auront du sens que si elles sont accompagnées par la promotion d'une véritable culture de sécurité. Il s'avère donc important de développer, traiter et soutenir cette culture de sécurité au niveau de toutes les couches de la société. Pour y parvenir, l'Etat, dans le cadre de la stratégie « Maroc Numeric 2013 » s'est engagé à :

- ✓ Mettre en œuvre un programme de sensibilisation et de communication sur la SSI ;
- ✓ Mettre en place des formations sur la SSI à destination des élèves ingénieurs ;
- ✓ Mettre en place des formations à destination des professions juridiques ;
- ✓ Définir une charte des sites marchands.

2.3.1 Mettre en œuvre un programme de sensibilisation et de communication sur la SSI

L'Etat doit définir et lancer des campagnes de sensibilisation et de communication sur la sécurité des systèmes d'information. Ces campagnes doivent être ciblées et axées sur

plusieurs problématiques. Par exemple pour la protection des enfants par rapport aux dangers de l'internet notamment en ce qui concerne la pédopornographie, les actions suivantes peuvent être envisagées[261].

- ✓ Former des cadres sur la méthode de sensibilisation dans les milieux de l'enseignement, des jeunes, de l'enfance et de la famille pour mener des campagnes au sein des écoles, des campings et des maisons de jeunes.
- ✓ Mettre en place des clubs d'internet et des salles multimédias dans les écoles.
- ✓ Inciter les associations qui œuvrent dans le domaine des enfants à s'intéresser davantage à la sensibilisation en matière des dangers de l'internet dont sont victimes les jeunes et les enfants.
- ✓ Financer les associations désireuses de mener des activités dans ce sens par l'Etat, fournir l'expérience et poser les jalons de la communication avec d'autres associations internationales œuvrant dans ce domaine.
- ✓ Obliger les cybercafés à aménager des salles destinées aux mineurs, dotées d'ordinateurs utilisant des logiciels de protection.

Quelque soit la cible envisagée, les compagnes de sensibilisation doivent s'inspirer, pour une meilleure efficacité, sur le modèle des campagnes destinées à favoriser l'usage de la ceinture de sécurité au volant. Une telle démarche permettra de sous tirer des utilisateurs en ligne un comportement sécurisé et respectueux de la légalité. Comme pour la ceinture de sécurité, un effort d'éducation à long terme est nécessaire pour que de telles mesures aient de l'effet.

Il est aussi fortement souhaitable d'organiser des actions périodiques pour s'inscrire dans la durée. Ainsi, l'organisation d'un séminaire annuel sur la cybercriminalité et des journées thématiques à l'image de ce qui se fait dans plusieurs pays permettra de véhiculer des messages importants sur les différents thèmes liés à la cybercriminalité.

2.3.2 Mettre en place des formations sur la SSI à destination des élèves ingénieurs

La promotion de la culture de sécurité passe aussi par la mise en place des formations à destination des étudiants de l'enseignement supérieur. En effet, face à la demande accrue

[261] Recommandations du rapport « Les crimes de l'internet et l'enfance au Maroc », CMF MENA http://www.tanmia.ma/article.php3?id_article=7520

des organisations publiques et privés en terme de personnels qualifiés et spécialisés en sécurité SI, il est devenu extrêmement urgent de proposer des formations spécialisées en SSI à destination des étudiants. Ceci permettra aussi par la même occasion aux nombreux professeurs et experts en sécurité de dispenser des formations mettant en valeur leurs connaissances, compétences et retours d'expériences dans le domaine.

C'est dans cette perspective que l'Ecole Nationale Supérieure d'Informatique et d'Analyse des Systèmes a enrichi son programme de formation pour y inclure désormais une option de sécurité des systèmes d'information[262]. L'objectif étant de former des ingénieurs informaticiens spécialistes en sécurité des systèmes d'information, et ce, en leur permettant :

- ✓ Une prise de conscience des enjeux liés à la sécurité des systèmes d'information ;
- ✓ Une acquisition des connaissances théoriques et pratiques en matière de cryptologie ;
- ✓ Une bonne approche des aspects organisationnels et juridiques et une assimilation des normes et des référentiels de bonnes pratiques en matière de sécurité et de gouvernance des SI ;
- ✓ Une maîtrise des principales technologies et solutions utilisées pour la sécurisation des SI.

Parallèlement au programme de formation, il faudra aussi penser à mettre en place un programme de réhabilitation *des hackers*. En effet, dédramatiser le recrutement *des hackers* est un point positif. C'est aussi une approche pour faire entrer dans les entreprises la culture de la sécurité. Ce modèle existe aux Etats-Unis et au Royaume-Uni dont les organisations n'hésitent pas à recourir aux services des *hackers* repentis pour mieux se protéger.

2.3.3 Mettre en place des formations à destination des professions juridiques

Durant les prochaines années, le Maroc sera devant un enjeu stratégique. Il s'agit de l'interprétation des impacts juridiques que peuvent avoir les infractions informatiques compte tenu de leurs complexités. Pour le relever, l'Etat doit créer plus de passerelles entre l'univers informatique et celui des juristes comprenant aussi bien des avocats, des magistrats que des policiers et des gendarmes. La formation en est un axe capital. En effet, pour pouvoir faire

[262] Hanane El Bakkali, « Création à l'ENSIAS de l'option Sécurité des Systèmes d'Information(SSI) », Ifrane, conférence régionale sur la Cybersécurité.
http://www.technologies.gov.ma/RegCSecConf10/RegCSecConf10_Presentations/H.%20El%20Bakkali,%20ENSIAS_Prez_Reg%20CyberSec%20Conf_Morocco%202010.pdf

appliquer la loi, il s'avère indispensable notamment pour les magistrats et avocats de se mettre à niveau en matière de la cybercriminalité.

De cette formation, il ne faut pas oublier les cyberenquêteurs. Qu'ils soient issus de la police ou de la gendarmerie, leurs sensibilisations à la lutte contre la cybercriminalité par le biais d'une formation spécifique est indispensable.

2.3.4 Définir une charte des sites marchands

Pour pouvoir renforcer la confiance des citoyens dans le commerce électronique, l'Etat s'est engagé dans le cadre de la stratégie « Maroc Numeric 2013 » à mettre en place une charte des sites marchands. Constituée à partir des meilleures pratiques en termes de sécurisation des sites de commerce électronique, cette charte permettra aux cyberconsommateurs de mieux qualifier le respect des exigences de sécurité par les différents sites. Le respect de la charte donnera lieu à un label qui sera mis en place en partenariat avec les fédérations notamment la CGEM.

Conclusion du chapitre

La cybercriminalité est un phénomène planétaire. Pour y faire face, de nombreuses initiatives nationales ont abouti à des résultats concrets. De l'amélioration de la connaissance du phénomène à travers la mise en place des organes d'investigation et de veille jusqu'à l'amélioration des aspects répressifs par la mise en place d'un cadre législatif adéquat et des institutions chargées de faire respecter la loi, en passant par la promotion d'une véritable culture de sécurité, nous disposons aujourd'hui d'une véritable « bibliothèque de meilleures pratiques » en matière de lutte contre la cybercriminalité.

Au Maroc, sous l'impulsion de la stratégie « Maroc Numeric 2013 », la confiance numérique se dote pour la première fois d'une véritable feuille de route permettant à terme d'aligner le Maroc sur les standards internationaux.

Conclusion Générale

Durant les prochaines années, l'internet sera omniprésent, atteignant selon certains experts jusqu'à 1 Gb/s, pour devenir aussi accessible et bon marché que l'électricité. Les internautes seront connectés en permanence via leur téléphone mobile, leur ordinateur portable et leur PDA. Ils seront de plus en plus disposés à adopter les nouveaux services sur le Web. Ainsi, le cyberespace fera partie intégrante de la vie quotidienne de tout un chacun.

Le Maroc n'échappera pas à cette tendance. Le nombre d'internautes marocains, qui n'a pas cessé de croître ces dernières années, continuera de grimper d'une façon exponentielle pour atteindre 12 millions d'internautes en 2012 selon l'ANRT. Cette croissance, qui sera tirée notamment par le haut débit et l'internet 3G, couplée à l'anonymat et au faible risque de se faire arrêter, jouera un rôle favorable pour le développement de la cybercriminalité. Ce qui est de nature à encourager l'émergence de nombreuses dérives et l'apparition d'utilisateurs peu scrupuleux. Les cyberdélinquants auront encore de beaux jours devant eux.

Si aujourd'hui, la plupart des actes de déviance dans le cyberespace marocain sont motivés par l'égo, la vengeance, le hacktivisme, et la recherche de la reconnaissance, dans les années à venir, en raison notamment de développement du commerce électronique et de la multiplication des canaux de transfert d'argent, les actes cybercriminels seront lancés principalement dans une perspective d'appât de gain. Nous assisterons ainsi à un véritable engouement pour la cybercriminalité. La convergence de la criminalité perpétrée dans le monde réel vers la criminalité numérique perpétrée dans le cyberespace sera de plus en plus appréciée par les mafias. Ainsi, le blanchiment d'argent, l'escroquerie, la fraude, le proxénétisme et la pédopornographie trouveront dans le cyberespace un terrain propice à leur développement.

Face à une cybercriminalité qui sera de plus en plus globale, variée, organisée et rentable, il est particulièrement important pour les pouvoirs publics d'adopter une approche transverse mêlant problématique géopolitique, sociologique, financière et juridique.

Bibliographie

Ouvrages

1. Mohamed Diyaâ TOUMLILT « Le commerce électronique au Maroc : Aspects juridiques » Les éditions Maghrébines.
2. Bouchaïb RMAIL, « Criminalité informatique ou liée aux nouvelles technologies de l'information et de la communication », Edition Somagram.
3. Mohamed CHAWKI, « Combattre la cybercriminalité », Edition 2009.
4. Myriam QUEMENER, Joël FERRY, « Cybercriminalité, défi mondial », 2éme édition, Economica, 2009.
5. Myriam QUEMENER, « Cybermenaces, entreprises, internautes », Economica, 2008
6. Eric FILIOL, Philippe RICHARD, « Cybercriminalité : les mafias envahissent le web », Dunod, 2006.
7. Eric FILIOL, « Les virus informatiques: théorie, pratique et applications », Springer Verlag, Collection IRIS, 2004
8. Franck FRANCHIN, Rodolphe MONNET, « Le business de la cybercriminalité », Herms Science Publications, Collection Management et Informatique, 2005.
9. Solange GHERNAOUTI-HELIE, « La cybercriminalité : le visible et l'invisible », Presses Polytechniques et Universitaires Romandes, collection le Savoir Suisse, 2009
10. Solange GHERNAOUTI-HELIE, « Sécurité informatique et réseaux », 2éme édition, Sciences Sup, DUNOD, 2008
11. Dominique MANIEZ, « Les dix plaies d'Internet : Les dangers d'un outil fabuleux », Dunod, 2008
12. David FAYON, « Web 2.0 et au-delà », Economica, 2008
13. Christiane FERAL-SCHUHL, « Cyberdroit, le droit à l'épreuve de l'Internet », Dalloz, 5éméédition, 2009
14. Stuart MCCLURE, Joel SCAMBRAY, Georges KURTZ, « Halte aux hackers »,4éme édition, OEM/Eyrolles, 2003.
15. Jean-Philippe BAY, « Tout sur la sécurité informatique », Dunod, 2005.
16. Ryan RUSSELL, « Stratégies anti-hackers »,2éme édition, OEM/Eyrolles, 2003.
17. Bruce SCHNEIER, « Secrets et mensonges », Vuibert, 200l.

18. Histoire des codes secrets de Singh. Lattès, 1999.
19. Les protocoles de sécurité d'Internet, S. Natkin, Dunod, 2002
20. NATKIN, « Les Protocoles de sécurité de l'internet : Fondements et techniques de sécurisation des NTIC », Dunod, 2002
21. Nacer LALAM, « La délinquance électronique », problèmes politiques et sociaux, 2008.
22. Cahier de la Sécurité N°6, « La criminalité numérique », Institut National des Hautes Etudes de Sécurité, 2008.
23. Yannick CHATELAIN et Loïck ROCHE, « Hackers ! Le 5e pouvoir. Qui sont les pirates de l'Internet ? », Maxima, 2002.

Rapports

1. Panorama de la cybercriminalité pour l'année 2008, CLUSIF (Club de la Sécurité des Systèmes d'Information Français) ;
2. 2007 Internet Crime Report du IC3, Internet Crime Complaint Center du FBI américain ;
3. 2007 Annual Study : U.S. Cost of a Data Breach, Ponemon Institute, LLC;
4. McAfee North America Criminology Report, Organized Crime and the Internet 2008;
5. Symantec Internet Security Threat Report, 2009;
6. Symantec Report on the Underground Economy, Novembre 2008 ;
7. Baromètre annuel sur la cybercriminalité en 2009, Kaspersky Lab ;
8. Baromètre annuel sur la cybercriminalité en 2008, Kaspersky Lab ;
9. Rapport 2007, Observatoire de la sécurité des cartes de paiement, Banque de France
10. Les enfants du Net (1) – les mineurs et les contenus préjudiciables sur l'Internet : Recommandations du Forum des droits sur l'Internet, 11 février 2004.
11. Les enfants du Net (2) – Pédopornographie et pédophilie sur l'Internet, Recommandations du forum des droits sur l'Internet, 25 janvier 2005
12. Rapport présenté par Thierry Breton relatif au chantier sur la lutte contre la cybercriminalité en date du 25 février 2005
13. « Les crimes de l'internet et l'enfance au Maroc », CMF MENA
14. « Rapport 2010 sur les menaces à la sécurité », SOPHOS

Sites utiles

Sites institutionnels

1. http://www.mcinet.gov.ma
2. http://www.technologies.gov.ma
3. http://www.anrt.ma
4. http://www.cnil.fr
5. http://www.legifrance.gouv.fr
6. http://www.nouvellesmenaces.com

Sites d'associations

1. Forum des droits sur l'internet : http://www.foruminternet.org
2. Clusif : http://www.clusif.fr
3. Cyberlex : http://www.cyberlex.org
4. Cercle européen de la sécurité et des systèmes d'information : http://www.lecercle.biz
5. Association pour le développement de l'informatique juridique (ADIJ) : http://www.adij.fr
6. Association internationale de la lutte contre la cybercriminalité http://www.cybercrime-fr.org/

Sites juridiques

1. http://www.legalisnet.fr
2. http://www.juriscom.net.fr
3. http://www.europa.eu.int
4. http://www.coe.int
5. http://www.droit-ntic.com
6. http://www.droitdunet.fr
7. http://www.internet-juridique.net
8. http://www.droit-ntic

Blogs et sites d'auteurs

1. Blog de Jean-Paul PINTE : cybercriminalité, sécurité des entreprises et ordre public : http://www.cybercriminalité.wordpress.com
2. Blog de veille juridique de Gérard HAAS : http://www.jurilexblog.com
3. Blog de Laurent HESLAUL : http://www.helloblog.fr
4. Blog de Orange Business Services : http://blogs.orange-business.com/securite/
5. Blog de Hamza HAROUCHI : http://www.hamza.ma
6. Blog de Ali EL AZZOUZI : http://www.cybercriminalite.ma

Dépôt légal : 2010 MO 1585
ISBN : 978-9954-9072-0-7

Edition : Ali EL AZZOUZI
Impression : Bishops Solutions
Couverture : Hamza HAROUCHI

Imprimé à Casablanca, Juin 2010