**UNIVERSITE ABDERRAHMANE MIRA DE BEJAIA**
**FACULTE DES SCIENCES ECONOMIQUES, COMMERCIALES ET SCIENCE DE GESTION**
**DEPARTEMENT DES SCIENCES ECONOMIQUES**

# MEMOIRE

*POUR L'OBTENTION DU DIPLOME DE MASTER EN SCIENCES ECONOMIQUE, OPTION : MONNAIE, BANQUE ET ENVIRONNEMENT INTERNATIONAL*

*Thème*

## LA CYBERCRIMINALITÉ:
## L'Algérie est-elle suffisamment outillée ? Le cas des banques algériennes

*Présenté par :*
**Sylia BELATTAF**

*Sous la direction du*
**Docteur N. MOUFFOK**
Université de Bejaia

**2014-2015**

# Remerciements

Je tiens à exprimer ma gratitude et mes remerciements
les plus sincères à mon enseignant encadreur
le Docteur. N. MOUFFOK,
pour sa disponibilité et ses précieux conseils.

*Dédicace :*

*Je dédie ce travail à Mes chers parents*

## *SOMMAIRE*

| Sigles et Abbreviations | |
|---|---|
| **ABC** | Arab Banking Corporation |
| **ADSL** | Asymmetric Digital Subscriber Line |
| **AEJO** | Association des experts judiciaires et de la wilaya d'Oran |
| **AML** | Anti Money Laundering (contre le blanchiment d'argent) |
| **ANSSI** | Agence National de Sécurité des Systèmes d'Information |
| **ARPT** | Autorité de Régulation de la poste et des Télécommunications |
| **APWG** | Anti Phishing Working Group |
| **ASA** | Association Scientifique Algérienne |
| **AT&T** | American Telephone & Telegraphe |
| **ATCI** | Algérie Télécompensation Interbancaire |
| **ATM** | Algérie Télécom Mobile (MOBILIS) |
| **BA** | Banque d'Algérie |
| **BAD** | Banque Africaine de Développement |
| **BADR** | Banque de l'Agriculture et du Développement Rural |
| **BEA** | Banque Extérieur d'Algérie |
| **BNA** | Banque Nationale d'Algérie |
| **BNP** | Banque Nationale Paris |
| **CCP** | Compte Courant Postal |
| **CERT** | Computer Emergency Response Team |
| **CERIST** | Centre de Recherche sur l'Information Scientifique et Technique |
| **CIB** | Carte inter Bancaire |
| **CIRFU** | Cyber Initiative and Ressource Fusion Unit |
| **CLUSIF** | Club de la Sécurité de l'Information Français |
| **CNEP** | Caisse Nationale d'Epargne et de prévoyance |
| **CNUCED** | Conférence des Nations Unis sur le Commerce et le Développement |
| **CPA** | Crédit Populaire Algérie |
| **CPI** | Centre de Pré compensation Interbancaire |
| **CSIS** | Centre for Strategic and International Studies |
| **DAB** | Distributeur Automatique de Billet |
| **GAB** | Guichet Automatique Bancaire |
| **DBPMF** | Direction des Banques Publiques et du Marché Financier |
| **DG** | Direction Générale |
| **DGT** | Direction Générale du Trésor |
| **DoS** | Denial of Service |
| **EDI** | Echange de Données Informatisées |
| **EEPAD** | Etablissement de l'Enseignement Professionnel A Distance |
| **EI** | Etat Islamique |
| **FRAD** | Formateurs Relais Anti-Drogue de la gendarmerie nationale |
| **FBI** | Federal Bureau of Investigation |
| **GSM** | Global System for Mobile |
| **IBM** | International Business Machine |

| | |
|---|---|
| **IC3** | Internet Crime Complaint Center |
| **IP** | Internet Protocol |
| **KMS** | Kiosque Multi-Services |
| **KYC** | Know Your Customer |
| **LOPPSI** | Loi d'Orientation et de la Programmation pour la Performance de la Sécurité Intérieur |
| **MPTIC** | Ministère chargé de la Poste et des Technologies d'Information et de Communication |
| **MTN** | Mobil Telephone Networks |
| **MTE** | Mutation Engine |
| **NASA** | National Aeronautics and Space Administration |
| **NCFTA** | National Cyber Forensics Training Alliance |
| **OCDE** | Organisation de Coopération et de Développement Economiques |
| **OCLCTIC** | Office Centrale de Lutte contre la Criminalité liée aux Technologies de l'Information de Communication |
| **OLF** | Office québécois de la Langue Française |
| **ONDRP** | Observatoire National de la Délinquance et des réponses Pénales |
| **ONS** | Office National des Statistiques |
| **ONU** | Organisation des Nations Unies |
| **OSCP** | Observatoire de la Sécurité des Cartes de Paiement |
| **OTA** | Orascom Télécom Algérie(DJEZZY) |
| **OTAN** | Organisation du traité de l'Atlantique Nord |
| **PEP** | Personne Politiquement exposées |
| **PIIC** | Politique de l'information, de l'Informatique et des Communications |
| **PKK** | Partiya Karkerên Kurdistan (Partie des travailleurs du Kurdistan) |
| **RIB** | Relevé d'Identité Bancaire |
| **RMI** | Réseau Monétique International |
| **RTGS** | Règlements Bruts en Temps réel de Gros montants (ARTS) |
| **SATIM** | Société d'Automatisation des Transactions Interbancaire et de Monétique |
| **SGA** | Société Générale Algérie |
| **SSI** | Sécurité du Système d'Information |
| **SQC** | Qualifications Consultants |
| **SQL** | Structure Query Language |
| **SSI** | Sécurité des Systèmes d'Informations |
| **SSRI** | Société de Sécurisation des réseaux Informatiques |
| **STAD** | Système de Traitement Automatisé de Données |
| **SWIFT** | Society for Worldwide Interbank Financial Transaction |
| **TDA** | Télédiffusion Algérie |
| **TIC** | Technologie d'Information et de Communication |
| **UIT** | Union International de Télécommunication (IUT) |
| **WEF** | World Economic Forum |
| **WLL** | Wireless Local Loop |
| **WTA** | Watania Télécom Algérie (OOREDOO) |

« La cybercriminalité est la troisième grande menace pour les grandes puissances, après les armes chimiques, bactériologiques, et nucléaires »

Colin ROSE

# INTRODUCTION GENERALE

Le progrès fulgurant des technologies de l'information et de la communication (TIC) ont conduit à l'introduction du concept moderne de « Société de l'information », ce dernier est un modèle de société qui a permis de mettre en avant le libre accès à l'information et œuvre ainsi à la retirer des mains du pouvoir central et de renforcer la démocratie. Encore, certaines évolutions notamment, le système de paiement en ligne (banque et magasin), les services mobiles dans la transmission de données par voie IP, le e-santé…etc. Autant d'exemples pour montrer que les TIC sont une partie intégrante de notre quotidien.

La mise à disposition sur le web de nombreux outils et services s'adressant à la population mondiale, a conduit à la croissance des actes cybercriminels qui s'est notamment accélérée durant ces trois dernières années[1], et la situation risque de s'amplifier avec la mise à disposition de : réseaux sociaux, blogs, forums, MySpace, Facebook, Youtube, Twitters,…etc. En plus de l'échange d'information, ces services permettent de faciliter le téléchargement et la publication. C'est cela qui peut rendre leurs utilisations vulnérables aux infections de logiciels malveillants[2].En 2014, on utilise dans le monde plus les Smartphones et les tablettes que les ordinateurs de bureaux pour se connecter à l'Internet car les équipements mobiles représentent une alternative pratique et économique. Deux utilisateurs sur trois de Smartphones ont une confiance totale dans ces appareils qui procurent un faux sentiment de sécurité et de merveilleuses applications (Apps) rendant la vie meilleure et plus facile dont les paiements par mobile qui vont dépasser dans le monde 1,3 trillions de dollars en 2015[3].

L'importance croissante qu'occupe l'internet dans nos vies quotidiennes, concerne tout particulièrement les services de banque en ligne et du commerce électronique, s'accompagne parallèlement d'une augmentation de la criminalité organisée dans le cyberespace. En Europe, les cybers délinquants volent des coordonnées bancaires et des données de carte de crédit qu'ils revendent pour seulement 1EUR par carte ou 60EUR lorsqu'il s'agit d'identifiants bancaires. La cybercriminalité est une activité lucrative qui traverse les frontières mais comporte beaucoup de risques[4].

[1]Article sur Les enjeux de la cybercriminalité, paru en juillet 2009 par Ali El Azzouzi, page 1.
[2]Eugène Kaspersky, Sécurité Globale, Défis de la cybercriminalité, « Cybercriminalité, une guerre perdue ? », Documentation française, article n°6. Hiver 2008-2009.PP.18-19.
[3] http://www.ssri.dz/la-cyber-securite-etat-des-lieux-en-algerie/
[4]Commission européenne - Affaires intérieures - La cybercriminalité - Avril 2012, page.1.

L'insécurité liée au web engendre des coûts, et les conséquences de celle-ci peuvent être similaires à celle liées au crime économique et financier. Qui, concrètement peut se traduire par un risque de réputation pour les banques, par la perte de marché pour les entreprises victimes, conduisant ainsi à la disparition d'emploi.

Les pertes financières dues à la cybercriminalité se mesurent pour l'année 2003 à 17 milliards USD et à 100 milliards USD, en 2007 de pertes causées par les logiciels malveillants[5] et selon le rapport du Center for Strategic and International Studies (CSIS) de Juin 2014, la cybercriminalité est une industrie en croissance, ses rendements sont importants alors que les risques pour les cybercriminels restent faibles. Le coût annuel probable de la cybercriminalité à l'économie mondiale est de plus que 400 milliards de dollars[6]. Malgré l'ampleur des préjudices à l'économie et à la sécurité nationale, des gouvernements et des entreprises continuent à sous-estimer la menace liée à la cybercriminalité alors que sa vitesse et sa sophistication n'arrêtent pas de se développer. Dans le Monde Arabe, la cybercriminalité est la deuxième forme la plus commune de la criminalité économique et le coût des pertes générées par la cybercriminalité varie de 500 000 à 100 millions de dollars par entreprise par an. Cela a même dépassé pour la première fois les recettes du marché illégal de stupéfiants. Ces estimations montrent clairement qu'il est vital de protéger les infrastructures de l'information.

Le développement des TIC d'une part, les services en ligne d'autre part, ont poussé les autorités à garantir le bien-être économique et la sécurité, cela devrait commencer par l'élaboration de stratégie de prévention qui doit être une partie intégrante des stratégies nationales de « cybersécurité », qui consiste en la protection des infrastructures de l'information et celle des internautes, comme c'est déjà le cas dans l'Union européenne et au Etats Unis. Les pays auront donc une responsabilité commune d'adopter une législation appropriée et cette contre utilisation des TIC que ce soit à des fins criminelles qu'à d'autres activités nuisant à l'intégrité du pays.

Beaucoup de pays luttent souvent avec efficacité contre la cybercriminalité tout en renforçant leur sécurité informatique, mais c'est bien loin d'être le cas en Algérie où les pouvoirs publics sont moins soucieux de développer la sécurité web. En fait, l'Algérie est peu connectée,

[5]Rapport de l'IUT, « comprendre la cybercriminalité : phénomène, difficultés et réponses juridiques »,Genève (Suisse), 09/2012, P.2.
[6] AbderlazizDerdouri, « la cybersécurité : Etat des lieux en Algérie », 19/12/2014. Voir le lien suivant : http://www.ssri.dz/la-cyber-securite-etat-des-lieux-en-algerie/

stratégie e-administration et e-santé inexistante et la stratégie « e-Algérie » est encore a ses balbutiements. Plusieurs entreprises algériennes sont à jour déconnectées, les factures, les fiches de paie et bons de commande ne sont pas toujours dématérialisés. Le paiement électronique reste faible, mais cela n'empêche pas l'Algérie de figurer dans la liste des pays les plus vulnérables en matière de cyber sécurité.

A cause d'une mauvaise politique d'introduction des technologies de l'information, la numérisation en Algérie tarde à bien décoller. Elle n'est peut-être pas le pays le plus exposé aux risques informatiques, néanmoins elle reste la cible d'un bon nombre de hackers ; elle est classée troisième dans le monde des pays à haut risque d'infections informatiques avec un taux de 52,05%[7].

Dans ce cadre, l'Algérie a pris l'initiative de faire une loi qui réglemente et encadre ce genre de délinquance, elle est donc spécifique, relative à la protection, la prévention et à la lutte contre toutes formes d'infractions liées aux TIC. Cette loi a été mise en œuvre le 5 aout 2009, venant compléter celle de 2004, par l'Assemblée Populaire Nationale et le Conseil de la Nation.

A la lumière de ce qui précède, nous avons illustré notre problématique, on se posant la question suivante : Face au phénomène sans frontière de la cybercriminalité, l'Algérie est-elle suffisamment outillée ? Et qu'en est –il du cas des banques algériennes ?

Cette question principale soulève des interrogations secondaires :

- Qu'est-ce que la cybercriminalité ?
- Quelle est la place des TIC en Algérie ?
- Quel est l'Etat des lieux de ce phénomène en Algérie ?
- A-t-elle tous les moyens nécessaires pour protéger les internautes ?
- Qu'à fait l'Algérie dans ce secteur, mise à part le petit texte de loi ? et serait-il couvrir tous les aspects de la cybercriminalité?

***Choix du thème :***

1. Un thème d'actualité influençant la finance de tout pays même où le système financier n'est qu'au stade embryonnaire (comme l'Algérie) ;

[7] Les informations bien en détails citées dans le lien suivant : http://www.ssri.dz/la-cyber-securite-etat-des-lieux-en-algerie/

2. L'Algérie a été victime de hacking dernièrement ;
3. Le sujet ne doit pas être restreint aux mains d'experts seulement ;
4. Prêter une attention suffisante des autorités publiques, des banques et tout étudiant et enseignant sur le sujet et l'implication d'une cybersécurité sur l'échelle nationale;
5. Absence de confiance numérique.

***Hypothèses :***

1. Le retard dont est victime l'Algérie en matière d'introduction de TIC serait la raison de la faible exposition de notre pays au phénomène de cybercriminalité ;
2. Une stratégie de cybersécurité est loin de préoccuper l'Etat Algérien ;
3. Les moyens de lutte contre la cybercriminalité restent insuffisants face à l'incompréhension, l'incompétence et l'absence de formation des autorités concernées.

***Méthodologie :***

La méthodologie de ce travail s'articule autour de trois chapitres. Le premier est destiné à un état des lieux sur les Technologies d'Information et de Communication au niveau mondial suivant trois indicateurs de mesure, Internet, large bande fixe et la large bande mobile. Ensuite on a procédé à la démystification du phénomène de cybercriminalité, en retraçant d'abord un historique de son évolution, ensuite son impact sur l'économie mondiale et enfin en déterminant les motivations diverses qui poussent les cybers délinquants à agir.

Le deuxième chapitre, nous l'avons consacré à la lutte contre la cybercriminalité. D'abord on a scindé les différentes infractions cybercriminelles classées selon l'IUT. Parallèlement, plusieurs pays ont intégré dans leur cyberespace différentes stratégies de cybersécurité et cyberdéfense adoptées pour lutter contre la cybercriminalité.

Dans le troisième chapitre, nous avons centré notre étude sur le cas algérien. Tout d'abord en mettant en exergue la place de l'Algérie dans la mondialisation numérique par l'introduction des TIC et l'apport de ces derniers dans l'économie ainsi que la dématérialisation de ses infrastructures, particulièrement au niveau du système bancaire algérien. Ensuite, un état des lieux de la cybercriminalité s'imposait pour nous permettre d'analyser le degré de sécurisation de notre Etat aussi bien au niveau national qu'au niveau du système bancaire. De ce fait, nous avons procédé par une enquête sous forme d'un questionnaire adressé aux différentes banques (publiques et privées) et avec leurs collaborations, nous sommes arrivés à des conclusions qui nous ont permis de confirmer ou infirmer les hypothèses initialement posées.

# - CHAPITRE I -

## Introduction :

Les nouvelles technologies d'information et de télécommunication (TIC) sont passées par trois (03) phases d'évolution ; la première était celle de « l'informatique centralisée », vers le milieu des années 60 jusqu'à la fin des années 70, où des systèmes d'orientation assistés par ordinateur ont été élaborés pour montrer le potentiel de ces technologies. Puis, vient la seconde phase qui a été celle des « micro-ordinateurs », au début des années 80 jusqu'au milieu des années 90, où son avènement a rendu l'utilisation interactive plus économique et a facilité la création et la diffusion de programmes simplifiés. Enfin, la troisième phase a été celle de l'utilisation « d'Internet » dès la fin des années 90.

*« Aux routes et aux autoroutes de béton correspondent les réseaux de transmission d'information et les «autoroutes électroniques » qui s'apprêtent à révolutionner l'ensemble des modes de vie. Désormais, nous pourrons aller travailler ou faire nos courses non plus en voiture mais en modem » (Pateyron, Salmon, 1996).*

L'arrivée d'internet signifiait qu'on pouvait créer des sites accessibles instantanément par les individus à partir de différents lieux, même de leur domicile. Une autre étape a vu le jour, c'est celle du « numérique », cela s'explique du fait que toutes les technologies à caractère analogique tel que : la télévision, l'ordinateur et le téléphone ont fusionné dans un ensemble numérique intégré (Cunningham et Fröschl, 1999). L'individu a donc accès à internet par son téléphone mobile que par sa télévision ; la largeur de bande permet l'accélération massive des capacités de transmissions. Néanmoins, cette évolution rapide s'avère aussi problématique pour une personne morale que pour une personne physique. En effet, de nouvelles infractions et de nouveaux délits sont nés avec le développement de l'informatique et d'internet, communément connus sous le terme de « Cybercriminalité ». C'est ainsi que l'ordinateur est devenu aussi bien un outil qu'une cible dans le cyber espace (Sûreté du Québec, 2009).

Le phénomène de cybercriminalité a été amplifié avec les TIC, surtout avec Internet. Il est devenu source de profits, générant plusieurs milliards de dollars, son attractivité est tellement grande que des milliers d'internautes, en quête d'argent facile, s'y laissent tenter. Certains cybercriminels se contentent de fabriquer des logiciels malveillants, d'autres les utilisent afin

de perpétrer des actions criminelles[1], des « mafias » structurées, des « script-kiddies »[2], etc. Autant de noms qui définissent les auteurs et les distinguent par rapport à leurs motivations. L'ONDRP[3] dans son rapport, a évalué les infractions subis par ce phénomène, 80% sont des escroqueries et des abus de confiance (sur Internet) et 20% correspondent aux falsifications ou usages de cartes de crédit[4]. L'impact de la cybercriminalité sur l'économie ne cesse d'augmenter et les pertes financières dues à ce phénomène passent de 17 milliards USD en 2003 à 100 milliards USD en 2007[5] et à près de 500 milliards USD en 2014.

Afin de bien structurer ce chapitre, on a vu indispensable de l'entamer par une première section dans laquelle on essayera de faire un tour d'horizon sur les TIC dans le monde pour mieux comprendre le sens des transformations que suppose aujourd'hui leur introduction et de savoir si ces dernières représentent une révolution, porteuses de transformations nouvelles au sein d'une économie. Dans la deuxième section, nous allons essayer de démystifier le phénomène de « Cybercriminalité » développé et rendu complexe avec l'évolution des TIC.

## Section 01 : Les Technologies de l'Information et de la Communication (TIC) : Une troisième révolution

Depuis leurs émergences, dès les années 1990, les technologies de l'information et de la communication (TIC) n'ont guère arrêté de poursuivre leur essor dans les pays de toutes les régions du monde, permettant à un nombre croissant de personnes d'être connectées. En effet, de plus en plus de pays atteignent une masse critique en termes d'accès et d'utilisation des TIC, ce qui accélère la diffusion de ces technologies et stimule encore davantage la demande générée par le développement de l'internet et des abonnements au cellulaire. Avant de mettre le cap sur l'évolution des TIC et de démontrer la fracture numérique persistante entre régions du monde, nous allons d'abord définir la terminologie de ce terme.

Pour les banques, investir dans les TIC correspond « à l'acquisition de matériel et de logiciels destinés à être utilisés dans la production pendant plus d'un an. Les TIC se composent de trois

[1] Emmanuelle MATIGNON, « la cybercriminalité : un focus dans le monde des télécoms », Mémoire de magistère, Université Paris 1 Panthéon-Sorbonne, 2012, page 8.
[2] Un groupe de jeunes adolescents âgés de 12 à 13 ans forment un réseau organisé qui a pour action des usages déviants et frauduleux.
[3] Observatoire National de la Délinquance et des réponses Pénales.
[4] Rapport de l'ONDRP, 2011.
[5] Rapport de l'UIT, « comprendre la cybercriminalité : guide pour les PED », 2009, page 14.

éléments : matériel informatique (ordinateurs et accessoires), équipement de communication et logiciel. L'élément logiciel se compose de logiciels standards, de logiciels sur mesure et de logiciels développés en interne. Cet indicateur s'exprime en pourcentage de formation brute de capital fixe non résidentielle »[6]. Avant internet, d'autres moyens l'ont précédé impliquant le client en tant que coproducteur de la prestation bancaire[7]. Mais, ce rôle n'a cessé depuis de s'accroître et connaît de nouveaux développements.

**I-Définition et terminologie**

En juillet 1998, Le comité PIIC[8] de l'OCDE, avec la collaboration de la Commission Statistique de l'ONU[9] et l'Eurostat, se sont permis de présenter une définition du secteur des TIC et cette dernière a été acceptée au niveau international. Nouvellement créé, Le secteur des TIC comprend : les secteurs manufacturiers et des services qui facilitent la transmission, le stockage et le traitement de l'information par des moyens électroniques[10]. Les définitions les plus importantes proposées par certains organismes et Etats, sont résumées dans le tableau ci-dessous :

[6] OCDE (2015), Investissement dans les TIC (indicateur). (Consulté le 07 Février 2015)- http://data.oecd.org/fr/ict/investissement-dans-les-tic.htm#indicator-chart

[7] Rowe, 1994, P. 256

[8] Le comité PIIC –Politiques de l'Information, de l'Informatique et des Communications- (en anglais, ICCP - Information, Computer and Communication Policy) créé en 1982 est un groupe d'expert chargé de réfléchir aux questions posées par ces technologies. En 1990, un (sous) groupe de travail sur les indicateurs de la société de l'information (le GTISI en anglais WPIIS –Working Party on Indicators for the Information Society-) est constitué pour construire des indicateurs statistiques sur la société de l'information.

[9] Cette Commission réunit les Directeurs Généraux des offices statistiques nationaux et notamment le groupe de Voorburg réunit, au sein de l'ONU, des experts internationaux chargés d'examiner les questions relatives à la production de statistiques des services, et nomment celles liées à la mesure de l'économie de l'information et de la communication notamment (ONU, 2003).

[10] Plus précisément : Concernant les secteurs manufacturiers : les produits d'une industrie considérée doivent être destinés à remplir la fonction de traitement de l'information et de la communication incluant la transmission et l'affichage, utiliser l'informatique pour détecter, mesurer et/ou enregistrer un phénomène physique ou pour contrôler un processus physique.

**Tableau N°1 : Les Définitions proposées des TIC**

| | |
|---|---|
| ONU et OCDE (1998) | Le secteur des TIC comprend les secteurs manufacturiers et les services qui facilitent la transmission, le stockage et le traitement de l'information par des moyens électroniques. |
| Etats- Unis (1987) | Les industries des technologies de l'information comprend les offreurs comprenant d'une part, les offreurs (grossistes et détaillants) d'ordinateurs et d'équipements informatiques ainsi que d'instruments électroniques de mesure et d'autre part, les logiciels et les industries de services incluant les industries qui fournissent des logiciels « prêts à l'usage » et les services associés aux ordinateurs : les industries d'équipement de communication et de service recensant les offreurs qui fournissent des infrastructures matérielles et immatérielles permettant la connexion entre ordinateur et serveur. |
| Union européenne et France (1998) | Le secteur TIC apparait sous la forme d'une liste d'activités recouvrant trois filières : l'informatique avec la fabrication des ordinateurs et des logiciels, les télécommunications qui comprennent les réseaux et donc Internet et enfin l'électronique. |

**Source:** https://halshs.archives-ouvertes.fr/halshs-00199011 publié le, 18/12/2007.

Aujourd'hui, des organismes tels l'ONU, la Banque mondiale ou l'ITU[11] considèrent que les TIC sont des facteurs et non des conséquences du développement économique. Elles disposent de trois caractéristiques :

- **Omniprésence :** c'est-à-dire que ces technologies sont présentes dans la plupart des secteurs comme l'éducation, la santé, la finance… ;
- **Amélioration :** elles ne cessent de progresser et d'évoluer, en contribuant ainsi à la baisse des coûts pour les utilisateurs, autre à faciliter le quotidiens des usagers ;
- **Source d'innovation :** en plus de leur évolution propre, ces technologies contribuent à l'élaboration de nouveaux produits ou processus.

- **Les TIC, une troisième révolution ?**

De par ces caractéristiques, les TIC contribuent au développement d'autres pans entiers de l'économie. On pourra ainsi dire qu'il s'agit d'une révolution informationnelle. D'abord, car elle a été jaugée par la plupart comme étant « la troisième révolution », classée parmi les mouvements les plus dominants qui ont participé au bouleversement de l'histoire économique

[11] IUT : International Union of Telecommunication, (en Français l'UIT : l'Union Internationale des Télécommunications), est un organisme de division de données et de statistiques sur les TIC dans le monde entier, Genève en suisse.

après la révolution industrielle et l'invention de l'électricité, l'ère des TIC arrive en provoquant des modifications profondes dans la structure de l'économie mondiale. Ainsi, durant sa diffusion, les grandes nations ont vécu une croissance forte et dure, permettant le passage de ces dernières d'une économie traditionnelle appuyée sur les ressources comme richesse des nations à une nouvelle économie [12] fondée sur le savoir qui porte sur l'information et la communication.

Nous avons fait remarquer que les récentes générations des systèmes d'information expriment des caractéristiques complètement différentes des précédentes. En effet, ce sont des technologies mises en œuvre pour faciliter ou réorganiser les processus de travail interactif sur une base non totalement programmée et cela à l'opposé des systèmes d'automatisation des tâches et procédures qui avaient précédé. La plupart des technologies consiste à révéler progressivement des caractéristiques puis à les épuiser, alors que le développement des TIC marque une différence qui fait sa force et son originalité, c'est-à-dire qu'à mesure que la trajectoire se déroule, des ruptures majeurs émergent et touchent chacune une performance particulière[13].

*« Dans les nouvelles économies, la technologie est le conducteur majeur non juste de la qualité de vie améliorée pour le peuple sous développé ou en voie de développement mais aussi un levier du développement économique pour les pays industrialisés, développés et même les pays émergents.»* [14]

**II- Etat des lieux des TIC[15]**

Le rapport de l'UIT (Union Internationale des Télécommunications), de fin 2013, note que chaque jour nous nous rapprochons de l'objectif d'avoir autant d'abonnements au cellulaire mobile que d'habitants sur la planète (6,8 Milliard d'abonnements en cellulaire mobile au total). La révolution des TIC dans les domaines de l'éducation, de la santé, de l'administration

[12] **Nouvelle économie** désigne la croissance générée à partir de la fin des années 1990.

[13] Nathalie COUTINET, HAL (archives-ouvertes), « Définir les TIC pour mieux comprendre l'économie », Décembre 2007, mémoire, Paris, P163.

[14] Adel Ben Youssef, Hatem M. Henni, « Les effets des technologies de l'information et de communication sur la croissance économique », article paru en 2004.

[15] Se référant au rapport de l'UIT de 2013 et 2014.

publique, des services bancaires, de l'environnement et du commerce, permet d'être au service de l'autonomisation de toute personnes.

Les TIC ne cessent de progresser comme le témoignent certains indicateurs : le taux de pénétration d'internet, taux d'abonnements à la large bande fixe et le taux d'abonnements à la large bande mobile, nous démontrons ainsi l'ampleur de la fracture numérique qui persiste dans plusieurs pays et ce sera notre sujet d'analyse dans ce deuxième point (II).

### a) Les TIC dans le monde

L'adoption des TIC dans le monde se poursuit à rythme soutenu au cours des dernières années. Ainsi, vers la fin 2014, le taux de pénétration d'internet a atteint les 42,3%[16] dans le monde et le nombre d'internautes est passé à 3 milliards contre 2,7 milliards en 2013. Mais, malgré tous ces progrès encourageants, on remarque, pourtant, d'importantes fractures numériques entre les régions du monde, 4,3 milliards d'habitants dont 90%[17] ne sont toujours pas connectés vivent dans les pays en développement.

#### a-1) L'accès à internet

« L'Internet a connu, ces dernières années, un développement phénoménal qui touche les pays en développement autant que les pays industrialisés. En Afrique, en particulier, même si les connexions se multiplient moins vite qu'ailleurs dans le monde, l'Internet a beaucoup modifié la donne. En 1994, il n'y avait sur la carte mondiale du réseau Internet que deux pays d'Afrique parfaitement équipés : l'Afrique du Sud et l'Egypte. A l'heure actuelle, tous les pays africains sont peu ou prou connectés au réseau mondial »[18].

[16] Taux estimé le 30 Juin 2014, basé sur une population de 7. 182. 406. 565, source: Internet World Stats- www.internetworldststs.com/stats.html.

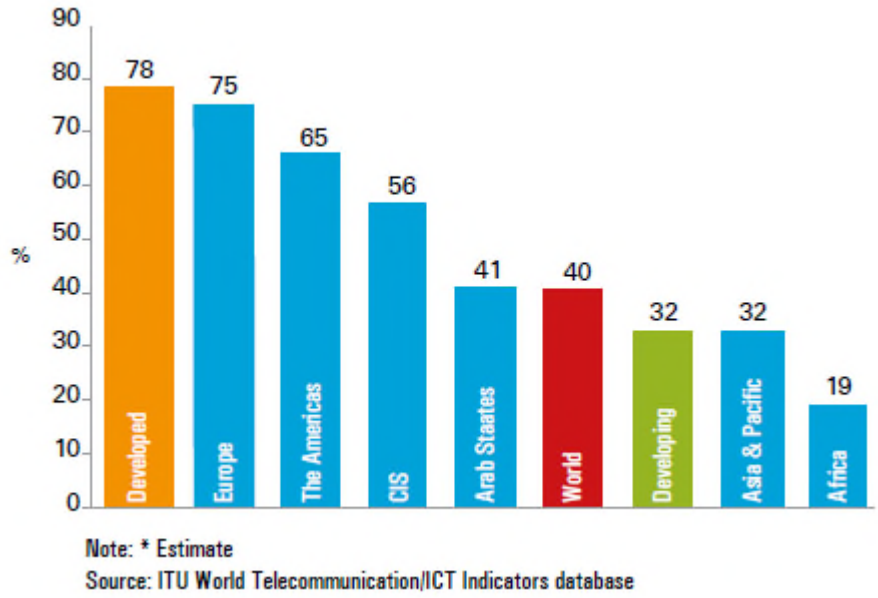
[17] Rapport de l'ITU, « Mesurer la société de l'information », P5, 2014, Genève, SUISSE.

[18] Publication de Clément DZIDONU, Président de l'Institut International des Technologies de l'Information, dans l'**ADEA** (Association of Development of Education in Africa), « Le développement de l'internet en Afrique », 1999, France. http://www.adeanet.org/adeaPortal/adea/newsletter/Vol11No2/fr_9.html

L'utilisation d'internet ne cesse de progresser et deux tiers des internautes vivent dans les pays en développement. En Fin 2014, presque 3 milliards de personnes utilisaient internet et cela correspondait à un taux mondial de pénétration d'internet de 40,4%[19].

Dans les pays développés, 78% des ménages ont eu accès à internet contre seulement 32% des pays en développement, comme le recense la figure 01.

**Figure 01 : Pourcentage d'individus utilisant internet par région (2014*)**




Note: * Estimate
Source: ITU World Telecommunication/ICT Indicators database

En Afrique, près de 20% de la population avait une ligne à la fin de l'année 2014 contre seulement 10 % en 2010. L'Europe a eu le taux de pénétration d'internet le plus élevé du monde avec près de 75% alors que dans les Amériques 65% avaient un accès internet à la fin 2014 et qu'un tiers de la population en Asie-Pacifique avait la ligne cette même année ce qui fait qu'environ 45% des utilisateurs d'Internet dans le monde seraient de la région Asie-Région du Pacifique.

Ce tableau ci-dessous récapitule, par régions du monde, le taux de pénétration d'internet, le nombre d'internautes, la population par région ainsi que la croissance de l'utilisation d'internet de 2000 à 2014.

[19] Rapport de l'ITU, « Mesurer la société de l'information », Genève, 2014, page 13.

**Tableau N°02 : Statistiques mondiales de la population et de l'accès Internet- 30/06/2014**

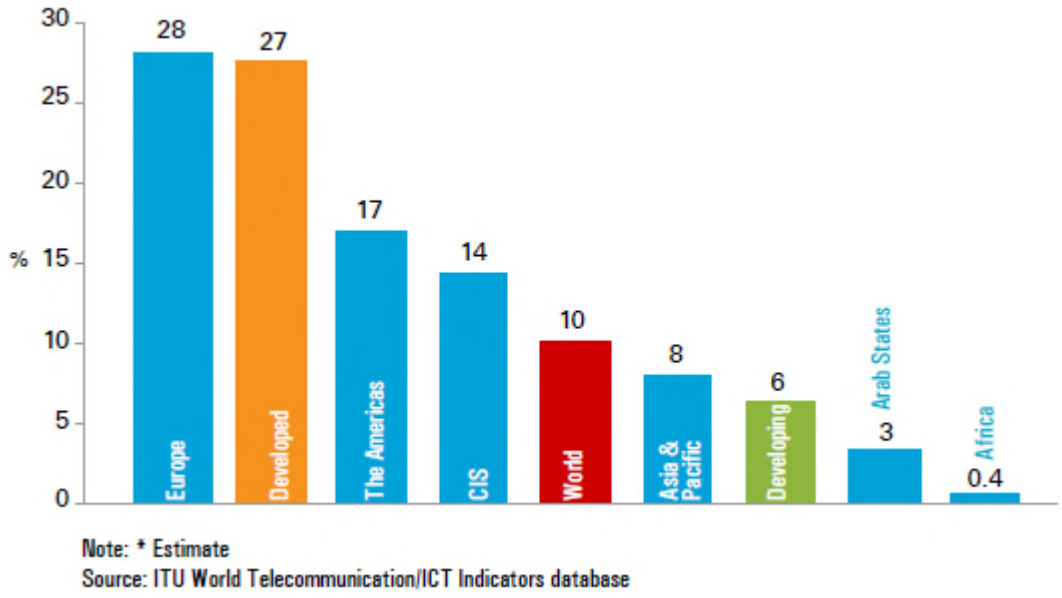
| Utilisation mondiale d'Internet et statistiques des populations 30 JUIN 2014 | | | | | | |
|---|---|---|---|---|---|---|
| **Régions du monde** | **Population (2014)** | **Usagers Internet (2000)** | **Usagers Internet (2014)** | **Pénétration (Population)** | **croissance 2000-2014** | **Utilisateurs d'Internet (%)** |
| **Afrique** | 1,125,721, 038 | 4, 514,400 | **297, 885,898** | 26.5 % | 6,498.6 % | 9.8 % |
| **Asie** | 3,996, 408,007 | 114, 304,000 | **1,386, 188,112** | 34.7 % | 1,112.7 % | 45.7 % |
| **Europe** | 825,824, 883 | 105, 096,093 | **582, 441,059** | 70.5 % | 454.2 % | 19.2 % |
| **Moyen orient** | 231, 588, 580 | 3, 284,800 | **111, 809,510** | 48.3 % | 3,303.8 % | 3.7 % |
| **Amérique du nord** | 353, 860, 227 | 108, 096,800 | **310, 322,257** | 87.7 % | 187.1 % | 10.2 % |
| **Amérique Latine** | 612, 279,181 | 18, 068,919 | **320, 312,562** | 52.3 % | 1,672.7 % | 10.5 % |
| **Océanie / Australie** | 36, 724,649 | 7, 620,480 | **26, 789,942** | 72.9 % | 251.6 % | 0.9 % |
| **TOTAL** | **7,182, 406,565** | **360, 985,492** | **3, 035,749, 340** | **42.3 %** | **741.0 %** | **100 %** |

**Notes: (1)** Le nombre d'usagers, taux de pénétration et statistiques mondiales du 30juin 2014. **(2)** Les informations sur cet indicateur (Internet) sont disponibles et publiées par Nielsen Online, par l'ITU, par GfK, local ICT Regulators et autres.
**Source:** www.internetworldstats.com (Internet World Stat- Usage and population Statistic)

### a-2) L'accès au large bande fixe

En 2014, le taux de pénétration au large bande fixe était de 10%, soit un nombre d'abonnement de 711 million. Mais, dans la plupart des pays développés le large bande fixe était déjà implanté et le taux de pénétration était de 27% (soutenu par un faible taux de croissance de 3,5% contre 4,8% en 2011) alors que dans les pays en développement le taux de pénétration était de 6% (contre 18% en 2011), comme nous verrons ci-dessous :

**Figure 02: Abonnements au large bande fixe en (2014*)**




D'après le rapport de l'UIT, les services étaient devenus plus abordables car en comparaison avec l'année 2013, il y avait près de 700 millions d'abonnements au large bande fixe[20] alors qu'on enregistrait 11 millions de plus en 2014 et un taux de pénétration mondiale de 9,8% contre 10% en 2014.

Le taux de pénétration de large bande fixe en Europe, qui est de 28%, était le plus élevé par rapport aux autres régions ce qui fait presque trois fois plus que la moyenne mondiale (10%), alors que la région des Amériques, par sa faible croissance de haut débit fixe estimé à 2,5%, atteignait un taux de pénétration de 17% à la fin 2014.

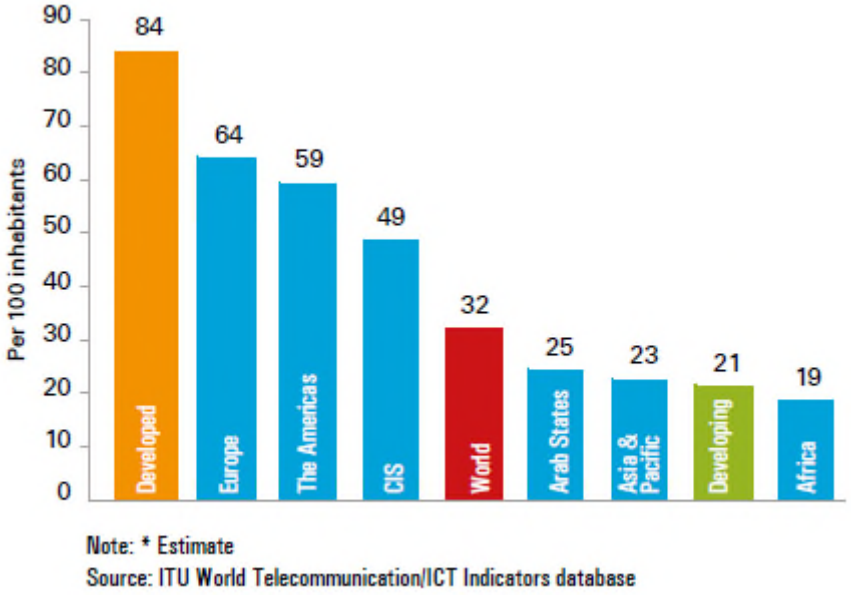
On remarque, un plus grand nombre d'abonnements au large bande fixe dans les pays en développement, par rapport aux pays développés. L'écart reste important en ce qui concerne les taux de pénétration au large bande fixe, qui est de 6% dans les pays en développement et inférieur à 1% en Afrique subsaharienne. Néanmoins, il affiche plus de 754 millions de connexions et plus de 35 opérateurs sur le continent[21], contre 27% dans les pays développés.

[20] Rapport de l'ITU, « Mesurer la société de l'information », Genève, SUISSE, 2013.
[21] Joël MACHARIA, « l'accès à internet n'est plus un luxe », article de la revue « Afrique Renouveau », paru en Avril 2014, page18.

**a-3) L'accès au large bande mobile**

A l'échelle mondiale, le large bande mobile a progressé de façon rapide, des taux de croissance supérieurs à 10% en 2014 avec un taux de pénétration de large bande mobile qui a augmenté de 9% à 32% au cours des 5 dernières années (soit quatre fois le taux observé en 2009). Selon le rapport de l'Union Internationale des Télécommunications, c'est une pénétration alimentée par le succès des smartphones et par les différents types de forfaits offerts sur le marché…etc. Toutefois, une différence reste à signaler entre pays développés et pays en développement avec des taux de pénétration de 84% et 21%, respectivement, comme le démontre la figure ci-dessous :

**Figure 03 : Abonnement au large bande mobile (2014*)**




Ce graphique nous fait remarquer que parmi les pays développés, c'est l'Europe qui a le plus haut niveau de pénétration au large mobile avec 64%, suivie des Amériques avec 59%, des Etats arabes à 25%, l'Asie pacifique à 23%, et enfin l'Afrique 19%. Les Amériques enregistrent plus de 500 millions d'abonnés comparé à l'Asie pacifique qui se voit atteindre 1 Milliard d'abonnés au large bande mobile.

Cependant, l'Afrique se distingue avec un faible taux de pénétration qui frôle les 20% (cela s'explique par la forte croissance dans des pays peuplés comme le Nigéria ou l'Afrique du sud

où le taux de pénétration avait atteint respectivement 37%, 29%, fin2013)[22], mais comparé à quatre ans auparavant où il n'était qu'à moins de 2% on peut dire que la progression dans les pays en développement est rapide. Néanmoins, la fracture entre ces derniers et les pays développés reste importante.

**b) Les banques et les TIC**

Les vagues d'innovation qui se succèdent dans le domaine des TIC a complètement modifié la nature des services bancaires et financiers, car « ils supposent l'utilisation de bases de données de plus en plus riches, de moyens de transmission et de paiement électroniques, de centres d'appels téléphoniques, d'équipements en informatique et téléphonie mobile et surtout de réseaux de télécommunication ouverts, qui ont renouvelé la relation entre les banques et leurs clients ainsi que les prestations financière et les métiers bancaires »[23].

Avec l'introduction d'internet, et grâce à toutes les TIC électroniques, l'industrie bancaire a pris son élan dans l'évolution des prestations de banque à distance et ainsi qu'apparait les banques sans guichet, communément appelée (e-bank) ou encore « Banque Online », qui ont développé d'autres types de services plus récents tel : l'achat de titres, octroi de prêts, en plus des services de carte à puce ou de guichet automatique.

Ainsi, c'est via ces multiples canaux que les clients ont accès aux différentes prestations de services bancaires à distance. Parmi ces services, nous présenterons, ci-dessous, les distributeurs et guichets automatiques bancaires, la carte bancaire,…etc. Nous pourrons, ainsi, dire que les banques sont devenues « multicanal »[24]. Les TIC offrent alors des services qui permettent de répondre à certaines questions qui tournent autour des modes de paiement électronique[25], de facturation électronique[26] et de règlement autre qu'en espèce :

[22] Rapport l'ITU, « Mesurer la société de l'information », Genève-SUISSE, 2014, Page 12.

[23] Michel BERNARD, directeur général adjoint du crédit agricole S.A, revue « HORIZON BANCAIRE » N° 316 - « Banque et nouvelles technologies », Février 2003, page 5.

[24] « Multicanal » correspond à une stratégie dans laquelle internet n'est qu'un moyen parmi d'autres de relation avec la clientèle (les agences, le minitel, centres d'appel téléphonique….), approche privilégiée par les établissements traditionnels.

[25] On entend les paiements effectués à l'aide des cartes de crédit ainsi que des diverses formes de monnaie et de chèques électroniques.

[26] Désigne la présentation et le paiement des factures par internet.

**b-1) Distributeur Automatique de Billets (DAB) et guichets automatiques bancaires (GAB) :**

**Le DAB :**

C'est un appareil qui permet le retrait d'argent avec une carte bancaire et d'un code confidentiel[27] individuel. Les sommes ainsi retirées sont ensuite portées au débit du compte du client[28].

**Le GAB :**

Automate qui permet au détenteur d'une carte bancaire d'effectuer de nombreuses opérations sans la présence ou l'intervention du personnel de sa banque et ce 24 H sur 24. Il permet, également, aux clients de la banque propriétaire du GAB d'effectuer des opérations telles que: la consultation de solde, la demande de RIB, demande de chéquiers, virement de compte à compte au sein de la banque, remise de chèques, versement d'espèces et retrait d'espèces. Les GAB peuvent, aussi, faire fonction de distributeurs de billets (DAB) pour l'ensemble des porteurs de cartes acceptées par l'appareil[29].

**b-2) La carte bancaire** :

Carte délivrée par un établissement de crédit comportant, le plus souvent, une puce électronique et une piste magnétique permettant, selon le cas, d'effectuer des retraits dans les distributeurs de billets et/ou des retraits et des paiements auprès des commerçants[30]. Les premières cartes ont été mises en circulation dés 1967 et à partir de 1970, la carte de paiement devient aussi carte de retrait[31] dans les distributeurs de billet appelés BANKOMAT[32]. Le développement de son utilisation rejoint alors celle des chèques au début des années 2000. On distingue différents types de cartes, parmi elles on cite :

[27] Code permettant au titulaire d'une carte bancaire d'effectuer des retraits ou des paiements en toute sécurité.

[28] Voir : http://www.banque-info.com/lexique-bancaire/d/distributeur-automatique-de-billets--dab

[29] Idem

[30] Idem

[31] Dont la seule utilisation est le retrait d'argent du distributeur ou éventuellement, à un guichet.

[32] Groupe de travail de IFCAM (Institue de Formation du Crédit Agricole Mutuel), « Moyen de paiement et services associés », 2013-2014, www.ca-ifcam.fr

**b-2-1-La carte de retrait**[33] : elle ne peut être utilisée que pour retirer de l'argent dans les distributeurs de billets (soit, uniquement ceux de l'établissement teneur du compte ou alors sur tout le territoire national). Le montant de retrait autorisé par opération et par période de 7 jours est limité.

**b-2-2-La carte de paiement**[34] : elle se représente sous forme d'un rectangle de plastique rigide comprenant, au recto, le nom de la carte, le numéro de la carte, la période de validité (qui est généralement de 2ans), le nom de la banque qui a délivré la carte ainsi que le nom du titulaire de la carte. Le retrait s'effectue dans un distributeur de billet ou de règlements chez les commerçants (qui utilisent un terminal de paiement électronique pour lire la carte) avec un code de 4chiffres que seul le titulaire doit connaître. Elles peuvent être utilisées à l'international (réseau Visa, Eurocard…) et le retrait est limité (exemple : en France, le retrait dans les DAB, est de 300 € par période de 7 jours pour les cartes classiques et 900 € pour les hautes gammes).

**b-2-3-la carte de crédit**[35] : une carte délivrée par un établissement de crédit permettant, entre autres, d'effectuer des paiements auprès des commerçants et dont l'utilisation est adossée à un crédit renouvelable[36]. C'est une carte bancaire classique qui procure certains avantages propres à l'enseigne de distribution (point de fidélité, réduction…). Face à la multitude des cartes de crédit sur le marché, la tentation du client est alors grande dans le fait de multiplier les cartes pour accroître les crédits et donc de se retrouver à un moment donné en situation de surendettement.

**b-2-4-Le porte monnaie électronique MONEO**[37] **:** c'est une carte à puce qui permet de payer les achats de petits montants sans avoir à manipuler de la monnaie et sans code confidentiel. Elle peut se présenter sous une carte spécifique ou alors intégrée dans la puce de la carte bancaire habituelle du client. Elle s'adresse, aujourd'hui, uniquement aux académies ou entreprises pour le paiement du restaurant (Resto U) ou parking.

[33] Jean- Luc SARRAZIN, BTS BANQUE « Techniques bancaires du marché des particuliers », 3e édition, Canada (Québec), 2013, page 52.
[34] Idem.
[35] http://www.banque-info.com/lexique-bancaire/c/carte-de-crédit
[36] Appelé aussi « crédit permanent » ou « crédit revolving », le crédit renouvelable est une réserve d'argent, accessible à tout moment, qui se renouvelle partiellement au fil des remboursements de l'emprunteur
[37] Jean Luc SARRAZIN, op-cite, page 54.

**b-2-5-La e-carte (réseau carte bleu)[38] :** Elle sert à réaliser des transactions sur Internet en toute sécurité. Ainsi, le client obtient une carte virtuelle valable qu'une fois et à un montant fixé d'avance par le client lui-même (lorsque la transaction est réalisée, la carte n'est plus utilisable. Le grand avantage de cette carte réside dans sa sécurité car même en cas de piratage, elle ne pourra être utilisée qu'une seule fois).

**b-2-6-Les cartes de hautes gammes et cartes de prestige[39] :**

- ✓ **Les cartes de hautes gammes :** elles sont destinées à des personnes qui réalisent des retraits importants et des paiements internationaux (exemple : INFINITY chez Visa, PLATINIUM chez Mastercard).
- ✓ **Les cartes de prestige :** Elles sont destinées à des clients qui se rendent souvent à l'étranger et bénéficient de revenu intermédiaire. Elles offrent beaucoup de services mais reviennent plus chers, comme les assurances spécifiques, un plafond de retrait plus élevé, etc.

L'Algérie ne dispose pas de tous ces types de cartes bancaires. Actuellement, on ne distingue que la Carte Interbancaire (CIB), qui est délivrée par des établissements bancaires installés en A1gérie et qui font partie du réseau de la SATIM (Société d'Automatisation des Transactions Interbancaires et de Monétique[40]). La CIB est liée au compte bancaire ou postal (en dinars) du titulaire de la carte. Elle propose deux types de cartes: la **carte GOLD** et la **carte classique[41]**.

**B-3) Chèque électronique :**

Il fait partie des modes de paiement en ligne, conçu pour remplacer les chèques papiers par un modèle électronique qui, pour l'authentification du cyberconsommateur, utilise une signature numérique [42](comparé au chèque traditionnel, là où la signature est manuscrite). Les chèques électroniques seront transmis à leurs destinataires par courriel ou par site Web. L'établissement de crédit, l'entreprise ou même les magasins, disposeront de matériel à lecture automatique des chèques, l'ordre de paiement sera alors numérisé et transmis directement à la banque tandis que le consommateur recevra, par courriel, une confirmation

[38] Idem.

[39] Idem, page 55.

[40] Voir le lien suivant : http://abbinvest.com/index.php?page=blog&var=18

[41] Voir le chapitre 3

[42] Office Québécois de la langue française, « bibliothèque virtuelle », Electronic check ou e-cheque (e-check) (http://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/internet/fiches/8370849.html)

de transaction incluant le numéro du chèque et le montant de cette dernière. « Leur utilisation minimise ainsi les frais de gestion externes pouvant être induits par l'utilisation des cartes à puce ou des cartes de crédit. Une bonne application des e-chèques consiste à les utiliser pour payer les factures mensuelles des achats effectués dans un magasin traditionnel ou dans un magasin on-line »[43].

En Algérie, l'introduction du chèque normalisé (venant remplacer le chèque classique) s'est faite en 2005, mais son utilisation n'a commencé qu'en 2006, selon le rapport de la Banque d'Algérie (BA).

Le tableau ci-dessous, nous présente les différentes prestations de services bancaires effectuées à distance, par exemple et par canal d'accès :

**Tableau N°03 : les prestations de services bancaires à distance**

| **Type de relation** | **Exemple d'utilisation par le client** | **Exemple de canal d'accès** |
|---|---|---|
| ***L'Accès aux informations*** | | |
| -Accès à l'information (interne ou externe) | -Informations sur les produits bancaires<br>-Cours des devises<br>-Cotations boursières | -Internet<br>-téléphone |
| -Accès aux informations individualisées | -Relevé de comptes, encours carte bancaire<br>-Consultation des comptes | -GAB/DAB<br>-Internet |
| Simulation | -Simulation de prêt<br>-Simulation de portefeuille titres<br>-Suivis de budget personnel | -Internet<br>-PC+ Logiciel Money |
| ***Action sur le processus transactionnel*** | | |
| Opération de base | -Virement bancaire<br>-Remise de chèque | -GAB/DAB<br>-Internet<br>-Automate vocal |
| Opérations évoluées | -Ordre d'achat ou de vente de titre<br>-Octroi d'un prêt | -Internet<br>-Services bancaires - téléphonique |
| ***Communication interpersonnelle à distance*** | | |
| Ccommunication en temps réel | -Opposition carte bancaire<br>-Situation d'urgence à l'étranger | -Centre d'appel téléphonique |
| Communication en temps différé | -Réclamation | -Internet (messagerie électronique)<br>-Téléphonie |

**Source :** Horizon bancaire, « l'accès directe au système d'information par le client final via les medias éléctroniques », Sylvie GERBAIX

[43] http://www.itpro.fr/a/cheques-electroniques/

Aujourd'hui, la technologie d'Internet sur les ordinateurs individuels a supplanté les logiciels bancaires spécifiques que les banques avaient diffusés auprès de leurs clients. Le téléphone portable et la télévision offrent, également, un accès Internet qui accélère le recours aux opérations bancaires et financières à distance.

L'usage d'internet dans le domaine bancaire est plus avancé aux Etats Unis et dans le nord de l'Europe. Aux USA, par exemple, un tiers des banques disposaient, en 2000, d'un site Internet, soient 3 500 banques. Un site transactionnel a été développé par 1142 banques et caisses d'épargne qui permettait aux clients de conduire des opérations bancaires.

« Depuis la création en 1995 de la première banque virtuelle, la Security First Network Bank, une dizaine de nouvelles banques fonctionnant uniquement sur Internet ont été agréées par les autorités américaines. Une quinzaine de banques traditionnelles ont lancé une activité Internet sous un nom différent pour attirer de nouveaux clients »[44].

L'activité Internet de courtage sur titres est considérée, aux États-Unis, comme la composante la plus dynamique du secteur financier. Les pays du nord de l'Europe sont, actuellement, les plus avancés pour la diffusion de services bancaires sur le web. Les restructurations bancaires intervenues dans la première partie des années 1990 ont conduit à une diminution sensible du nombre des agences que les banques ont compensé par le développement des services bancaires par Internet.

En Allemagne, les quelques 12 millions de comptes bancaires en ligne représentent 15 % du total des comptes bancaires. Les comptes de titres en ligne, 1,3 million, représentent 6 % du total des comptes titres. En France, plus de 70 établissements de crédit ont établi un site Internet dont près d'une trentaine proposent la consultation des soldes des comptes et plus d'une vingtaine offrent des services de réalisation de certaines opérations bancaires[45].

[44] Etude du rapport annuel de la commission bancaire 1999.

[45] Voir le site : < http://www.comscore.com/fre/actualites_et_evenements/Press-Releases/2012/2/The-Netherlands-and-France-Have-the-Highest-Penetration-of-Online-Banking >

**Tableau N°4 : Top 5 des marchés européens de services bancaires en ligne**

| **Top 5 des marchés européens de services bancaires en ligne, classés en pourcentage de reach, Décembre 2011<br>Total Audience Européenne, 15 ans et plus, Domicile et travail** | | |
|---|---|---|
| | **Services bancaires** | |
| | **Total visiteurs uniques (en milliers)** | **Pourcentage de reach** |
| Pays-Bas | 7 954 | 66,3% |
| France | 25 782 | 59,9% |
| Suède | 3 489 | 55,9% |
| Royaume-Uni | 19 943 | 53,2% |
| Finlande | 1 804 | 53,1% |

**Source :** comScore Audience Metrix- bilan de l'usage d'internet en Europe pour le mois de décembre 2011.

« 2 internautes néerlandais sur 3 ont accédé à des sites de services bancaires en ligne. Les sites de services bancaires en ligne ont atteint 66,3% de l'audience totale internet au Pays-Bas, plus fort taux de pénétration en Europe. Les Pays-Bas ne sont pas seulement le premier marché en Europe mais également à l'échelle mondiale. La France arrive en seconde position avec 59,9% de l'audience accédant à des sites comme ceux du Crédit Agricole ou de la Société Générale. Les internautes suédois sont également friands des services bancaires en ligne (55,9%) et positionnent ainsi le pays en troisième place du classement Européen »[46].

**B-4) Le m-banking** (ou m-payment)

Au delà des services offerts par la banque, on voit émerger un autre type de service offert par les opérateurs téléphoniques au profit de la banque ; l'Afrique est la région du monde où le développement des téléphones mobiles a été le plus rapide en 2008, le secteur est arrivé a maturité en Afrique du Nord avec un taux moyen de pénétration de 93%. En nombre d'abonnés (pour l'année 2008), le Nigeria 60 millions, l'Afrique du Sud 47 millions, l'Egypte

[46] http://www.comscore.com/fre/actualites_et_evenements/Press-Releases/2012/2/The-Netherlands-and-France-Have-the-Highest-Penetration-of-Online-Banking.

37 millions, l'Algérie 31 millions, le Maroc 24 millions et la Tunisie 9 millions. Les opérateurs ont concentré leurs investissements sur les réseaux de deuxième génération (2G), avant de basculer au réseau haut débit de troisième génération (3G), 45% des connexions aux réseaux 3G proviennent de l'Afrique du sud (la Libye et l'Egypte représente 82% pour 2008). Ce phénomène est très important en Afrique, quelques chiffres illustrent ce dernier :

- 5% du PIB, représente les recettes des services de télécommunication.
- 10% de leur revenu mensuel, est la part que consacre les ménages dans la téléphonie, ce dans certain pays comme la Namibie, l'Ethiopie ou la Zambie (alors qu'elle ne représente que de 3% dans les pays développés).
- Le mobile est le moyen de communication le plus utilisé, sa pénétration a atteint 80% contre 55% dans les pays développés.
- Système de cartes prépayées est le plus répandu sur le continent, compte tenu du faible taux de bancarisation de la population, 92% des abonnés à la téléphonie mobile ont adopté le système de « Scratch cards[47] ».
- Déploiement du m-payment, par Orange 2009[48], dans les pays à faible taux de bancarisation où le service devient un levier majeur au développement et au décloisonnement, complément des services bancaires « traditionnels ».
- Le taux de pénétration du mobile est le plus souvent bien supérieur au taux de bancarisation, les services de ***m-banking*** se montrent plus efficients et moins coûteux que les services bancaires traditionnels (Selon la Banque mondiale, seulement 20 % des ménages possèdent un compte bancaire), à travers des partenariats entre banque et compagnie d'opérateur mobile, exemple : En Afrique du Sud, une banque (First National Bank of South Africa) travaille en partenariat avec la compagnie Mobile Telephone Networks (MTN) qui offre des services aux Sud-Africains disposant déjà d'un compte en banque, mais qui désire recevoir et envoyer de l'argent en utilisant leur cellulaire[49],

[47] C'est un système de cartes à gratter.

[48] Article d'Henri Tcheng, Jean-Michel Huet, Isabelle Viennois, Mouna Romdhane, sur « Les télécoms, facteur de développement en Afrique », dans l'Expansion Management Review, N° 129, Editeur Roularta, pp110-120 ; Marc Rennard et Olivier Buonanno, France Télécom Orange. page 9.

[49] Les modèles de *m-banking*, Source : adapté de Bankable Frontier Associates/ Department for international Developement (mai 2006). Thierry Taboy, Sofrecom

Le mobile permet d'accélérer l'accès à des services tels que le paiement en ligne, la banque et le microcrédit ; ce dernier s'inscrivant pleinement dans des usages culturels tels les tontines. Le ***m-payment*** (paiement par téléphone mobile) ouvre ainsi la voie aux micro-financements devenus indispensables aux personnes désirant lancer leurs activités. Depuis l'année 2005, plusieurs offres sont opérationnelles, on cite[50] :

- **M-Pesa :** c'est une plate-forme de *m-payment* développée par le groupe Vodafone au Kenya en collaboration avec le « Financial Deepening Challenge Fund ». C'est un système utilisé pour permettre la distribution des prêts à ses clients, accordés par une institution de micro-finance (FAULU), le remboursement est réalisé via le réseau de distribution de Safaricom.
- **Wizzit** : apparait en 2005 en Afrique du Sud. Issu d'une division de la Banque d'Athènes, ce système fournit aux titulaires de comptes Wizzit un accès conforme au système d'*e-payment* sud-africain, il leur permet de retirer des espèces via la carte de paiement Maestro incluse dans l'offre. Les comptes bancaires Wizzit sont ouverts par des agents, payés à la commission, appelés Wizzkids.
- **Celpay :** lancée en Zambie par l'opérateur Cartel, représente une offre qui permet aux clients de payer et régler des factures ainsi que de transférer des fonds. En 2006, 2 % du PIB du pays ont transité par ce mode permettant à ceux qui n'avaient pas accès au secteur bancaire d'en bénéficier à présent.
- **Zébra :** a était mis en place en 2007 par Orange dans plusieurs de ses filiales. Ce système permet non seulement des rechargements virtuels de crédits téléphoniques mais aussi des opérations *C2C (customer to customer)* et, donc, devient un nouveau moyen d'échanger de l'argent entre individus.

### III- Avantages et risques :

Les nouvelle technologies de l'information et de la communication viennent répondre aux demandes de consommation de tous les pays du monde. La société se transforme et voit émerger le concept de « société d'information »; l'information est en libre accès et offre d'immenses possibilités. Aujourd'hui, les TIC servent de base au développement et à l'utilisation des services en réseau ce qui est avantageux en termes de coût, de renforcement

[50] Voir : <http://www.cairn.info/zen.php?ID_ARTICLE=EMR_129_0110 >

des capacités techniques et humaines améliorant, en conséquence, les conditions de vie des pays. Néanmoins, cette expansion s'accompagne de nouveaux dangers qui portent atteinte à la société d'aujourd'hui[51], visant les infrastructures de l'information et les services Internet.

Certains soulignent, ainsi, que les technologies de l'information et de la communication permettent :

- D'améliorer les mécanismes et les procédures de contrôle (Beniger, 1986) ;
- Une plus grande flexibilité et une moindre dépendance à l'égard du marché, des compétences spécifiques (Walton, 1989, Sproull & al. 1986) ;
- De contribuer à redéfinir les frontières habituelles de la concurrence (Cash et al, 1985) ;
- De renforcer et à créer des liens et des connexions entre l'entreprise et son environnement immédiat (fournisseurs, clients ou autres entreprises du secteur) (Malone & al1987, Johnson & al. 1988)[52].
- Les TIC offrent des opportunités économiques tant aux populations urbaines que rurales. Elles permettent d'augmenter la productivité et l'efficacité des marchés ;
- Les TIC jouent un rôle indéniable dans le développement social [53] : par le **désenclavement des territoires** : exemple de la fondation Vodafone pour les Nations Unis qui ont mis en place un plan permettant le financement de l'association télécoms sans frontières, ce projet consiste à mettre en place, à n'importe quel endroit de la planète, des centres de communications d'urgence (raccordement à un réseau de téléphonique, connexions Internet…) ;
- Les TIC contribuent au **développement des soins**[54] : la médecine à distance offre une bonne solution. Exemple : en République sud-africaine, un système de suivi des malades de la tuberculose a été mis en place : l'envoi des SMS permet de rappeler la prise de médicament aux heures nécessaires. Aussi, par le biais de rappels réguliers, permet d'insister sur l'importance de la contraception et de la vaccination, consultation à distance pour le traitement de la cataracte où le médecin ausculte les malades grâce aux images transmises, etc.

[51] Rapport de l'UIT, « Comprendre la cybercriminalité : Guide pour les pays en développement », Avril 2009, page 10/11.
[52] Pour une synthèse de ces relations entre les technologies de l'information et la structure des organisations, on pourra, notamment, se reporter à Rowe et al. (1995) ou Markus et al. (1988).
[53] Henry Tcheng, Jean Michel Huet, Isabelle Viennois, Mouna Romdhane, 2008, article sur « Les télécoms facteur de développement en Afrique », de la revue « l'Expansion Management Review » n° 129, Ed Express Roularta, pp110-120. (http://www.cairn.info/zen.php?ID_ARTICLE=EMR_129_0110 )
[54] Op-cit

- **l'enseignement a distance**[55] : il constitue un levier important pour le développement de l'éducation. Exemple : L'université virtuelle africaine (UVA), depuis 1997, forme des scientifiques, des ingénieurs, des techniciens, des hommes d'affaires et des professionnels capables de contribuer au développement de leur pays ;
- Les TIC permettent une augmentation de la rapidité des transactions ainsi qu'une baisse de leurs coûts ;

Au fur et à mesure que les TIC se développent, des risques sont en nette hausse, exogène et qui ne sont pas un facteur de perturbation, et sont classés en fonction de leur nature :

- **Les accidents** : comportent les accidents physiques (incendies, explosion, dégâts des eaux), pannes, force majeure (tremblement de terre, tempête, inondation), pertes de services essentiels (électricité, télécommunication) ;
- **Les erreurs** : comme les erreurs de conception, les erreurs de réalisation et les erreurs à l'utilisation ;
- **La malveillance**[56] : on recense les vols et vandalismes, les fraudes (utilisation non autorisée des ressources du système d'information pour un travail personnel, pour le détournement de fond ou d'information), les attaques logiques (sabotage immatériel, infection informatique, cheval de Troie, virus…), divulgations (utilisation non autorisée des ressources du système d'information).

**Conclusion :**

De toutes les Technologies d'information et de communication, Internet est l'outil le plus utilisé, un élément majeur mais qui, à lui seul, ne peut impulser le développement en vu de tous les services qu'il procure, les organisations y deviennent dépendantes, ce qui introduit une certaine vulnérabilité. Il comporte des dangers parfois méconnus ou même laissés dans l'ombre, et ils se rencontrent dans presque tous domaines : atteintes à la vie privée, violence du contenu de certain sites visités, cyber escroquerie, cyber délinquance et la

[55] Op-cit
[56] Se point est développer dans la section 02.

désinformation[57], etc. Autant de délits qui peuvent être réunis et expliqués en un seul terme « Cybercriminalité »[58].

[57] Qui est l'utilisation d'informations erronées
[58] Voir la section 02

## **Section 02 : Le phénomène de cybercriminalité**

La tendance à la numérisation est grandissante, et parmi les infrastructures les plus croissantes des TIC, Internet reste la plus rapide. La demande de connectivité à Internet et d'interconnexion des systèmes a conduit à l'intégration de l'informatique dans des produits notamment les voitures et les bâtiments, la distribution d'électricité, les infrastructures de transport, les services (notamment logistiques) des armées, les services bancaires[59], etc. En effet, au tout début, l'internet n'a pas été développé avec un système de sécurité. Ses composants (en matériels, logiciels et protocolaires) étaient et demeurent soumis à de nombreuses failles qui ont favorisé l'émergence de nouvelles formes de criminalités et de comportements déviants dans le cyberespace. C'est ainsi que la cybercriminalité est née[60].

La cybercriminalité peut toucher aussi bien les citoyens que les entreprises et les administrations et même un Etat. « La cybercriminalité fait chaque jour plus d'un million de victimes dans le monde. Certaines subissent un vol de données bancaires et de carte de crédit par le biais de courriels semblant provenir de leur banque. D'autres se font escroquer par de faux sites marchands ou sont victimes d'un piratage de leur téléphone intelligent. Les médias sociaux sont également la cible d'attaques; à titre d'exemple, jusqu'à 600 000 comptes Facebook subissent chaque jour des tentatives de piratage »[61].

Dans cette section, nous allons essayer de cerner le concept de « Cybercriminalité » adopté par l'Europe et les Etats Unis, puis relayer quelques indicateurs concernant les cyber-crimes et, surtout, trouver ce qui motive les cybers délinquants. Dans le deuxième point, on a jugé nécessaire de faire une distinction entre cybercriminalité et criminalité apparentée….

[59] Rapport de l'IUT : « Comprendre la cybercriminalité : guide pour les pays en développement », Avril 2009.
[60] Ali El AZZOUZI, « La cybercriminalité au Maroc », Casablanca (Maroc), 2010, page 14.
[61] Commission européenne, Affaire intérieures, La cybercriminalité, voir le lien : http://ec.europa.eu/public_opinion/whatsnew_fr.htm (Avril 2012). ou a télécharger en PDF sous : < https://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCEQFjAA&url=http%3A%2F%2Fec.europa.eu%2Fdgs%2Fhome-affairs%2Fe-library%2Fdocs%2Fcybercrime_fact_sheet%2Ffactsheet_cybercrime_v.03_fr.pdf&ei=e7RVVcmCI4LzUtTzgKAJ&usg=AFQjCNF-OhNNqy1f-JD6KIrDSYXz6mjRPg&bvm=bv.93564037,d.ZGU >

**I- Qu'est-ce que la cybercriminalité :**

La cybercriminalité reste, encore, un concept flou. Au travers de ce point, nous allons d'abord citer les définitions légales adoptées par certains Etats et celles proposées par des organismes tels l'OCDE et l'ONU. Puis, nous allons essayer de décortiquer et d'expliquer ce phénomène en commençant par son historique, démontrant l'impact économique qu'il pourrait avoir et, enfin, les motivations des individus à commettre des actes cybercriminels.

**I-1) Définitions légales de la cybercriminalité :**

Nous allons présenter des définitions légales de la cybercriminalité, dictées par l'Europe selon la convention de Budapest du 23 novembre 2001, et celles adoptées par les Etats Unis et qui diffèrent d'un Etat fédéral à un autre, ajoutant à cela la définition proposée par l'OCDE et l'ONU :

**a) Définitions adoptée en Europe :**

La cybercriminalité est, donc : « *Ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la communication, ainsi que celles dont la commission est facilitée ou liée à l'utilisation de ces technologies* ». (Convention de Budapest du 23 novembre 2001) ;

La Commission européenne précise que *« la cybercriminalité devait s'entendre comme des infractions pénales commises à l'aide de réseaux de communications électroniques et de systèmes d'informations ou contre ces réseaux et systèmes »*.

**b) Définition adoptée au Etats unis :**

Le concept de cybercriminalité aux Etats Unis diffère d'un Etat à un autre et d'un département de police à un autre. Selon le Département de la justice (United states department of Justice), la cybercriminalité est considérée comme « une violation du droit pénal impliquant la connaissance de la technologie de l'information pour sa pénétration, son investigation ou ses procédures pénales »[62].

De son coté, le Code pénal de Californie (section 502), définit une liste d'actes illicites qui tombent sous le coup de la cybercriminalité. Il considère comme cybercriminalité le fait :

« *D'accéder, ou de permettre intentionnellement l'accès, à tout système ou réseau informatique afin a) de concevoir ou réaliser tout plan ou artifice pour frauder ou extorquer ;*

[62] *U.S. Department of Justice* <http://www.justice.gov/>.

*b) d'acquérir de l'argent, des biens, ou des services, dans le but de frauder ; c) d'altérer, de détruire, ou d'endommager tout système, réseau, programme ou données informatiques* »[63].

En revanche, le Code pénal du Texas (section 33.02) considère comme cybercriminalité, le fait d'accéder à un ordinateur, à un réseau, ou à un système informatique sans avoir l'autorisation de son maître [64] . La confusion opérée par ces législations, entre la cybercriminalité et la criminalité informatique, s'avère symptomatique d'une difficulté d'appréhender cette forme de délinquance. Ainsi, M. WALL déclare que : « *le terme cybercriminalité ne signifie plus qu'un acte illicite qui est d'une façon ou d'une autre relatif à l'ordinateur* »[65].

**Dans le cadre du 10éme Congrès des Nations-Unies** (2000), la cybercriminalité était définie comme: *"toutes les formes d'activités criminelles conduites à partir d'un ordinateur dans l'espace d'un réseau local ou d'une entreprise, ainsi que d'un réseau plus large comme Internet"*, ou encore *"toute infraction susceptible d'être commise à l'aide d'un système ou d'un réseau informatique, dans un système ou un réseau informatique, ou contre un système ou un réseau informatique"*.

**c) Définition adoptée par l'OCDE :**

La cybercriminalité renvoie à « *tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou de transmission de données »*[66] ;

**d) Définition adoptée par l'O.N.U :**

Elle traite de « *tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent »*[67].

[63] Code pénal de l'Etat de Californie (section 502).

[64] Code pénal de Texas (section 33.02).

[65] D. WALL, "Crime and the Internet" (N.Y., Routledge), 2001, p. 3.

[66] H. ALTERMAN et A. BLOCH, « La Fraude Informatique » (Paris, Gaz. Palais), 3 sep. 1988, p. 530.

[67] Dixième Congrès des Nations Unies, à Vienne, sous le titre « la prévention du crime et le traitement des délinquants », [10 – 17 avril 2000], disponible sur <http://www.uncjin.org/>,(consulté le 12/11/2014).

**I-2) Démystification de la cybercriminalité** (Proposition de définition) :

Pour révéler la réalité et enlever le flou qui se pose sur ce phénomène, on propose de définir le lieu de ces crime « le cyberespace », puis donner un historique sur les attaques cybercriminelles et son évolution dans le temps, démontrer ses dimensions, souligner l'impact assez important sur l'économie et définir, enfin, les motivations qui poussent les cyberdélinquants à agir.

**a) Le cyberespace** :

Le terme cyberespace[68] est forgé par William Gibson où il le décrit comme un lieu dépourvu de murs. Le cyberespace se présente comme un espace indéfini, un espace virtuel [69] d'ordinateurs tous reliés entre eux grâce à des réseaux explorés par les cybernautes.

**b) Historique et évolution des attaques cybercriminelles :**

Malgré l'actualité de ce phénomène, la cybercriminalité est apparue dans les années 60 avec les premiers outils informatiques, et depuis elle n'a cessé d'évoluer avec l'évolution de la technologie devenant ainsi plus complexe et plus dure à cerner.

- **Les années 60 : Les premiers débats sur la délinquance informatique**

Dans les années 60, les systèmes informatiques introduits étaient plus compacts et moins Coûteux[70]. Dès les premières années, des infractions apparaissaient et visaient à détériorer physiquement les systèmes informatiques et les données stockées. Par exemple, au Canada et

[68] Le préfixe « cyber » serait emprunté au terme « cybernétique » créé à partir du grec *Kubernésis* ou *kubernân* qui signifie « l'action de diriger ou de gouverner ». Le terme serait utilisé pour la premier fois en 1948 par l'un des ses pères fondateurs, N.WIENNER, dans son ouvrage « *Cybernetic or control and communication in the machine* »(Cybernétique ou contrôle et communication dans une machine) qui voulait signifier, par cyber, la science nouvelle destinée à couvrir tous les phénomènes mettant en jeu des mécanismes de traitement de l'information. GIBSON est considéré comme étant le parrain du lexique foisonnant des « cybermots » dont, notamment : *cybercriminalité, cyberespionnage, cyberterrorisme, cyberpolicier, cybervigilance, cybercafé, cyberespace...*, pour désigner un fait, un acte ou une activité réelle qui se transposerait dans l'espace virtuel du Net. A ce sujet, lire : M. CHAWKI., p.10 ; Stéphane LEMAN-LANGLOIS, Criminologie, vol. 39, N°1, 2006, p.65, disponible sur les site :www.erudit.org

[69] Selon le philosophe Pierre LEVY « *Est virtuelle une entité déterritorialisée, capable d'engendrer plusieurs manifestations concrètes en différents moments et lieux déterminés, sans être pour autant elle-même attachée à un endroit ou à un temps particulier* ». Sur la nature de cyberespace, voir : <http://www.archipress.org/levy/index.html> (consulté le, 14/11/2014).

[70] Voir: Slivka/Darrow, "Methods and Problems in Computer Security", Journal of Computers and Law, 1975, p. 217 *et seq.*

en 1969, une manifestation d'étudiants provoque un incendie entraînant la destruction des données informatiques hébergées au sein de l'université[71].

C'est vers le milieu des années 60, que les Etats-Unis ont entamé les premiers débats portant sur la création d'une autorité centrale chargée du stockage des données pour l'ensemble des ministères[72]. Ainsi, l'utilisation abusive des bases de données et les risques qu'elle présente en termes de respect de la vie privée sont abordés[73].

- **Les années 70 : Apparition des ordinateurs dans le secteur économique**

Dans les années 70, l'utilisation des systèmes et des données informatiques a pris de l'ampleur. A la fin de la décennie, et avec la baisse des coûts, la technologie informatique a été largement adoptée au sein de l'administration et des entreprises ; le nombre d'ordinateurs centraux utilisés aux Etats-Unis a été estimé à 100 000[74]. Cette période se caractérisait par une évolution des atteintes à la propriété lancées contre les systèmes informatiques [75] (qui dominaient dans les années 60), vers de nouvelles formes d'infractions assistés par ordinateurs, dont notamment l'utilisation illicite des systèmes informatiques [76] et la manipulation des données électroniques.

- **Les années 80** : **Emergence des copies illégales et des violations des droits de propriété intellectuelle**

Cette période a connu l'augmentation mondiale des ordinateurs personnels et du nombre des systèmes informatiques. Cette évolution a connu des effets indésirables, parmi eux l'émergence de l'intérêt porté aux logiciels qui engendrent les premières formes de piratage (copies illégales) et d'infractions liées à la propriété intellectuelle (intrusion de système). En distribuant des logiciels par le biais des réseaux, les délinquants ont été en mesure de diffuser des programmes malveillants et des virus informatiques ont vu le jour.

[71]Consulté : Kabay, "A Brief History of Computer Crime: An Introduction for Students", 2008, page 5, voir sous le lien : www.mekabay.com/overviews/history.pdf.
[72] Ruggles/Miller/Kuh/Lebergott/Orcutt/Pechman, Rapport du Comité sur la préservation et l'utilisation des données économiques, 1965, voir le lien:
<www.archive.org/details/ReportOfTheCommitteeOnThePreservationAndUseOfEconomicData1965 >
[73] Pour un aperçu du débat aux Etats Unis et en Europe, voir: l'article de Sieber, « Computer Crime and Criminal Law », 1977.
[74] Stevens, "Identifying and Charging Computer Crimes in the Military, Military Law Review", Vol. 110, 1985, p. 59.
[75] Gemignani, "Computer Crime: The Law in '80, Indiana Law Review", Vol. 13, 1980, page 681.
[76] Freed, "Materials and cases on computer and law", 1971, p.65.

**Quelques exemples :**

- En **1981,** Ian Murphy, alias « Captain Zero », a été la première personne inculpée pour un crime informatique aux Etats unis, suite à son intrusion dans le système informatique de la société AT&T[77], il a réussi à modifier le programme de facturation étendant les heures creuses à toute la journée.
- En **1986,** Le premier virus informatique voit le jour au Pakistan, il se nommait « Brain » et infectait les ordinateurs IBM.
- En **1987,** Le virus « Jerusalem » a été détecté alors qu'il a été conçu pour supprimer les fichiers infectés les vendredi 13. C'est le premier virus capable d'infecter et de détruire des fichiers.

- **Les années 90 : Les premières affaires de cybercriminalité**

Dans cette décennie, il eu l'arrivée de l'interface graphique « WWW », qui avait contribué à accroitre le nombre d'internautes et à entrainé de nouveaux défis. La rapidité de l'échange d'informations a fait augmenter la complexité des enquêtes relatives aux délits commis qui n'étaient jusque là limités qu'au niveau local mais avec internet ils acquéraient une dimension transnationale[78].

**Quelques exemples :**

- En **1991,** Dark Avenger a créé MTE qui est un logiciel permettant de rendre des virus polymorphes, c-à-d pouvant se transformer en plus de 4 000 milliards de formes différentes, et donc extrêmement difficiles à détecter.

- En **1994,** Vladimir Levin, un mathématicien russe inculpé pour une affaire de fraude informatique, s'est introduit au réseau informatique de la CityBank et avait effectué un virement de 10 millions de dollars sur son compte bancaire.

- En **1995,** un vol de 20 000 numéros de cartes de crédit a été effectué par Kevin Mitnick.

[77] Le plus grand fournisseur de services téléphoniques locaux et de longue distance des Etats Unis.
[78] Pour plus de détail sur la dimension transnational des cybercrimes voir: Sofaer/Goodman, « Cyber Crime and Security » – « The Transnational Dimension of Cyber Crime and Terrorisme», 2001, page 7.

- En **1998 :** deux événements ont eu lieu :

**1)** Piratage du site New York Times et de sites militaires U.S ;

**2)** Apparition du « Cheval de Troie » qui permettait un accès complet aux PC (Personnel Computer) infectés[79].

- En **1999,** il s'est produit un hacking d'une banque chinoise et un détournement de 87000 dollars par deux cybercriminels chinois. Des groupes de hackers serbes menaçaient l'OTAN en affirmant de détruire leur système informatique en réponse à la guerre contre la Serbie.

- **Les années 2000 à nos jours (21ème Siècle**) :

Tout comme les décennies précédentes, ce siècle voit naître de nouvelles formes d'infractions assistées par ordinateur et de cyberdélit. Parmi elles, le « hameçonnage »[80] et les « attaques par botnet »[81] ainsi que les infractions commises au travers des communications par «voix IP»[82] et de «l'informatique en nuage »[83]. Les Etats et les organisations régionales et internationales tentent de relever ces défis qui se présentent à eux plus complexes et conséquents et s'efforcent de proposer des solutions selon le degré de priorité accordé à la cybercriminalité.

**Quelques exemples :**

- En **2005**, Farid Essebar, aussi connu sous le pseudonyme de Diabl0, était le créateur du virus informatique « Zotob », qui a affecté des institutions comme le département de la sécurité intérieure américain et les médias comme CNN et le New York Times.

[79] David S. Wall, "Cybercrime, *The Transformation of Crime in the Information Age"*, Polity Press, 2007, p 47.
[80] Le « Hameçonnage », communément appelé *phishing*. Il s'agit d'une escroquerie qui abuse de la crédulité de l'internaute afin de lui soutirer des renseignements personnels.
[81] BotNet (acronyme de Bot (Robot) et Net (Réseau)) est un réseau de milliers à plusieurs millions d'ordinateurs compromis par un parasite de zombification. Ces " Machines Zombies " sont regroupées sous le commandement d'un pirate qui peut ainsi exploiter la somme des puissances de calcul et des largeurs de bandes passantes de tous "ses" Zombies. Ces BotNets sont loués à des commanditaires, cybercriminels, pour lancer de violentes vagues de **Spam** ou de Phishing ou des attaques en Déni de service faisant " tomber " les serveurs internet des cibles contre lesquelles on s'oppose où dont on veut extorquer de l'argent (gouvernements, administrations, sociétés commerciales, banques, sites de jeu en ligne, etc. ...).
[82] Simon/Slay, Voice over IP: Forensic Computing Implications, Article de 2006.
[83] Velasco San Martin, Jurisdictional Aspects of Cloud Computing, 2009; Gercke, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, P. 499.

- En **2012 (**Aout)**,** le groupe pétrolier Aramco a été la cible d'une cyberattaque[84] et plus de 30 000 ordinateurs du groupe pétrolier, basé en Arabie Saoudite, on été infecté par un virus extérieur.

- En **2014,** « Gameover Zeus », un des plus vastes réseaux de machines zombies (botnets) qui permettait de contrôler un programme espion destiné à pénétrer dans les comptes bancaires des victimes et de piloter Crypto-locker, un logiciel qui crypte les données des victimes et réclame ensuite une rançon pour les décrypter.

- En **2015,** le site de la compagnie aérienne allemande Lufthansa[85] a été victime d'une attaque informatique, le vendredi 10 avril. Des individus ont réussi à se procurer les données personnelles d'utilisateurs du site LH.com. L'attaque a été menée via un « botnet » (machine zombie), une série de noms d'utilisateurs et de mots de passe ont été automatiquement testés jusqu'à l'aboutissement du méfait. Aussi, en Avril 2015, la chaine TV5 monde a été victime de piratage par des militants islamistes se revendiquant de l'organisation Etat Islamique (EI)[86].

### c) Dimension de la cybercriminalité :

Selon le rapport de l'UIT, la cybercriminalité est souvent présentée par une dimension internationale. Les contenus illicites qui se transmettent par courrier transitent souvent par plusieurs pays avant d'atteindre leur destinataire. Ils sont parfois stockés à l'étranger, c'est pourquoi les Etats concernés par un cyberdélit doivent collaborer aux enquêtes diligentées[87]. Partout dans le monde, l'informatique repose fondamentalement sur la même technologie. Les ordinateurs et les téléphones portables vendus en Asie ressemblent de très près à ceux vendus en Europe. Même chose pour le cas d'Internet, car avec la normalisation des réseaux, les pays africains utilisent les mêmes protocoles que les Etats Unis[88]. C'est pour cela que les internautes du monde entier peuvent avoir accès aux mêmes services. L'harmonisation des normes techniques a donc permis la mondialisation des technologies et des services,

[84] Plus d'informations sur le lien suivant : http://www.zdnet.fr/actualites/le-groupe-petrolier-aramco-cible-d-une-cyberattaque-l-acte-d-activistes-39775459.htm
[85] Plus de détail voir : http://www.lenetexpert.fr/lufthansa-victime-dune-cyberattaque-le-net-expert-informatique/
[86] Voir : http://www.lenetexpert.fr/la-chaine-tv5-monde-victime-dun-piratage-de-grande-ampleur-par-des-individus-se-reclamant-du-groupe-etat-islamique-le-net-expert-informatique/
[87] Voir : Putnam/Elliott, International Responses to Cyber Crime, in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism, 2001, P.35.
[88] Les plus importants protocols d'informations sont : TCP (transmission control protocol) et le IP (Internet Protocol) ; pour plus d'information voir: Tanebaum, « Computer Networks », 2002; Comer, « Internet working with TCP/IP – Principles, Protocols and Architecture », 2006.

seulement elle devrait également conduire à l'harmonisation des législations nationales (ce qui pourrait être une bonne initiative pour l'Algérie). Comme l'ont démontré les négociations de la convention du Conseil de l'Europe sur la cybercriminalité, le droit national évolue beaucoup plus lentement que les techniques.

Alors, si Internet ne connait pas de contrôle aux frontières, des moyens de restriction de l'accès à certaines informations[89] tel que le blocage de l'accès à certains sites et le refus de connexions venant de certains pays, et cela par le filtrage des adresses IP[90] (le « ciblage IP[91] »). Certes, ces mesures ne sont pas sans failles, n'empêche, elles restent utiles pour préserver les différences territoriales dans un réseau mondial.

**d) L'impact économique de la cybercriminalité :**

L'ampleur de la cybercriminalité va continuer à croitre au fur à mesure que les activités des entreprises et les services se font en ligne et que le nombre d'internautes à travers le monde augmente. Selon certains rapports relatifs à l'impact de la cybercriminalité en 2014, on retient :

**d-1) Le marché de l'emploi :**

Les entreprises sont des victimes parmi d'autres des attaques cybercriminels entrainant des pertes d'information, de vol de propriété intellectuelle…etc. Le rapport CSIS[92], de juin 2014, a mesuré l'impact des attaques sur la création de l'emploi et d'après eux, les cybercrimes auraient conduit à la perte de 200.000 emplois aux USA et à 120.000 en Europe[93].

**d-2) Le coût[94] :**

Le coût annuel de la cybercriminalité est estimé à plus de 400 milliards de dollars (entre 375 et 575 milliards de dollars) pour l'économie mondiale. Ce coût comprend les conséquences du

[89] Voir :Zittrain, History of Online Gatekeeping, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2,P.253.

[90] Une adresse IP : est un numéro d'identification qui est attribué de façon permanente, ou provisoire, à chaque appareil connecté à un réseau informatique utilisant l'Internet.

[91] Le ciblage IP : est une démarche de géo-localisation sur adresse IP et qui peut être utilisée pour le ciblage publicitaire dans le cadre des campagnes de publicité en ligne. Après avoir intégré au sein de leurs solutions une des bases d'adresses IP qualifiées au niveau géographique.

[92] Rapport CSIS -Center for Strategic and International Studies, 2014. < http://www.tomshardware.fr/articles/cybercriminalite-attaque,1-53657.html>

[93] D'après le rapport du CSIS (Center for Strategic and International Studies) sponsorisée par McAfee. Voir le lien : < http://www.tomshardware.fr/articles/cybercriminalite-attaque,1-53657.html>

[94] Selon Abdelaziz Derdouri, Directeur General SSRI, article sur « Impact économique global de la cybercriminalité : 445 milliards de dollars », 9juin 2014. Voir le lien : <http://www.ssri.dz/impact-economique-global-de-la-cybercriminalite-en-2013-400-milliards-de-dollars/ >

vol d'informations personnelles de millions de personnes. En 2013, ces vols ont concernés plus de 40 millions d'internautes aux Etats Unis, 54 millions en Turquie, 20 millions en Corée du Sud, 16 millions en Allemagne et plus de 20 millions en Chine. D'après les estimations de 2013, il y a eu plus de 800 millions de fichiers personnels volés. La cybercriminalité coûte extrêmement cher, elle est rendu plus lucrative que le marché mondial du cannabis, de la cocaïne et de l'héroïne confondues (D'après le rapport Norton Cybercrime, 2010)

**e) Les motivations des cybercriminels :**

Le cybercrime est une activité à croissance démesurée. Les opérations de cybercrime ont comme facteur commun l'anonymat virtuel dont profitent les cyber-attaquants, car leurs chances d'être détectés sont moindres. Cette activité attire différents types de personnes qui utilisent leurs propres techniques et méthodes pour s'impliquer, ils ont des motivations propres à eux. Il est parfois difficile de cerner toutes les motivations des cybercriminels mais en gros, on peut distinguer quatre (04) des plus majeures[95] :

**e-1) L'idéologie** : elle vise à défendre une conviction (politique ou religieuse). A travers des attaques, le cybercriminel a pour objectif d'interrompre des services, à diffuser des messages partisans ou à divulguer les données d'une entreprise et ainsi nuire à son image ;

**e-2) Les gains financiers directs** : pour la majorité des cybercriminels, l'argent est la principale motivation[96], il s'agit, par exemple, du vol de données bancaires (en particulier des numéros de cartes), de données personnelles mais aussi de données critiques de l'entreprise comme les secrets industriels ou les informations concernant sa stratégie. Elles seront revendues par la suite ou utilisées pour réaliser des fraudes ;

**e-3) La déstabilisation entre Etats ou le Cyberterrorisme :** est une motivation à laquelle visent les cybercriminels par la destruction des systèmes ou le vol de données stratégiques qui pourraient nuire au bon fonctionnement des services vitaux des Etats ;

[95] Souligné par les synthèses « SOLUCOM », Management & IT consulting, Observatoire de la transformation des entreprises, n° 47, sur la Cybercriminalité : comment agir dés aujourd'hui, Octobre 2013.
[96] D'après les données du Kaspersky Lab, < http://blog.kaspersky.fr/quest-ce-qui-motive-les-cybercriminels-largent-evidemment/372/ >

**e-4) L'obtention de capacités d'attaques :** autre motivation qui se développe. Elle consiste à voler les secrets des mécanismes de sécurité (mots de passe, certificats, failles de sécurité, etc.) ou à attaquer les SI (Système d'Information) des fournisseurs (info-gérants, opérateurs de télécom, fournisseurs de solution de sécurité) de sociétés qui seront visées ultérieurement. Ces éléments sont utilisés plus tard pour lancer la véritable attaque. Les cybercriminels ne se fixent plus aucune limite dans la réalisation de leurs desseins. De nos jours, ces attaques peuvent toucher n'importe quelle entreprise, quel que soit son secteur d'activité. Comme l'a récemment montré l'actualité, ce schéma ci-dessous résume les quelques organismes et Etats qui ont été victimes de cyber attaques :

**<u>Schéma 01 :</u> Les motivations des cybercriminels et quelques exemples d'Etats ou entreprise ciblés**


**Source :** Les synthèses « SOLUCOM », Management & IT consulting, Observatoire de la transformation des entreprises, n°47 sur la cybercriminalité : comment agir dés aujourd'hui, Octobre 2013.

**II- La distinction de la cybercriminalité et les criminalités apparentées :**

Dans le point précédent, on a tenté de définir le phénomène de cybercriminalité dans son ampleur, sa complexité et sa capacité à toucher plusieurs domaines. Certains auteurs tombent

parfois dans la confusion de sens lorsqu'ils désignent sous la terminologie de « pirate » tous les délinquants en informatique. Dans ce présent point, nous allons distinguer entre la cybercriminalité et les criminalités apparentées, d'abords par une distinction relative aux termes juridiques puis par une distinction relative aux auteurs de l'infraction[97].

**II-1) La distinction relative aux termes juridiques :**

La cybercriminalité désigne toute infraction qui implique l'utilisation des technologies informatiques. Ainsi que certaines notions sont exprimées indifféremment comme « criminalité informatique », « délinquance informatique », « criminalité de haute technologie ». La distinction entre la cybercriminalité et ces trois précédentes notions s'établira comme suit :

**a) La cybercriminalité et la criminalité informatique :**

La cybercriminalité et la notion de criminalité informatique sont étroitement liées, cependant il existe une distinction qu'on juge utile de mettre en exergue. La criminalité informatique représente « l'infraction générique dont la cybercriminalité est une variante ». Cette dernière est une forme de criminalité informatique, forme qui ne s'exprime que sur et à travers le réseau de télécommunication, contrairement aux autres délits informatiques qui nécessitent pas d'interaction avec le réseau de télécommunication[98] (M. Chawki, 2006).

Quelques auteurs ont proposé leurs définitions en visant l'ordinateur comme moyen de commettre l'infraction. Selon M. TIDEMANN, la criminalité informatique recouvre « Tout acte illégal commis par ordinateur »[99].

Selon Mme.L.D. BALL, la criminalité informatique est « une action illicite où l'ordinateur joue un rôle principal pour la commettre »[100].

[97] M. Chawki, « Essai sur la notion de cybercriminalité », IEHEI, juillet 2006, P. 25

[98] Voir P. DELEPELEERE, *op. cit.*; E. CESAY, "Digital Evidence and Computer Crime", Academic Press, Londres, 2000, P.9.

[99] K. TIEDEMANN, « Fraude et Autres Délits d'Affaires Commis à l'Aide d'Ordinateurs », Revue. D.C.P, Bruxelles 1984, n° 7, P.612.

[100] L. D. BALL, "Computer Crime in The Information Technology Revolution". T. FORESTER, MIT Press, Cambridge, 1985, PP. 543-544.

**b) La cybercriminalité et la criminalité en col blanc :**

L'auteur américain SUTHERLAND, dans son étude en 1939, était le premier qui ait mit en évidence la délinquance en col blanc « white collar crime ». Selon lui, il s'agissait de la criminalité des classes supérieures en lien avec les affaires, leurs cultures et leur milieu professionnel.

En 1970, H. EDELHERTZ a proposé une définition, acceptable, où il décrivait la criminalité en col blanc comme : « Un acte illégal perpétré sans le recours à la contrainte physique usant de la dissimulation ou l'artifice, afin d'obtenir de l'argent ou des propriétés pour éviter un paiement ou de la perte de l'argent ou pour obtenir des affaires ou des avantages personnels ».

M. DELEPELEERE relève une distinction entre cybercriminalité et criminalité en col blanc, qu'on note comme suit :

- La criminalité en col blanc vise toujours des objets d'ordre économique alors que la cybercriminalité poursuit d'autres buts à caractère politique, par exemple (comme le cyber terrorisme).
- La criminalité en col blanc menace le monde de l'entreprise alors que la cybercriminalité menace, en plus, les particuliers, voir même les Etats. Il conviendrait alors d'affirmer que si la cybercriminalité présente des interactions avec la criminalité en col blanc, il y'a certains délits informatiques qui ne rentrent pas dans cette catégorie, car la criminalité en col blanc est multiple et conditionnée par la nature de l'interaction commise.

**c) La cybercriminalité et la criminalité de haute technologie :**

Selon M. Chawki, la criminalité de haute technologie peut couvrir deux catégories[101] :

- Les infractions liées aux systèmes informatiques non connectés aux réseaux de télécommunications ;
- Les infractions liées aux systèmes informatiques connectés aux réseaux de télécommunications.

[101] M. Chawki, op-cit, P, 30.

Selon la définition donnée à la cybercriminalité, le premier type d'infraction ne tombe pas sous cette catégorie. En revanche, la seconde peut être classée sous la catégorie de la cybercriminalité dans la mesure où les infractions impliquent un réseau de télécommunication. Nous pouvons affirmer que quelques infractions de haute technologie peuvent être considérées comme des cybercriminalités et que d'autres ne peuvent pas l'être.

### II- La distinction relative aux auteurs de l'infraction :

Vu la confusion prêtée au terme « cybercriminalité », certains auteurs commettent parfois des confusions de sens en désignant sous la terminologie de « Hacker » ou « Pirate » tous les délinquants en informatique. Il convient donc de déterminer et distinguer le sens de chacun. On énumère donc les : Hackers, Crackers, Crashers, Phreakers, Carders, et les Script-Kiddies comme suit :

**a) Le Hacker[102] :**

Le terme « Hacker » provient du verbe to hack (en anglais), qui signifie : « une personne qui prend du plaisir à explorer en détail un système programmable et qui cherche sans cesse à étendre ses connaissances dans ce domaine ».

Selon M. Chawki, le terme hacking, comme défini dans le New Hacker's Dictionnary[103], signifie :

- Toute personne qui s'intéresse à explorer les systèmes informatiques ;
- Un expert dans une langue particulière(C+, C++) ou dans des systèmes d'exploitation ;
- Une personne forte dans les détails de la programmation ;
- Une personne qui s'intéresse au défi intellectuel ;
- Un personne qui essaie de découvrir les informations sensibles.

Aussi, le terme hacking est synonyme de « piracy », donc de contrefaçon. Ce qui confère au terme « Pirate » deux notions, on désigne :

- ✓ La personne entrant par effraction à l'intérieur d'un système informatique ;
- ✓ Le contrefacteur, lorsqu'il est utilisé au sens de « piracy ».

[102] Voir le document : M. Chawki, op-cit, P. 32.

[103] A télécharger en format PDF sur le lien suivant: https://www.google.fr/#q=new+hacker%27s+dictionary+pdf

D'après la définition émise par l'OLF (l'office québécois de la Langue Française) sur le pirate informatique[104], on distingue trois formes de piratage informatique :

- ✓ La pénétration des réseaux et systèmes informatiques ;
- ✓ La copie frauduleuse des logiciels ;
- ✓ L'utilisation des programmes comme « cheval de Troie » pour accéder aux systèmes informatiques. D'après J.-F. CASILE[105], le piratage informatique, au sens juridique, est donc la reproduction sans droit d'un logiciel. Et ce sens différent de son sens courant échappe parfois à quelques professionnels du droit pour désigner le pirate.

**b) Le « Crasher »[106]** :

Ce terme provient du verbe to crash (de l'anglais), qui signifie « s'écraser ». Le crasher est considéré comme la personne qui pénètre à l'intérieur d'un système informatique et détruit des données.

**c) Le « Cracker »** :

C'est une personne qui soit détruit ou introduit des données dans le système. Un crack est dit d'un programme chargé de modifier le logiciel original afin d'en supprimer les protections[107].

**d) Le « Phreaker »** :

Désigne l'auteur d'une fraude informatique constituée par l'utilisation des lignes téléphoniques (par la corruption, le détournement de téléphone portable, de modem…etc.).

Pour conclure, la distinction retenue entre le pirate, le Hacker, le Crasher et le phreaker, ne permet pas complètement de déterminer une typologie des délinquants en informatique. Néanmoins, elle met en exergue une différence de nature, d'objet et de motivation que le concept de cybercriminalité ne pourrait contenir[108].

[104] « le criminel informatique qui exploite les failles dans une procédure d'accès pour casser un système informatique, qui viole l'intégrité de ce système en dérobant, altérant ou détruisant de l'information, ou qui copie frauduleusement des logiciels ».
[105] J.-F. CASILE : « Le Code Pénal Á L'Epreuve De La Délinquance Informatique » (Thèse, Aix-Marseille), 2002, P24.
[106] M. Chawki, op-cit, P. 34.
[107] Voir le lien suivant : <http://fr.wikipedia.org/wiki/Cracker_(d%C3%A9plombeur_de_logiciels) >
[108] M. Chawki, Op-cit, P. 35.

**e) Les « Script-kiddies »** :

Ce sont des jeunes utilisateurs du réseau utilisant des programmes trouvés sur Internet pour vandaliser des systèmes informatiques, mais leurs motivation n'est qu'amusement. Peu compétents, ils se contentent d'utiliser des outils d'exploitation automatique pour trouver des machines vulnérables[109]. Néanmoins, ils peuvent présenter parfois une menace réelle pour la sécurité des systèmes.

**f) Les « carders »** :

Ils s'attaquent principalement aux systèmes de cartes bancaires pour en exploiter les failles. Le terme « *carding* » désigne le piratage de cartes bancaires et d'après un spécialiste de la conformité du domaine du secteur financier, ACTIMIZE, le *carding* devient un métier très fructifiant[110].

**Conclusion :**

Le caractère globalisé du réseau Internet ne permet pas d'appréhender la criminalité sur ce dernier vu que c'est un moyen de communication mondiale qui permet la circulation de tous types de données. Ainsi, les délits perdent de leur visibilité et de leur netteté introduisant une certaine confusion chez les citoyens ce qui les pousse à croire qu'ils pourraient commettre en toute impunité, tous types d'infractions sans entrevoir de frontières, de divergences de mobile et de différences de profil des auteurs.

[109] Ali AZZOUZI, « Cybercriminalité au maroc », Casablanca (Maroc), 2010, page 86.
[110] Plus de détail voir : http://www.actimize.com/index.aspx?page=news196.

**CONCLUSION**

Le concept de cybercriminalité, communément utilisé par plusieurs auteurs, se définit comme toute action illégale dans laquelle un ordinateur est l'instrument ou l'objet de délit[111]. Ce phénomène est le fruit d'une évolution économique conduite par le développement des TIC. La cybercriminalité ne se limite pas qu'à Internet, même s'il en est le principal vecteur. Avant tout, il est considéré comme un espace qui abolit les frontières et les barrières culturelles. Une liberté d'information qui revête un aspect fragile incitant à des menées malveillantes voir criminelles inspirées par l'idéologie, la concurrence ou la recherche de gains illicites[112]. Enfin, avec cette nouvelle forme de criminalité, il apparait évident que c'est à l'Etat, aux administrations et aux entreprises de sensibiliser les internautes, de cerner les dangers et les prévenir sans porter atteinte à la liberté fondamentale.

[111]Olivier Iteanu, « Tous cybercriminels », Jacques-Marie Laffont éditeur, 2004, dans le livre de Eric Pryswa, « cybercriminalité et contrefaçon », édition FYP, France, 2010, page 18.
[112] Voir le rapport du groupe de travail Interministériel sur : « La lutte contre la cybercriminalité », par Marc ROBERT, Février 2014, P. 8.

# - CHAPITRE II -

# Chapitre II : La lutte contre la cybercriminalité

## Introduction

En cybercriminalité on distingue deux termes, le «cybercrime » et le « crime assisté par ordinateur ». Alors que le premier est une forme de crime informatique, qui fait appel aux technologies de l'Internet pour sa réalisation [1] (il implique un réseau informatique), le deuxième, désigne les infractions qui affectent uniquement des systèmes informatiques autonomes. En revanche, il est difficile de retenir un critère susceptible d'englober tous les actes et toutes les infractions (étant donné leurs nombreuses différences), il est donc difficile d'élaborer une classification adéquate sachant que la convention du Conseil de l'Europe a tenté d'en donner une.

De leur coté, les cybercriminels emploient un bon nombre de techniques et d'arnaques qui sont devenues très populaires ces derniers temps du fait de la croissance exponentielle des réseaux sociaux, des messageries par e-mail et autres formes de communication électronique. Ces techniques sont très utilisées par les cyberdélinquants dans l'art de la manipulation afin d'obtenir certaines informations sensibles de leurs victimes ou de les convaincre de réaliser certaines actions qui pourraient compromettre leurs systèmes.

Selon Marco GERCKE, la cybersécurité joue un rôle essentiel dans le développement des technologies de l'information et des services en ligne. Pour garantir leur sécurité et leur bien-être économique, les pays doivent absolument renforcer la cybersécurité (et la protection des internautes) en protégeant les infrastructures essentielles de l'information, objectif qui préside aujourd'hui au développement des nouveaux services mais aussi à l'élaboration des politiques gouvernementales. La prévention de la cybercriminalité fait partie intégrante de toute stratégie nationale de cybersécurité et de protection des infrastructures essentielles de l'information comme pour l'Union Européenne et les Etats Unis ; leur stratégie comprend, notamment, l'adoption d'une législation appropriée contre l'utilisation des TIC à des fins criminelles et contre les activités visant à nuire à l'intégrité des infrastructures essentielles du pays, il s'agit là d'une responsabilité commune qui demande de la part des autorités, du secteur privé et de la population, une action coordonnée en matière de prévention, de résolution des incidents et de reprise après incident[2].

Dans ce chapitre, nous verrons, d'abord, les différentes catégories d'infractions liées à la cybercriminalité en première section puis, nous allons prendre, comme exemple, l'Europe et

[1] Rapport de l'UIT, « Cybersécurité, guide pour les PED », 2007, P.43.
[2] Rapport, « Comprendre la cybercriminalité : phénomène, difficultés, et réponses juridiques », élaboré par le professeur Marco Gercke, septembre 2012, P.2.

les Etats Unis dans leur course de lutte et de réponse (politique et juridique) face aux attaques cybernétiques.

## Section 01 : Infractions et techniques de cybercriminalité

Actuellement, l'objet d'attention est le cyberespace en raison du développement économique qu'il représente, mais également pour les menaces dont il recèle. Face à la difficulté d'appréhender la notion de cybercriminalité, et celle du cybercriminel, notre référence émane de la définition posée par la convention internationale de la cybercriminalité qui a été adoptée par le Conseil de l'Europe à Bucarest le 23 novembre 2001. Elle constitue de nos jours le texte international le plus précis et le plus ambitieux en termes de répression des actes cybercriminels. Trois catégories d'infractions sont définies dans la convention, qui sont : 1) les infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes ; 2) les infractions informatiques ; 3) les infractions combinées.

Dans cette section, on essayera d'établir un classement des infractions les plus courantes selon le rapport de l'UIT, puis un ensemble des techniques de la cybercriminalité sera mis en exergue, des infections informatiques jusqu'aux arnaques les plus répondues.

### I) Les différentes infractions :

Selon le rapport de l'UIT, les différentes infractions cybercriminelles sont classées en trois catégories : I-1) Infractions contre la confidentialité, l'intégrité et la disponibilité des données et du système informatique ; I-2) Infractions informatiques ; I-3) Infractions combinées.

#### I-1) Infractions contre la confidentialité, l'intégrité et la disponibilité des données et du système informatique

Cette catégorie d'infractions, porterait atteinte à au moins un des trois principes juridiques : la confidentialité, l'intégrité et la disponibilité. Ce type d'infractions est récent, parmi elles:

##### a) Accès illégal (piratage, craquage) :

Avec le développement d'Internet, Le « Hacking » (piratage), considéré comme l'une des infractions informatiques les plus anciennes[3], est devenu un phénomène de masse ; il désigne l'accès illégal à un ordinateur. Parmi les organisations qui ont été victimes de

[3] Voir l'article de: Levy, "Hacking Offences, Australian Institute of Criminology", 2005.

piratage, on site : Yahoo !, Google, Ebay, la NASA (*United state National Aeronautics and Space Administration*), le Pentagone…etc. Le piratage englobe quelques infractions qui sont :

- ✓ Le craquage d'un mot de passe ou de sites Internet protégés ;
- ✓ Exploitation d'une faille logicielle ou matérielle pour obtenir illégalement un mot de passe permettant d'entrer dans un système informatique ;
- ✓ Création de site Internet d'espionnage (qu'on appelle aussi « Spoofing ») qui amène l'utilisateur à révéler son mot de passe ;
- ✓ Installation de logiciel ou matériel d'enregistrement de frappe. Ce dernier enregistre toutes les frappes au clavier, c.-à-d. tous les mots de passe saisis sur l'ordinateur ou dispositif.

L'accès illicite aux systèmes informatiques est en nette hausse, et d'après le rapport de l'UIT, trois facteurs pourraient expliquer ce phénomène :

- La protection inadaptée et insuffisante des systèmes informatiques : Il y'a de nombreux ordinateurs qui ne disposent pas d'une protection contre les accès illégaux[4]. D'après les analyses de l'université du Maryland, un système informatique non protégé risque une attaque dans la minute qui suit sa connexion à Internet. On recense 12,824, 759 attaques en 30 jours (du mois d'avril 2015)[5].
- Le développement d'outils et logiciels d'automatisation des attaques : à l'aide de certains logiciels, un pirate peut attaquer des milliers de systèmes informatiques à partir d'un seul ordinateur[6]. Il peut également augmenter la portée de son attaque en ayant accès à d'autres ordinateurs via un botnet[7].
- Le rôle grandissant des ordinateurs privés dans les stratégies de piratage : les pirates concentrent leurs attaques sur les ordinateurs privés car c'est dans ces derniers que sont stockés les informations sensibles comme : le numéro de carte de

[4] Wilson,"Computer Attacks and Cyber Terrorism, Cybercrime & Security", IIV-3, P.5.
[5] Publié par HackerWatch, une communauté en ligne dédiée au partage d'informations de sécurité. Elle vise à identifier et à bloquer les menaces, notamment le trafic indésirable. Source : http://www.hackerwatch.org
[6] Ealy, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools and Prevention.
[7] Voir Wilson, "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress", 2007, P. 4.

crédit, coordonnées bancaires, etc. De plus, ils peuvent intégrer l'ordinateur privé dans leur botnet et l'utiliser pour commettre des infractions ultérieures[8].

**b) Espionnage de données :**

Lorsque le système est connecté à Internet, en vu de leur contenu en données sensibles, un pirate essayera de s'introduire et de saisir ces données. En effet, l'espionnage est une activité rentable, d'abord pour la possibilité d'accès à distance, ensuite pour la valeur des données confidentielles.

Pour accéder aux systèmes informatiques, les pirates utilisent diverses techniques[9] :

- ✓ L'utilisation de logiciels conçus pour rechercher les ports non protégés[10] ;
- ✓ L'utilisation de logiciels conçus pour contourner les mesures de protection ;
- ✓ L'ingénierie sociale[11].

Les pirates utilisent souvent des « Spyware » (logiciels espions) qu'ils installent dans les ordinateurs des victimes, ce qui leurs permettront de transmettre les données. Parmi les logiciels espions, « l'enregistreur de frappe »[12].

**c) Interception illégale :**

Elle représente l'interception des communications électroniques ou les transferts de données (qui pourraient être copiées ou modifiées), dans le but de récolter des informations. L'interception peut se faire de différentes manières, de l'accès physique aux lignes de réseau (écoute téléphonique et surveillance des transmissions radios). Les pirates visent tous types d'infrastructures de communications notamment : les lignes fixes, communications hertziennes[13], etc.), aussi les services Internet (messageries électroniques, les discussions en

[8] Idem.
[9] Sieber, Council of Europe Organised Crime Report 2004, P.88.
[10] Ealy, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", P.9. « **Un port »** : Correspondant à la couche de transport du modèle OSI, la notion de **port** logiciel permet, sur un ordinateur donné, de distinguer différents interlocuteurs. Ces interlocuteurs sont des programmes informatiques qui, selon les cas, écoutent ou émettent des informations sur ces ports. De façon plus simple, c'est des portes qui donnent accès au système d'exploitation (Microsoft Windows, Mac OS, GNU/Linux, Solaris…). Pour fonctionner, un programme (par exemple, un jeu à accélération 3D/2D, ou un logiciel de retouche photo) ouvre des portes pour entrer dans le système d'exploitation, mais lorsque l'on quitte le programme, la porte n'a plus besoin d'être ouverte, voir : http://fr.wikipedia.org/wiki/Port_%28logiciel%29.
[11] Cette technique désigne la manipulation des personnes dans le but d'accéder à des systèmes informatiques. Elle est généralement très efficace. Voir : Granger, « Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus », 2001.
[12] Il s'agit d'un programme conçu pour enregistrer toutes les frappes effectuées sur le clavier d'un ordinateur. Il est difficile à installer mais également à détecter.
[13] Un **faisceau hertzien** est un système de transmission de signaux, aujourd'hui principalement numériques, il exploite le support d'ondes radioélectriques par des fréquences porteuses allant de 1 GHz à 40 GHz. Ces

ligne, voix IP, etc.)[14], puis cherchent à identifier les points faibles du système et à l'aide d'équipement appropriés, ils peuvent enregistrer les données transférées entre des ordinateurs et le système auxquels ils sont connectés.

**d) Atteinte à l'intégrité des données :**

D'après l'article 323-3 du code pénal, l'Atteinte à l'intégrité des données est « le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement des données qu'il contient […] »[15].

Pour les entreprises et les administrations, les données informatiques représentent des données vitales et tout accès illégale peut causer des dommages (financier soient-ils ou non). Les pirates peuvent violer des données de différentes façons :

- ✓ Par effacement
- ✓ Par suppression
- ✓ Par altération
- ✓ Par limitation d'accès.

On peut prendre, comme exemple : un virus informatique qui opère « par effacement » de données. Alors qu'autre fois il se diffusait par voie de dispositif de stockage (disquettes et autres..), de nos jours, c'est via Internet qu'il se manifeste (par courriel, ou fichiers téléchargés par les utilisateurs…). Ces nouvelles méthodes ont permis d'accélérer la diffusion de virus et d'accroitre les infections. Ces dernières années, les virus sont capables d'installer des portes dérobées (back-doors), qui permettent aux pirates de prendre l'ordinateur à distance ou de chiffrer certains de ses fichiers (la victime alors aura à payer pour obtenir la clé du chiffrement)[16].

**e) Atteinte à l'intégrité du système :**

L'article du code pénal le définit comme « le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données […] »[17]. La destruction de fichiers, de

émissions sont notamment sensibles aux obstacles et masquages (relief, végétation, bâtiments…) aux précipitations, aux conditions de réfractivité de l'atmosphère, aux perturbations électromagnétiques et présentent une sensibilité assez forte aux phénomènes de réflexion (pour les signaux analogiques mais la modulation numérique peut, au moins en partie, compenser le taux d'erreur de transmission dû à ces nuisances). ;

[14] Rapport « comprendre la cybercriminalité », op-cit, 2012, P.20.

[15] Code pénal national français et européen de protection des données personnelles, voir le document suivant : ENDERLIN Clément, Un focus sur la cybercriminalité, 2011, P.42.

[16] Bates, « Trojan Hors : AIDS Information Introductory Diskette Version 2.0 in wilding skulason, Virus Bulletin 1990, page 3, Rapport de l'IUT, « comprendre la cybercriminalité : guide pour les PED », page 30.

[17] Code pénal français et européen.

programmes, le « flaming », sont des attaques qui pourrait provoquer des dysfonctionnements du système informatique (ralentissement ou paralysie). L'attaque la plus connue est celle qualifiée d'attaque par déni de service ou « Denial of service »[18]. Ce dernier se traduit par une saturation du site [19] . Les attaques informatiques s'appliquent également aux systèmes informatiques. Les entreprises intègrent de plus en plus Internet dans leurs processus de production et bénéficient ainsi d'une disponibilité sur 24 heures et d'une accessibilité dans le monde entier. Les pirates parviennent à déstabiliser le fonctionnement des systèmes informatiques et peuvent donc causer de lourdes pertes financières. Parmi les attaques à distance contre les systèmes informatiques :

- ✓ Les vers informatiques[20] ;
- ✓ Les attaques par refus de services (DoS)[21] . (voir le tableau ci-dessous)

[18] Le "Denial-of-service", ou déni de service, est une attaque très évoluée visant à rendre muette une machine en la submergeant de trafic inutile. Il peut y avoir plusieurs machines à l'origine de cette attaque (c'est alors une attaque distribuée, voir fiche DDoS) qui vise à anéantir des serveurs, des sous-réseaux, etc. D'autre part, elle reste très difficile à contrer ou à éviter. Parmi les attaques propres à créer un déni de service, nous pouvons rappeler entre autres :

- Les buffers overflows (mails, ping of Death...)
- L'attaque SYN
- L'attaque Teardrop
- L'attaque SMURF
- Les virus

Voir le lien : https://www.securiteinfo.com/attaques/hacking/dos.shtml

[19] ENDERLIN Clément, Un focus sur la cybercriminalité, 2011, P.42.

[20] Sieber, « Council of Europe Organised Crime Report 2004 », P.107. Les vers informatiques, comme les virus, sont un sous-ensemble des logiciels malveillants. Ils désignent des programmes informatiques auto reproducteurs, qui déstabilisent le réseau en lançant de multiples processus de transfert de données. Ils peuvent influer sur les systèmes informatiques de deux façons:

- en fonction de la charge utile du ver, l'infection peut perturber le bon fonctionnement de l'ordinateur et le ver peut utiliser les ressources système afin de s'auto-reproduire sur Internet;
- l'augmentation du trafic sur le réseau peut rendre certains services (notamment des sites Internet) indisponibles.

Egalement voir le rapport de l'UIT : « La cybercriminalité : guide pour les PED », 2009, P.34.

[21] On parle de déni de service quand une personne ou une organisation est privée d'un service utilisant des ressources qu'elle est en droit d'avoir en temps normal. On trouvera, par exemple, des dénis de service touchant le service de courrier électronique, d'accès à Internet, de ressources partagées (pages Web), ou tout autre service à caractère commercial comme Yahoo! ou EBay. Le déni de service est un type d'attaque qui coûte très cher puisqu'il interrompt le cours normal des transactions pour une entreprise; les sommes et les enjeux sont énormes et cela ne peut aller qu'en s'aggravant tant que des parades réellement efficaces n'auront pas été trouvées. Voir le lien : https://www.securiteinfo.com/attaques/hacking/dos.shtml

**Tableau n°5 : Attaques de types DOS**

| Rang | Pays | Nombre d'attaques | Part du total (en%) |
|---|---|---|---|
| 1 | Chine | 138 | 15,9 |
| 2 | Royaume-Unis | 33 | 3,8 |
| 3 | Espagne | 21 | 2,4 |
| 4 | Allemagne | 20 | 2,4 |
| 5 | Australie | 12 | 1,4 |
| | Autres | 642 | 74,1 |

**Source :** ATLAS, 2011

### I-2) Infractions informatiques :

C'est une catégorie qui regroupe des infractions commises à l'aide d'un système informatique. A la différence des autres catégories, elle ne concerne pas strictement la violation de principes juridiques. Elle comprend donc:

- ✓ La Fraude et fraude informatique
- ✓ La falsification informatique
- ✓ L'usurpation d'identité
- ✓ L'utilisation abusive de dispositifs

#### a) La Fraude et fraude informatique :

C'est l'un des délits les plus courants sur Internet, car elle peut être automatisée, aussi réalisée à l'aide de logiciels qui permettent de cacher l'identité du fraudeur.

D'après le rapport de l'UIT sur la cybercriminalité, les escroqueries les plus fréquentes du type « Fraude » sont :

##### a-1) Fraude de carte bancaire :

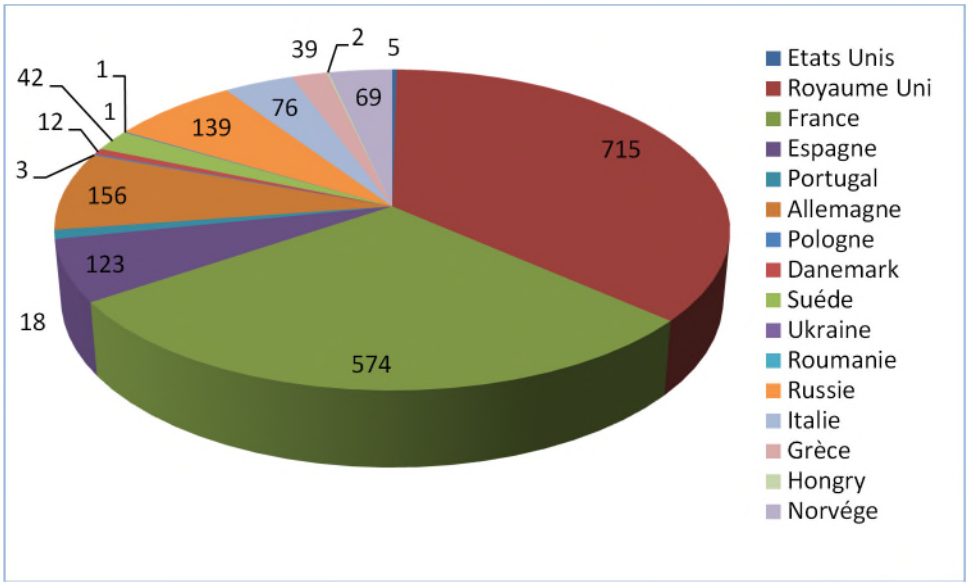
Une fraude de carte bancaire correspond à une usurpation d'identité bancaire[22]. Cette dernière est utilisée pour régler un achat ou faire une transaction à l'insu du titulaire de la carte bancaire et de sa banque. La fraude de carte bancaire se fait soit pas vol physique de la carte bancaire ou bien par la mémorisation des informations (lors d'un paiement), également provenir de votre ordinateur si celui-ci est victime de virus ou de logiciels espions (spyware), mais dans la majorité des cas, les fraudes à la carte bancaire sont dues à des paiements sur

[22] Voir le lien suivant : http://www.certissim.com/fraude.html

internet sur des sites peu ou pas sécurisés. Les fraudes à la carte bancaire peuvent induire des retraits de millions de dollars, 45 millions de dollars ont été détournés dans 24 pays, et les processeurs de cartes piratées sont localisés aux Etats- Unis et en Inde.

Les fraudes à la carte bancaire, dans le monde, a conduit à des détournements et pertes colossales pour certains pays, comme nous l'affiche le graphique ci-dessous pour l'année 2013 :

**Figure 04** : **Les pertes liées aux fraudes à la carte bancaire**




**Source :** Etablie à partir des données d'Euromonitor, FICO, Nilsen Report.

Les systèmes de sécurité des cartes bancaires, à puce, sont d'une importance secondaire contre les attaques de logiciels malveillants. Les numéros de cartes bancaires dérobés aux États-Unis sont utilisés par les pirates du monde entier. Les cartes bancaires européennes, bien qu'elles soient équipées de technologies de sécurité plus avancées (puces et codes PIN), sont facilement utilisées aux États-Unis où la protection est uniquement limitée à la bande magnétique des cartes[23].

**a-2) La fraude aux enchères en ligne :**

Les enchères en ligne sont des services de commerce électronique. Selon le rapport de l'UIT sur la cybercriminalité en 2006, prés de 20 milliards de dollars de biens ont été vendus sur **eBay**[24] (le plus grand site d'enchères au monde). Les plates-formes d'enchères ne peuvent pas distinguer entre les utilisateurs honnêtes et malfaiteurs, c'est ainsi que les fraudeurs profitent

[23] http://www.leparisien.fr/economie/votre-argent/fraude-a-la-carte-bancaire-une-perte-de-513-millions-en-france-22-04-2015-4714959.php#xtref=https%3A%2F%2Fwww.google.dz%2F

[24] Voir : http://WWW.eBay.com

de l'absence de contacte (le face à face) entre les acheteurs et vendeurs. On distingue deux escroqueries très courantes :

- Exiger aux acheteurs le paiement avant livraison d'un produit qui n'existe pas.
- Faire un achat et demander à être livré, dont l'intention de ne pas payer.

**a-3) La fraude aux avances sur commission[25] :**

Ce type de fraudes consiste à envoyer des mails qui sollicitent l'aide d'un destinataire pour transférer de grosses sommes d'argent. Dans le mail, on précise souvent que le destinataire recevra un pourcentage s'il accepte de faire transférer l'argent par son compte personnel, aussi d'envoyer une somme minime pour valider ses coordonnées bancaires (exemple des jeux de loterie USA) et ces dernières seront utilisées par le malfaiteur pour commettre des actes frauduleux.

**b) Falsification informatique[26] :**

Ce type d'infractions désigne la manipulation de documents numériques, elle comprend :

- La création d'un document qui semblerait provenir d'une institution digne de confiance ;
- La manipulation d'images électroniques ;
- L'altération de documents contenant du texte.

Autre fois, les falsifications informatiques étaient rares car la plupart des documents étaient sur papier, mais de nos jours, les documents sont numériques et il est devenu facile de les manipuler (de copier, modifier,…) sans perte de qualité.

**c) Usurpation d'identité[27]** :

Considéré comme une nouvelle criminalité instituée, par la loi d'orientation et de programmation, pour la performance de la sécurité intérieure (LOPPSI). Concrètement, l'usurpation d'identité consiste à utiliser sur Internet, sans votre accord, des informations permettant l'identification tel que :

- ✓ Nom et prénom
- ✓ Adresse électronique

[25] Pour plus d'informations, voir: Reich, "Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security", IF-1, page 1. Aussi: Oriola, "Advance fee fraud on the Internet: Nigeria's regulatory response, Computer Law & Security Report", Volume 21, Issue 3, P.237.

[26] Voir: ITU Global Cybersecurity Agenda/ High-Level Expert Group, Global Strategic Report, 2008, page 39.

[27] ENDERLIN Clément, Mémoire de recherche, Diplôme universitaire Sécurité intérieur/ extérieur dans l'Union Européenne, "Les moyens juridiques et institutionnels nationaux et européens de lutte contre la cybercriminalité dans le cyberespace », 2011, P.49.

- ✓ Numéro de téléphone
- ✓ Numéro de sécurité sociale ou numéro de passeport
- ✓ Mots de passe de comptes non financier
- ✓ Mot de passe de comptes financiers

Les infractions désignées par l'usurpation d'identité se déroulent en trois phases[28]:

**-Première phase :** le malfaiteur obtient des informations se rapportant à l'identité de la victime (par des logiciels malveillants ou attaques par fraudes informatiques).

**-Deuxième phase :** les informations recueillies seront vendues (les informations relatives aux cartes de crédit peuvent par exemple être vendues à 60 dollars)[29].

**-Troisième phase :** Les informations seront utilisées pour commettre de nouvelles infractions (exemple de falsification de documents d'identification ou de fraudes à la carte de crédit).

#### d) Utilisation abusive de dispositifs

Les infractions commises sur Internet, telles que la diffamation ou la fraude en ligne, nécessitent qu'un ordinateur ait un accès à un réseau et celles qui sont plus sophistiquées nécessitent l'utilisation de logiciels spécialisés. Ces opérations sont devenues accessibles grâce aux outils de deuxième génération, qui permettent d'automatiser de nombreux cyberdélit (par exemple, les programmes de transfert de fichiers vers des serveurs de partage ou depuis ces serveurs). Vu la facilité de pouvoir se procurer ces outils informatiques, le nombre de cyber délinquants augmente.

### I-3) Infractions combinées :

Les escroqueries relèvent de plusieurs types d'infractions que l'on site comme suit :

- ✓ Cyberterrorisme
- ✓ Guerre numérique ou « cyberguerre »
- ✓ Cyberblanchiment
- ✓ La monnaie virtuelle

[28] Mitchison/Wilikens/Breitenbach/Urry/Portesi – Identity Theft – A discussion paper, P.21.
[29] Voir: 2005 Identity Theft : Managing the Risk, Insight Consulting, P.2.

**a) Cyberterrorisme :**

Les attaques par réseau qui visent les infrastructures telles que les transports et les systèmes d'approvisionnement en énergie mais aussi l'utilisation des technologies de l'information dans les conflits armés (cyberguerre) ont démontré que la sécurité n'est pas au point.

C'est à la suite des attentats du 11 septembre qu'ont débuté les débats autour de l'utilisation des TIC par les terroristes, Internet comme moyen de préparation des attaques. Les organisations ont, alors, mis à jour les différentes façons dont les organisations terroristes utilisent les TIC et Internet[30] :

- Pour faire de la propagande : En 2004, l'*Institute of Peace* (Institut pour la paix) des Etats Unis a indiqué que quasiment toutes les organisations terroristes possèdent un site Internet, notamment le *Hamas*[31], le *Hezbollah*[32], le *PKK*[33] et *Al Qaida*[34]. Les terroristes ont utilisent des sites communautaires de partage de vidéos (Youtube, par exemple) pour diffuser des messages et faire de la propagande[35].

- Collecter des informations : Il y 'a, par exemple, des programmes d'apprentissage en ligne expliquant comment fabriquer une bombe et d'autres programmes, montrant dans des camps d'entrainement virtuels , comment manier des armes. En 2003, le Département de la Défense Américaine à été informé qu'un manuel de formation lié à *Al Qaida* indique qu'il était possible de trouver des informations sur des cibles

[30] Voir: Sieber/Brunst, "Cyberterrorism, The use of the Internet for terrorist purposes", Council of Europe Publication, 2007; Gercke, Cyberterrorism, "How Terrorists Use the Internet, Computer und Recht", 2007, P.62.

[31] Hamas, acronyme partiel de « Harakat al Muqawama al-Islamiya »(en arabe), « Mouvement de résistance islamique », est un mouvement islamiste constitué d'une branche politique et d'une branche armée, principalement actif à Gaza. Créé en 1987 par Sheikh Ahmed Yassin, Abdel Aziz al-Rantissi et Mohammed Taha, il prône la destruction de l'État d'Israël et l'instauration d'un État islamique palestinien sur tout le territoire de l'ancienne Palestine mandataire. Voir : http://fr.wikipedia.org/wiki/Hamas.

[32] Le Hezbollah « parti de Dieu », est l'une des organisations terroristes les plus actives au monde. Basé au Liban du sud, et fondé en juin1982, il a su construire un réseau mondial de terreur. La liste de ses activités terroristes compte attentats-suicides, détournements d'avions, assassinats, contrebande d'armes et tirs de roquettes sur les populations civiles. Depuis sa création, des centaines d'innocents ont été tués et des milliers ont été blessés à cause du Hezbollah. Les États-Unis, l'Union Européenne, l'Angleterre et le Canada ont déjà **désigné le Hezbollah comme une organisation terroriste**. Voir : http://tsahal.fr/glossaire/hezbollah/

[33]C'est le **Parti des travailleurs du Kurdistan** ; il a été créé en 1978 par Abdullah Öcalan. Ce dernier, d'obédience marxiste, a lancé une guérilla militaire contre la Turquie en 1984 pour exiger la reconnaissance de la minorité kurde. Considéré comme terroriste par l'UE, il mène actuellement des pourparlers de paix avec Ankara (qui ne reconnait pas l'identité Kurd). Pour plus d'informations, lire : http://lci.tf1.fr/monde/moyen-orient/qui-est-le-pkk-bras-arme-des-kurdes-de-turquie-7764114.html.
Voir le lien suivant : http://fr.wikipedia.org/wiki/Parti_des_travailleurs_du_Kurdistan

[34] Weimann, rapport USIP, "How Terrorists use the Internet", 2004, page 3. Voir également: Crilley, "Information warfare: New Battlefields – Terrorists, propaganda and the Internet", Aslib Proceedings, Vol. 53, No. 7 (2001), P.253.

[35]United States Homeland Security Advisory Council, Report of the Future of Terrorism, 2007, P.4.

potentielles en utilisant des sources publiques. En 2006, le New York Times a signalé que des informations concernant la construction d'armes nucléaires étaient disponibles sur un site Internet du gouvernement, et que ces dites informations prouveraient que l'Irak avait l'intention de développer des armes nucléaires.

- Préparer des attaques dans le monde réel : par voie des technologies de l'information, les terroristes préparent leurs attaques soit par mail ou par l'utilisation de forums, etc. Comme exemple : les terroristes utiliseraient les jeux en ligne pour préparer des attaques, ils permettraient de simuler le monde réel à l'aide de personnages (avatars) agissant dans un monde virtuel et servir à simuler les attaques[36].

- Publier du matériel de formation : Internet est le moyen utilisé pour la diffusion de matériel de formation. Par exemple en 2008, les services secrets occidentaux ont découvert un serveur Internet qui permet d'échanger du matériel de formation et de communiquer[37].

- Communiquer : les organisations terroristes n'utilisent pas les TIC uniquement pour la création de sites Internet et faire des recherches dans les bases de données, mais ils ont recours à des technologies de chiffrement et à des moyens de communication anonymes pour coordonner leurs attaques et échanger les instructions, par courriel, concernant les cibles et le nombre d'attaquant[38].

- Financer le terrorisme : Internet peut être utilisé pour financer le terrorisme, cela s'effectue en sollicitant des donations en ligne par paiement électronique ou indiquer les modalités de donation sur leur site, exemple du site « Hizb al-Tahrir » fournit les coordonnées d'un compte bancaire à l'usage des donateurs potentiels. Ou alors, des donations, avec paiement en ligne, par cartes de crédit. Financement par de fausses boutiques en ligne, d'abord cette dernière présente l'avantage d'être accessible par tout le monde, en plus il parait difficile de prouver que les transactions financières effectuées

[36] Rapport de l'UIT sur « comprendre la cybercriminalité : guide pour les PED », 2009, P.65 ; Aussi voir: Chen/Thoms, Cyber Extremism in Web 2.0 – An Exploratory Study of International Jihadist Groups, Intelligence and Security Informatics, 2008, P. 98.
[37] Musharbash, Bin Ladens Intranet, Der Spiegel, Vol. 39, 2008, P.127.
[38] Voir: les articles de Weimann, "How Modern Terrorism Uses the Internet", The Journal of International Security Affairs, spring 2005, No. 8. Aussi: Thomas, Al Qaeda and the Internet: The danger of "cyberplanning», 2003.

sur les sites correspondent à des donations (ce qui peut être une contrainte pour les enquêteurs surtout si les systèmes de paiement sont anonymes ou que la boutique est gérée dans un autre pays).

- Lancer les attaques contre « les infrastructures essentielles »[39] : Les infrastructures sont plus vulnérables aux attaques, surtout s'elles sont interconnectées par des réseaux informatiques et de communication. Une attaque perpétrée sur un réseau crée des perturbations. Une interruption de service, par exemple, même de courte durée peut entrainer de lourdes pertes financières (les services civils : comme les entreprises de commerce électronique ; les services de l'armée ; etc.). ; Exemple de l'ouragan Katrina aux Etats Unis, qui a montré la dépendance de la société à l'égard de ces services (interruption des services civils). Aussi, en 2004, le ver informatique Sasser qui a infecté des millions d'ordinateurs dans le monde, surtout ceux des compagnies aériennes, et qui a entrainé l'annulation de plusieurs vols.

Etant donné la vulnérabilité des technologies de l'information et la dépendance grandissante[40] à leur égard, il sera alors indispensable d'intégrer cette menace dans les stratégies de prévention et de la répression du « Cyberterrorisme ».

**b) Guerre numérique ou "cyberguerre" :**

Il désigne l'utilisation des TIC pour mener une guerre dans le cyberespace. Il partage certaines caractéristiques avec le Cyberterrorisme. Les attaques par réseau sont moins coûteuses que les opérations militaires traditionnelles[41] et à la portée de tous les Etats (petits et grands). Actuellement, des études portent sur les attaques qui visent les infrastructures essentielles et sur le contrôle de l'information dans les conflits. Les infrastructures de l'information constituent une cible clé pendant les conflits armés. Exemple de cyberguerre, on évoque les attaques des systèmes informatiques en Estonie[42] et aux Etat- Unis[43]. On ne peut

[39] Les infrastructures essentielles représentent l'élément vital de la durabilité et de la stabilité d'un Etat, et la mise hors d'usage où la destruction aurait pour effet de fragiliser la défense ou la sécurité économique d'un Etat. C'est, donc, évident qu'elle soit une cible potentielle des attaques terroristes. Ces infrastructures comprennent le transport, les réserves de gaz et de pétrole, les systèmes de télécommunication, le système d'alimentation, le système bancaire et financier, le système d'alimentation en eau et les services d'urgence. Voir le rapport de l'UIT sur la cybercriminalité 2009, P.67.

[40] Sofaer, Goodman, "Cybercrime and Security – The Transnational Dimension», dans: Sofaer, Goodman, "The Transnational Dimension of Cyber Crime and Terrorism», Article de 2001.

[41] Molander, Riddile, Wilson, Strategic Information Warfare, 1996, P.15.

[42] Traynor, "Russia accused of unleashing cyberwar to disable Estonia", The Guardian, 17.05.2007.

[43] Thornburgh, "Inside the Chinese Hack Attack", dans le journal "Time", du 25/08/2005.

classer comme « cyberguerre », les attaques commises avec des moyens physiques (les armes, les explosifs,…) contre des infrastructures.

**c) Cyberblanchiment :**

Certes, les techniques traditionnelles de blanchiment présentent un certain intérêt pour les sommes importantes. Néanmoins, Internet apporte plusieurs avantages, si on prend les services financiers en ligne par exemple, ils offrent la possibilité d'effectuer des transactions financières rapidement et multiples dans le monde.

Les transactions électroniques ont permis aux cybercriminels de s'affranchir des transactions en monnaie physique et du transport d'argent liquide. Comme l'a souligné le rapport de l'UIT, le blanchiment de capitaux s'effectue généralement en trois phases[44] :

1) Le placement ;
2) L'empilage ;
3) L'intégration.

Internet présente beaucoup d'intérêt dans la phase d'empilage (appelé aussi masquage), par le biais de cyber-casinos[45] ou par l'utilisation de monnaie virtuelle où les transactions sont difficiles à suivre (pour un enquêteur).

**d) La monnaie virtuelle :**

D'après le rapport du ministère des finances et des comptes publics (de juillet 2014), la monnaie virtuelle est une monnaie non officielle émise sous forme numérique et elle n'a pas de matérialisation physique (pas de pièce ni de billet). C'est un instrument de paiement qui permet d'effectuer des transactions en ligne. Il en existe 1à, principales monnaie représentant 10 milliards d'euros. Parmi elles on cite[46] :

- AMAZON COIN : créée par le mastodonte américain de l'e-commerce, utilisable sur les applications, les jeux, etc;

-DOGECOIN : créée par Billy MARKER, un ancien d'IBM, en 2013, elle a un chien comme mascotte ;

[44] Rapport de l'UIT, op-cit, P.69.

[45] C'est l'utilisation de casino en ligne, contrairement à un casino réel, il ne nécessite pas de gros investissements financiers. La réglementation n'est pas aussi stricte et la difficulté s'explique par :

- La difficulté de contrôle d'identité des clients (vu qu'il n'y a pas de contacte face à face) ;
- Le fait que les prestataires sont situés dans différents pays ;
- L'absence de code législatif ou pénal (explication faite par le rapport de l'UIT 2009, comprendre la cybercriminalité).

[46] Voir le lien : http://frenchweb.fr/5-monnaies-virtuelles-alternatives-au-bitcoin/153443

- FASTCOIN : l'équipe de développement est composée de 10 personnes, se trouvant aux quatre coins du monde et elle a un guépard comme effigie ;

- ZEROCOIN et DARKCOIN[47] : sont des crypto-monnaies qui intègrent du chiffrement permettant d'éviter toute traçabilité des transactions. Créées début 2014, elles apparaissent, de par leur anonymat et leur non-traçabilité, comme un moyen de servir d'intermédiaire à l'économie souterraine ;

- BITCOIN : constitue la monnaie virtuelle la plus connue dans le monde. Créée en 2009 par Satoshi Nakamot (pseudo qui désigne le groupe programmateur), elle permet d'échanger des biens et services entre les utilisations sans avoir recours à la monnaie légale[48].

Le paiement en liquide permettait aux acheteurs de certains types de produits de cacher leur identité, s'ajoute à cela le problème de la carte de crédit, ces derniers ont été des moteurs de développement de système de paiement virtuel et donc à mettre en place des monnaies virtuelles. Exemple des monnaies virtuelles dites « or » : sont un système de paiement qui repose sur des comptes dont la valeur est gagée sur des réserves d'or. Les comptes appelés « e-gold » sont ouverts en ligne dans plusieurs pays, et certains des prestataires proposent même des services de retrait en liquide et de virement *peer-to-peer* (de personne à personne)[49].

### II- Les techniques de la cybercriminalité :

Les pirates ne sont jamais à court d'idées et avec Internet, leur imagination n'a plus de limites et chaque année on découvre de nouvelles techniques[50] d'attaques qui dérivent des méthodes classiques. Pour distinguer ces techniques, nous les avons classées selon trois (03) catégories : II-1) les infections informatiques, II-2) les attaques cybernétiques, II-3) les arnaques.

[47] Groupe de travail sur les « monnaies virtuelles », du Ministère des finances et des comptes publics, juin 2014, P. 6.

[48]Revue de « Banque de France », Focus- les dangers liés au développement des monnaies virtuelles : l'exemple du « bitcoin », n° 10-5 décembre 2013. Disponible via le lien suivant:https://www.banque-france.fr/uploads/tx_bdfgrandesdates/Focus-10-stabilite-financiere.pdf

[49] Voir le document: Woda, "Money Laundering Techniques With Electronic Payment Systems», Information & Security, Vol. 18, 2006, P.40.

[50]Les nouvelles techniques d'attaques sont plus tournées vers le secteur industriel, alors qu'avant c'était les administrations qui étaient les plus visées. Pour connaitre l'actualité des techniques d'attaques, voir le lien suivant :http://www.latribune.fr/technos-medias/informatique/20130416trib000759796/cyber-criminalite-les-nouvelles-techniques-d-attaques-toujours-plus-perfectionnees-et-redoutables.html.

### II-1) Les infections informatiques :

Ce sont des programmes ou des sous-programmes malveillants qui sont destinés à saturer, perturber, modifier ou détruire tout ou une partie des éléments indispensables au fonctionnement de l'ordinateur (voir l'annexe n°5). Cela se fait à l'insu de l'utilisateur en vu de porter atteinte à la confidentialité et l'intégrité de ses données ou de son système[51]. Elles regroupent deux familles, a) les infections simples, b) les infections auto- reproductrices :

#### a) Les infections simples :

C'est des programmes simples qui ont une fonctionnalité malveillante qui se déclenche à un moment donné. Il s'installe dans le système et s'active généralement par l'exécution d'un fichier par l'utilisateur. Une fois sa mission accomplie, il se désactive du système et ne réside plus en mémoire. Parmi les infections simples[52] :

**a-1) Les bombes logiques** :

Programme avec une fonction cachée qui s'exécute après un délai ou une réponse à une commande,…etc. Elle est considérée comme la seule infection qui a pour but unique de nuire.

**a-2) Les chevaux de Troie** :

C'est également un programme avec une fonctionnalité cachée dont la mise en œuvre est immédiate et systématique. Il se dissimule dans une application a priori inoffensive et souvent attractive qui se décompose pour exécuter des tâches dites « malignes » et notamment l'insertion d'une bombe logique.

**a-3) Les accès dissimulés** :

Appelés également « backdoors », c'est des programmes qui permettent à un ordinateur externe de prendre le contrôle d'une application. L'accès dissimulé est le fait de laisser une porte ouverte dans un logiciel pour pouvoir l'utiliser sans passer par une quelconque phase d'authentification, il est ainsi possible d'accéder à des données personnelles, profil d'utilisateur, …etc.

**a-4) Les logiciels espions** :

Appelés aussi « spyware », ce sont des programmes ou sous- programmes qui fonctionnent de manière autonome (les cookies, applet Java, contrôles ActiveX), ils sont conçus dans le but de collecter des informations et de les envoyer à leurs concepteurs. Il s'agit, donc, de codes malicieux inclus dans un système qui lui provoquerait un risque de saturation.

---

[51] E. FILIOL, « Les virus informatique : théorie, pratique et applications », Ed. Springer, 2004, P.79.
[52] Frédéric DUFLOT, « les infections Informatiques Bénéfiques », 2004, page 16-17. http://www.juriscom.net

**b) Les infections auto- reproductrices** :

Un programme auto- reproducteur a une structure semblable à celle d'un programme simple, sa finalité est de perturber ou de détruire le système. Il est résidant en mémoire et à son exécution le programme cherche à se reproduire, il se duplique afin de se propager. Dans les infections auto- reproductrices, on distingue ; b-1) le virus, b-2) le ver.

**b-1) le virus** :

C'est un programme capable d'infecter d'autres programmes en les modifiant pour inclure une copie de lui-même. Le virus ne peut pas fonctionner d'une manière indépendante, l'exécution du programme hôte est nécessaire à son activation. Il se multiplie et entraine ainsi corruption, perturbation et/ou destruction. Il existe quatre (04) catégories principale de virus[53] :

- Les virus programmes, ils cherchent à infecter les fichiers exécutables ;
- Les virus système, ils infectent les zones systèmes des disques durs (secteur de partition) ou celui de démarrage ;
- Les virus multipartites, qui infectent les zones systèmes des disques durs puis une fois résidant dans la mémoire vive, infectent les fichiers exécutables sur les unités logiques. (exemples : Tequila, One-Half)
- Les virus interprétés regroupent les virus de macro sur les documents et les virus de Script qui utilisent un langage de programmation particulier qui est destiné à contrôler l'environnement d'un logiciel.

**b-2) Le ver** :

D'après Peter DENNING (1990), c'est un programme qui est capable de fonctionner de manière indépendante. Il se propage de machine en machine au travers des connexions réseau. Un ver ne modifie pas un programme, il ne fait que transporter des parties de code qui, par la suite, pourront servir à activer un virus. Donc, les vers ne sont que des sous-ensembles dans la catégorie virus[54].

[53] Pour plus de détails concernant cette catégorie d'infections, voir : CLUSIF, « les virus informatiques », décembre 2005, PP. 10- 15. Disponible sur : http://www.clusif.asso.fr

[54] CLUSIF, Op-cit, P.10.

**II-2) Les attaques cybernétiques :**

C'est l'exploitation d'une faille de système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système. On recense quatre attaques cybernétiques : les attaques cryptographiques, de déni de service, de technique et de web[55] :

**a) Les attaques cryptographiques[56] :**

Elles peuvent être des attaques de mot de passe, main in the middle[57]ou des attaques par déni de service.

**b) les attaques techniques :**

Elles se font par usurpation d'adresse IP, par des spam, l'analyse réseau ou écoute réseau (interception illégale), etc.

**c) les attaques web :**

Elles sont fréquentes et sous formes d'attaques par falsification de données, par injection de code malicieux ou par infection de commande (SQL[58]), etc.

**II-3) Les arnaques :**

Les cybercriminels ont mis au point des techniques pour tromper les internautes et les pousser à divulguer des données confidentielles les concernant. Parmi les arnaques les plus répandues : a)L'ingénierie sociale, b) le SCAM et le SPAM, c) le Phishing ou Hameçonnage, d) la loterie internationale.

**a) L'ingénierie sociale :**

Elle est, aussi, appelée « élicitation[59] », en anglais « social engineering ». C'est une technique de manipulation psychologique, c'est l'art de convaincre ou l'art d'arnaquer et l'art d'obtenir

[55] Les menaces sont en hausse et prennent plusieurs formes, voir le site suivant pour les menaces les plus fréquentes en 2015 : http://blogues.radio-canada.ca/triplex/2014/12/22/2015-montee-des-attaques-cybernetiques/

[56] Le mot cryptographie est un terme générique désignant l'ensemble des techniques permettant de chiffrer des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique.

[57] Voir : http://openclassrooms.com/courses/la-cryptographie-asymetrique-rsa/rsa-qu-est-ce-donc

[58] **SQL** : Structured Query Language, est un langage informatique normalisé servant à exploiter des bases de données relationnelles, il permet de modifier, ajouter ou de supprimer des données dans les bases de données des entreprises ou des banques.

[59] « élicitation » du verbe « éliciter » : qui est l'art d'extirper frauduleusement de l'information à l'insu de son interlocuteur.

d'un utilisateur ses codes d'identification, mots de passe et références bancaires. C'est l'outil populaire auprès des cybercriminels, elle repose sur les attaques de type Phishing, spam, …etc.).

**b) Le SCAM ou SPAM :**

- **Le SCAM :** les Scams sont des cyber-arnaques ou cyber-escroqueries par email, appelés communément le « Scam nigérien » ou « Nigeria419 »[60]. Ce dernier est le plus courant, c'est des mails dont lesquels un dignitaire d'un pays africain (généralement) vous sollicite à servir d'intermédiaire pour une transaction financière tout en vous promettant un bon pourcentage de la somme.
- **Le SPAM :** le spam ou « pollupostage » désigne les communications électroniques massives, notamment, d'email non sollicitées par les destinataires à des fins publicitaires ou malhonnête. La plupart des publicités portent sur les médicaments, le crédit financier, les casinos en ligne et les logiciels craqués[61].

**c) Le PHISHING ou HAMEÇONNAGE**:

Mis au point par les cyberdélinquants pour obtenir des informations sur les utilisateurs, le "phishing", ou hameçonnage, consiste pour le fraudeur à se faire passer pour un organisme qui vous est familier (banque, administration fiscale, caisse de sécurité sociale,…), en utilisant son logo et son nom. L'utilisateur reçoit un e-mail dans lequel il lui est demandé de "mettre à jour" ou de "confirmer suite à un incident technique" ses données, notamment bancaires[62]. Les attaques par « hameçonnage » ont pour objectif d'amener les victimes à révéler des données personnelles ou confidentielles. On distingue plusieurs attaques de « hameçonnage », qui comprend trois phases :

1. Les cybercriminels identifient des sociétés légitimes qui proposent à leurs clients des services en ligne et communiquent avec eux par voie électronique ou par mail (exemple : les banques) ;
2. Les cybercriminels créent des sites Internet (appelés aussi des sites d'espionnage) qui ressembleraient aux sites de la société, ils demandent ensuite aux victimes de

[60] « Nigéria » : pour le pays d'origine de cette arnaque, « 419 » : pour le numéro d'article du code nigérien qu'ils violent. Voir : <http://www.altospam.com/glossaire/scam.php >

[61] Plus de détails, voir le lien : < http://www.internetsanscrainte.fr/s-informer/quest-ce-quun-spam >

[62] Voir le lien : <http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/spam-phishing-arnaques-signaler-pour-agir/>

s'identifier, ainsi collectent les informations les concernant (numéros de compte, mots de passe,…) ;

3. Les cyberdélinquants, après avoir envoyé des mails aux internautes qui ressemblerait aux mails mis par la société dont ils sont clients (la banque) et où il leurs est demandé de se connecter pour des motifs de sécurité ou de contrôle et que s'ils refusent, des mesures telles que la fermeture du compte seront appliquées. Le mail contient, alors, un lien sur lequel la victime va cliquer et dès que les données personnelles sont saisies, les cybercriminels se connectent au compte de la victime et effectuent des opérations de virement, demande de passeport, ouverture de compte, etc. Ces attaques sont efficaces et en hausse, vu qu'on recense 55000 sites de hameçonnage (signalés par l'APWG[63] en avril 2007[64]), et prés de 115 565 attaques[65] de phishing dans le monde d'après le rapport de l'APWG d'avril 2014.

Cette technique ne serre pas qu'à obtenir des mots de passe et effectuer des opérations bancaires en ligne, mais également l'obtention d'accès au système informatique et aux numéros de sécurité sociale (élément important aux USA qui sert à commettre des infractions tel le vol d'identité). Le tableau ci-dessous nous montre la répartition des attaques de hameçonnage par type d'industrie dans le monde statistiques de novembre 2013 :

**Tableau n°6 : répartition des attaques de d'hameçonnage (phishing) dans le monde par type d'industrie**

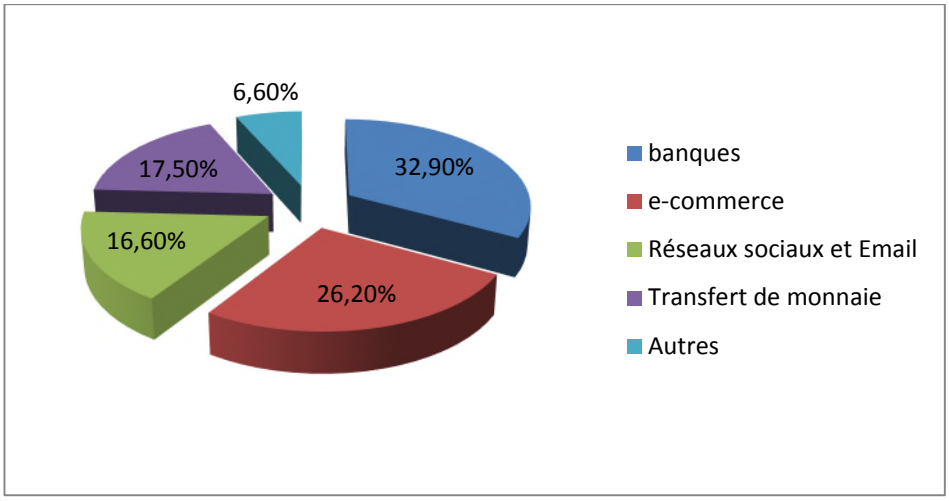
| Type d'industries | banques | e-commerce | Réseaux sociaux et Email | Transfert de monnaie | Autres |
|---|---|---|---|---|---|
| **2013** | 32,9% | 26,2% | 16,6% | 17,5% | 6,6% |

**Source:** Etabli à partir des données du rapport de l'APWG, 10 April 2014 : http://www.apwg.org

La représentation graphique du tableau, ci-dessus, donnera alors :

[63] Anti-Phishing Working Group. For more details, see: http://www.antiphishing.org.
[64] "Phishing Activity Trends», Report for the Month of April 2007.
[65] Voir Le rapport, "Global Phishing Survey 2H2013 : Trends and Domain name Use, clés statistiques, Avril 2014, P.3.

**Figure 05 : Attaques d'hameçonnage (phishing) par type d'industrie**




Source : Elaborer sur la base, rapport, "Global Phishing Survey 2H2013 : Trends and Domain name Use, clés statistiques, Avril 2014.

Les attaques de hameçonnage sont plus orientées vers le secteur bancaire et le e-commerce, respectivement 32,9% et 26,2%.

Le tableau suivant nous donne quelques chiffres sur le nombre d'attaques d'hameçonnage qu'ont rencontré les trois pays suivant : Algérie, Maroc et Tunisie, par nombre de sites et durée moyenne des attaques :

**Tableau n°7: Statistiques des attaques de phishing et disponibilité par le TLD.**

| TLD | Location | Attaques de phishing | Noms de Domaines utilisés pour le phishing | Domains dans le registre (nov 2013) | domaines de phishing par 10.000 domaines | d'attaques par 10.000 domaine | Disponibilité moyenne hh:mm | Disponibilité médiane hh:mm |
|---|---|---|---|---|---|---|---|---|
| **Dz** | **Algérie** | 3 | 2 | 5,256 | 3,8 | 5,7 | 10:58 | 12:15 |
| **Ma** | **Maroc** | 44 | 33 | 43,325 | 7,6 | 10,2 | 33 :51 | 11 :08 |
| **tn** | **Tunisie** | 34 | 24 | 19,500 | 12,3 | 17,4 | 96 :57 | 7 :40 |

**Source:** Global phishing Survey: Trends and Domain Name Use, April 2014. http://www.apwg.org

**d) La loterie internationale :**

C'est une arnaque qui prend pour cible un certain nombre d'internautes. Les cyber-arnaqueurs utilisent des messages électroniques promettant des gains de « loterie ». Ces messages

frauduleux ont pour but d'initier un dialogue afin d'extorquer de l'argent, des informations personnelles ou confidentielles, ou alors d'inciter à cliquer sur un lien qui mène à un site malveillant. La forme la plus répandue de ce type d'arnaques : une lettre (voir l'annexe n°1) dans laquelle ont dit que vous avez gagné une forte somme à une loterie organisée (qui peut prendre les noms les plus connus Microsoft, Google, Coca Cola,…etc.). La somme à gagner augmente d'année en année, elle est passée de 100.000 euro en 2008 à 250.000 euro en 2013. Pour toucher cette somme, vous devez tout simplement donner vos références bancaires pour que le virement soit effectué (voir l'annexe n°04). Généralement ces cyber-arnaqueurs ne sont qu'une seule personne qui utilise des noms, des boites email et titres usurpés et différents et c'est de là que vient la difficulté de retracer cet escroc. Lorsque le cyber criminel aura récolté toutes les informations personnelles et bancaires, il volera votre identité et videra vos comptes bancaires en commettant des transactions en votre nom. On recense quelques noms utilisés pour les sociétés de loterie[66] :

- Bright Lotto
- Techie Lottery International
- Lucky Day LotteryInternational
- Lucky Strike Lottery UK
- National Lotto Competition
- Swiss Union International
- LoteriaLa primitiva
- Mega Lottery International
- Quafrilafrik
- ExtanisAfrica
- Loteria del rosario
- Big Lottery Fund
- Zeemaland Lotto International
- Euro-Afro-American-Sweepstake Lottery

**Conclusion**

La diversité et l'imbrication des infractions et des techniques fait qu'il est difficile de les classer, et ce malgré certaines propositions faites par l'IUT ou la convention du Conseil

[66] Cette sélection de noms des sociétés de loterie changent régulièrement, on les retrouves sur le lien suivant : <http://www.arobase.org/arnaques/loteries.htm > mis à jour le 14 SEP 2014.

européen. Néanmoins, on remarque que derrière la majorité des attaques, l'origine de la faille est humaine. La victime se laisse facilement berner, et sans le savoir, elle se fait dérober : mots de passe, accès et contacts qui permettent, ensuite, une attaque plus en profondeur dans le système. Alors, face à cette nouvelle forme de crimes, beaucoup d'Etats ont adopté un arsenal de lutte et de défense ainsi que des stratégies de cybersécurité afin de sensibiliser, prévenir et incriminer.

## Section 2 : Les réponses de l'Europe et des Etats-Unis face à cette nouvelle forme de crimes

La cybercriminalité intéresse plusieurs acteurs, tant publics (comme les parlementaires, les administrations,…) que privés ce qui démontre le caractère transversal de ce phénomène mais, également, les limites des organisations qui tentent de cerner les normes de lutte contre la cybercriminalité qui ne cesse d'évoluer, « un droit en marche qui se cherche encore »[67]. L'actualité de la question d'une « cyberdéfense » et d'une « cybersécurité », dévoile la nécessité de chaque Etat de disposer d'une stratégie globale et d'une grille juridique cohérente. Les spécialistes rencontrent de réelles difficultés à cerner le phénomène et appréhender le contenu technique et apporter des réponses pertinentes, c'est pour cela qu'ils ont décidé d'élargir leur étude en s'attachant à encadrer, aussi, les attentes des usagers, des consommateurs, des victimes individuelle, du monde de l'entreprise, des magistrats, des policiers et des gendarmes non spécialisés pour mieux saisir les difficultés qu'ils rencontreraient et ce tout en œuvrant à la protection des libertés fondamentales[68].

### I- La réponse de l'Europe :

En Europe, la lutte contre la cybercriminalité repose sur une coopération internationale qui rassemble entre le prolongement de l'activité opérationnelle des services d'enquête et des autorités judiciaires.

#### a) Les outils européens de lutte contre la cybercriminalité[69] : *entre réalité et espérance*

Le Conseil de l'Europe et l'Union européenne ont œuvré à la création d'outils normatifs communs pour le traitement des attaques et la protection des systèmes, qui sont :

[67] Rapport sur la cybercriminalité « protéger les internautes », 2014, P.2.
[68] Rapport de l'UIT, op-cit, 2009, P.99.
[69] Rapport sur la cybercriminalité, op-cit, 2014, P.55.

- **Les attaques contre les systèmes d'information et les systèmes de traitement automatisé de données (STAD)[70]** : L'Union a adopté une directive 2013/40/UE du 12 aout 2013, qui devait être transposée par chaque Etat membre avant le 4 septembre 2015, elle impose donc :

  - D'incriminer l'accès illégal à des systèmes d'information, l'atteinte illégale à l'intégrité d'un système d'information et à l'intégrité de données ainsi que l'interception illégale de transmission non publique de données informatiques, avec des minima de peines.
  - De répondre à de nouveaux modes d'atteinte à la sécurité des réseaux d'information, telle que l'utilisation de « réseaux-zombies ». Autre cette directive, la convention de Budapest prévoit la mise en place de contactes nationaux opérationnels 24h/24 et 7j/7, et l'instauration de procédures qui permettraient de répondre à une demande d'assistance émanant d'un autre Etat membre (dans les 8 h après réception de la demande).

- **La protection des réseaux et la directive dite « cybersécurité » :** Pour assurer un niveau de sécurité des réseaux, une coopération en matière de gestion de crise cyber et de réponse aux incidents et de sécurité de l'information dans l'Union Européenne, trois moyens sont proposés :

  - Imposer dans chaque Etat membre, l'instauration d'une autorité nationale sur la sécurité des réseaux d'information et d'une stratégie nationale de cybersécurité d'un C.E.R.T. (Computer Emergency Response Team);
  - Créer un « réseau européen des autorités nationales de cybersécurité», adopter un plan européen de coopération durant les crises « cyber » et constitution d'un réseau informatique d'échange d'informations sensibles ;
  - Instaurer le principe de la notification obligatoire d'incidents informatiques significatifs par les opérateurs économiques, introduire la possibilité pour l'autorité nationale de conduire des audits réguliers et d'exiger la mise à disposition, par les opérateurs, des informations nécessaires et introduire un principe de sanction en cas de non respect des dispositions.

[70] L'atteinte au STAD est la première infraction définie par la convention de Budapest, en 2001, et qui l'appréhende comme l'accès illégal, l'interception illégale de l'atteinte à l'intégrité des données ou d'un système, de l'abus de dispositif ou de la falsification de données.

- **La protection de l'intelligence économique et le secret des affaires :** La Commission Européenne devait présenter un projet de directive qui vise à protéger les « secrets d'affaires » (technologies ou savoir faire particuliers) au parlement en février 2014. Ce texte suivant dit donc : « L'accès non autorisé à tout document (…) ou fichier électronique ou copie non autorisé de ces éléments ». Aussi, le projet prévoit des dommages et intérêts pour les entreprises victimes d'un vol ou d'une appropriation illicite d'informations confidentielles.

- **La vente de contrefaçons et le piratage sur Internet :** La convention de Budapest renvoie aux principaux accords internationaux existant : la convention universelle sur le droit d'auteur ; Accord sur les aspects commerciaux des droits de propriété intellectuelle ;… Suite à une consultation réalisée fin 2012, la Commission a décidé de ne pas proposer de révision de la directive 2004/49/CE relative au commerce électronique, pour privilégier la question de la responsabilité des intermédiaires d'Internet.

- **Les discriminations :** le protocole additionnel à la convention de Budapest, adopté le 07/10/2002, demande aux Etats de lutter contre la diffusion de matériels racistes et xénophobes par les systèmes informatiques et préconise ainsi une harmonisation du droit pénal et l'amélioration de la coopération internationale. La décision cadre 2008/913/JAI du 28 novembre 2008, sur la lutte contre certaine formes et manifestations de racisme et xénophobie, demande aux Etats membres d'accuser tout fait, propos et comportement qui vise à « l'incitation publique à la violence ou à la race visant un groupe de personnes ou de membre d'un tel groupe, défini par référence à la haine, la couleur, la religion, l'ascendance, l'origine nationale ou éthique » et si ces incitation ce font « par diffusion ou distribution publiques d'écrits, d'images ou d'autres supports »[71].

**b) Stratégie globale[72]** : *une nécessité*

La stratégie commande d'identifier la lutte contre la cybercriminalité par rapport aux concepts de cybersécurité et de cyber-défense, mais avant toute chose « la prévention, l'internaute » qui est considéré comme l'acteur principal de la réponse à la cybercriminalité, car la sensibilisation et parmi les solutions qui mettront en échec les menées des délinquants.

[71] Rapport sur la cybercriminalité, op-cit, 2014.

[72] Idem, P.95.

Cependant, l'Etat ne peut réagir seul. La stratégie consiste, alors, à développer un partenariat public-privé, ensuite réorganiser les services de l'Etat pour rendre l'action de ce dernier plus efficiente et cohérente, enfin elle doit s'accompagner des moyens nécessaires notamment en ressources humaines pour les services spécialisés.

L'Europe souhaite adopter une stratégie globale anti-cybercriminalité et pour cela elle doit s'interroger notamment sur La:

- Sécurité des systèmes d'information
- Prévention
- Formation des acteurs (programme de soutien)
- Partenariat public-privé
- Réorganisation de services de l'Etat

**b-1) Sécurité des systèmes d'information :**

Pour faire face aux risques d'attaques informatiques, l'ANSSI[73] (Agence Nationale de Sécurité des Systèmes d'Information), créée en juillet 2009, se voyant confier des missions de défense des systèmes d'information, aboutit, en 2010, à la définition d'une stratégie nationale de défense et de sécurité des systèmes d'information par la France. Cette stratégie dite de « cyber sécurité » repose sur 4 objectifs :

- Etre une puissance mondiale de cyber défense, afin de protéger les réseaux de communication électroniques (contre les cyber-espionnage) ;
- La protection de l'information de souveraineté, pour garantir une liberté de décision d'ordre diplomatique, militaire, scientifique, technologique, commerciale ou financière ;
- Renforcer la cybersécurité des infrastructures vitales nationales, c'est–à-dire des opérateurs publics et privés (les réseaux de télécommunication) et Internet car ils

[73] l'ANSSI a un rôle qui est d'ordre préventif: elle joue, le rôle d'expert étatique s'agissant de la sécurisation des systèmes d'information auprès des administrations comme des opérateurs sensibles. Elle réalise donc, des diagnostics (sur les moyens de communication sécurisés de l'Etat ou, pour prendre des exemples intéressants le système judiciaire, les bracelets de surveillance électronique, la gestion des clés dans les établissements pénitentiaires, la future plate-forme des interceptions judiciaires...), fait des recommandations (par exemple, sur les badges d'accès, la vidéo-surveillance...). Elle assure, aussi, une mission d'audit et d'inspection, à la fois au plan organisationnel et s'agissant des risques d'intrusion (centrales nucléaires, tunnel sous la Manche, application pénale Cassiopée...). Elle exerce, encore, un contrôle sur les investissements étrangers dans le domaine de la sécurité informatique. Elle entretient, enfin, des relations étroites avec les organismes comparables des pays étrangers. Voir le rapport sur la lutte contre la cybercriminalité, « protéger les Internautes », rédigé par Marc ROBERT, Février 2014, P.105

concourent à la satisfaction des besoins de vie des populations et à l'exercice de l'autorité de l'Etat.

- Assurer la sécurité dans le cyberespace, par la protection des systèmes d'information par la sensibilisation des entreprises et des particuliers grâce à une meilleure adaptation du droit et une amélioration de l'entraide judiciaire internationale.

**b-2) La prévention[74]** :

La prévention est une priorité qui distingue deux facettes : prévenir les internautes des dangers qu'ils encourent ; prévenir la commission des infractions :

- **Prévenir les internautes** : c'est les informer des risques qu'ils encourent sur Internet et des moyens de s'en prémunir. Toute personne peut être victime de cyber-infractions. Informer les internautes c'est d'abord les protéger contre eux même car souvent il peut être le « facilitateur involontaire »[75].

  Parmi les actions de prévention mises en œuvre par les départements ministériels, on cite :

  - **La délégation aux usages de l'Internet** : créée en décembre 2013, elle a pour mission de généraliser l'accès à Internet et former le grand public des usages des nouvelles technologies.
  - **La gendarmerie Nationale** : elle a adapté un dispositif de lutte contre les cyber menaces avec l'opération « permis Internet » qui consiste à sensibiliser les publics scolaires aux danger d'Internet et donner des conseils pour une utilisation sécurisée ainsi que la distribution d'un guide du bon usage des médias sociaux adapté au milieu professionnel.
  - **Les policiers formateurs anti-drogue (FRAD)** : ils sont sollicités pour parler des dangers de l'Internet en s'appuyant sur des vidéos pour favoriser une prise de conscience.
  - **L'OCLCTIC[76]** : depuis 2009, il gère une plate forme nationale téléphonique dite « info Escroquerie », pour les particuliers qui sont exposés à des tentatives d'escroquerie sur Internet, litige commercial ou civil.

[74] Voir le rapport sur la lutte contre la cybercriminalité, op-cit, P.103.
[75] On désigne le fait que l'internaute dévoile avec crédulité des informations confidentielles et personnelles par voie de « Spam » ou «Phishing », comme il a été cité en première section du chapitre 02.
[76] L'office Centrale de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) a été créé le 15 mai 2000. Les missions de l'Office recouvrent l'animation et la coordination opérationnelle et technique, au niveau national, de lutte contre la cybercriminalité. Il lui appartient

- **L'ANSSI** : s'emploie à mettre en ligne du matériel pédagogique ou des conseils pratiques.

- **Prévention de la commission des infractions** :

  La sensibilisation des internautes ne suffit pas car les modes opératoires ne cessent de se renouveler[77]. La recherche et l'industrie européenne se mobilisent sur la conception de logiciels de sécurité susceptibles de prévenir voir répondre à la délinquance organisée. Ils préconisent, donc :

  - Une sécurisation par défaut d'un certain nombre d'accès informatique ;
  - L'initiative ou l'impulsion des pouvoirs publics à bloquer certains flux informatiques ou supprimer les outils utilisés pour commettre des infractions ;
  - De faire de l'internaute le premier acteur de sa propre sécurité et de la lutte contre les propos et comportements illégaux ;
  - Le développement d'espaces d'information en ligne ou par téléphone ;

**b-3) Formation des acteurs[78] :**

La formation des magistrats, policiers, gendarmes, douaniers et fonctionnaires des autres administrations contribue à la lutte contre cette criminalité. A cet égard, il est préconisé de :

- Sensibiliser, à caractère obligatoire, l'ensemble des acteurs à la cybercriminalité, aux enjeux et aux modes de traitement dans les différentes écoles de formation ;
- Institutionnaliser une formation dans les différents services territoriaux ainsi que les juridictions non spécialisées ;
- Mettre en œuvre des formations plus approfondies qui seraient prolongées par la création d'un réseau social interne qui favoriserait les échanges inter-actifs ainsi que l'entraide;
- Enrichir la formation sur la base de volontariat pour assurer l'actualisation des connaissances ;

également de fournir une assistance technique, pour les dossiers les plus sensibles et les plus complexes, à d'autres services de police ou de gendarmerie. Il est le point de contact international dans son domaine de compétence et participe aux travaux opérationnels et stratégiques des enceintes internationales (G8, Europol, Interpol, etc.) ; voir le lien : http://www.pointdecontact.net/partenaires/oclctic

[77] Les infections informatiques et les techniques d'arnaques ne cessent d'évoluer tout en s'adaptant aux nouveaux services mis à la disposition des internautes, tout comme les auteurs de ces menaces qui ne cessent de renouveler leurs modes opératoires. Plus de détail voir le rapport de l'Euro sur la lutte contre la cybercriminalité et protection des internautes, P.110.

[78] Voir le rapport sur la cybercriminalité, protéger les internautes, 2014, PP.113-124.

- Développer des actions partenariales entre les différentes écoles ainsi qu'avec les acteurs privées compétents pour favoriser une approche pluridisciplinaire ;
- Inciter les universités à accroitre les formations spécialisées en la matière pour développer l'expertise de lutte contre la cybercriminalité.

**b-4) Le partenariat public-privé**[79] : l'enjeu de lutte contre la cybercriminalité nécessite un dialogue entre l'ensemble des acteurs pour l'échange d'informations, l'analyse de la menace ou encore de recherche et de développement. On présente un certain nombre de partenariats sous différentes formes :

- Dialogue institutionnel, on cite :

  - L'observatoire de la sécurité des cartes de paiement(OSCP)[80] : il réunit les pouvoirs publics, les acteurs économiques et sociaux concernés par la sécurité des instruments de paiement et les experts (au titre de leurs compétences individuelles).

  -**PHAROS** : c'est une plate-forme de signalement des contenus illégaux ou des activités illégales sur Internet. Il est placé au sein de l'O.C.L.C.T.I.C.,

- Dialogue partenarial : représente les associations et les partenariats, on distingue quelques-uns comme:

  -**Signal Spam**[81] : association qui rassemble des représentants du pouvoir public membre de droit, des opérateurs de communication (Orange, SFR, Google) et des entreprises qui œuvrent dans la sécurité numérique.

  -**Association phishing initiative**[82] : cette association regroupe MICROSOFT, PAYBAL et le CERTLEXI, elle a pour but de prévenir les tentatives de hameçonnage (phishing) mettant en ligne un site pour signalement aux internautes.

  -**Forum international sur la cybersécurité** ; c'est une grande conférence internationale qui permet d'établir un dialogue avec l'ensemble des acteurs de la cybersécurité.

[79] Rapport sur la cybercriminalité, Op-cit, 2014,
P.125.

[80] Il a pour missions *(cf. art. L.141-4 et R.141-1 du code monétaire et financier) :*
-de suivre la mise en œuvre des mesures adoptées par les émetteurs et les commerçants pour renforcer la sécurité des cartes de paiement- d'établir des statistiques en matière de fraude sur la base d'information que lui adressent les émetteurs de cartes de paiement - d'assurer une veille technologique en la matière, dans le but de proposer des moyens de lutter contre les atteintes de cette nature à la sécurité des cartes de paiement.

[81] http://www.signal-spam.fr

[82] http://www.phsihing-initiative.com

- Recherche et formation[83] : constitue les relations nouées entre l'Etat, et les différents services de l'Etat, et des établissements de formation ou de recherche et parmi lesquelles on cite :

  -**CYBERLEX** [84] : créée en 2006, cette association de droit et des nouvelles technologies regroupe les techniciens, les juristes, les avocats, et professeurs de droit ; elle organise des échanges réguliers sur le droit de l'Internet.

  -**Le CLUSIF**[85] : c'est un club professionnel constitué en association indépendante et ouverte à toute entreprise et collectivité. Elle sensibilise les acteurs et agit pour la sécurité de l'information.

  -**Le CESIN**[86] : le club des experts de la sécurité de l'information et du numérique est une association composée d'experts de sécurité dans des entreprises privées ou publiques, des spécialistes de droit de la sécurité, associant les représentants des services de l'Etat. Elle a pour objet le partage d'expérience et la coopération entre professionnels de la sécurité de l'information et du numérique.

**b-5) La réorganisation des services de l'Etat[87]** :

Les enjeux, que cette criminalité représente, appellent à une nouvelle efficacité de l'Etat, qui passe par 3 niveaux :

- Création d'une Délégation Interministérielle de lutte contre la ybercriminalité : sous la direction du premier ministre, elle aurait pour mission de définir puis d'impulser une stratégie d'ensemble, en synergie avec les autorités de cyber défense et de sécurité des systèmes d'information, veiller à la réalisation de plans de formation par les différents départements et acteurs, assurer l'interface avec le secteur privé dans le cadre d'une agence de régulation qui veille à la mise en œuvre des normes applicables, elle servirait d'instance de médiation pour les internautes, etc.
- L'organisation judiciaire : créée au sein du ministère de la justice, elle serait chargée de veiller à l'harmonisation des normes et à l' évolution des dispositifs judiciaires, de participer à

[83] Voir le rapport de lutte contre la cybercriminalité, PP. 132-133.
[84] http://www.cyberlex.org/
[85] http://www.clusif. asso.fr
[86] http://cesin.fr/
[87] Voir le rapport de lutte contre la cybercriminalité, op-cit, P.137.

l'ensemble des travaux nationaux et internationaux , de mettre en œuvre une politique pénale spécifique, etc.

➢ L'organisation centrale de police judiciaire : qui a pour tâche d'harmoniser la formation des policiers et gendarmes spécialisés, de participer à la gestion des plates-formes PHAROS et aux groupes d'enquête les concernant, etc.

**c) L'arsenal juridique** :

Les Etats ont pris conscience de la nécessité d'une approche transfrontalière de la cybercriminalité, en raison de la dimension internationale de ce phénomène.

La convention oblige les Etats qui l'ont ratifiée à prendre des mesures propres pour, ériger en infraction pénale, un certain nombre de comportements et en particulier[88] :

- Article 4 - Atteinte à l'intégrité des données- : *« le fait intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques ».*
- Article 5 – Atteinte à l'intégrité des systèmes- *: « l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration ; l'altération ou la suppression de données informatique ».*
- Article 6 – Abus des dispositifs- : *« la production, la vente, l'obtention pour l'utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition, » […] « la possession i) d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions (précédentes), ii) d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, » […] « dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions (précédentes) ».*
- Article 7 – Falsification informatique- : *« l'introduction, l'altération, l'effacement ou la suppression intentionnelle et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou*

[88]Pour voir la convention du Conseil Européen, consultez le lien suivant : http://www.senate.be/www/?MIval=/publications/viewPub.html&COLL=S&LEG=5&NR=1497&VOLGNR=1&LANG=fr

*utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient directement lisibles ou intelligibles ».*

- Article 8- Fraude informatique- : *« le fait intentionnel et sans droit de causer un préjudice à autrui i) par toute introduction, altération, effacement ou suppression de données informatiques ii) par toute forme d'atteinte ou fonctionnement d'un système informatique, » […] « dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui ».*

Le tableau ci-dessous résume certaines bases légales et les peines auxquelles le cybercriminel est soumis. Elles sont classées par catégories[89] :

**Tableau n°8 : Les bases légales des principales infractions**

| Catégories | Libellés des infractions | Texte de loi | Codification | Peines |
|---|---|---|---|---|
| **Atteintes aux systèmes de Traitement automatisé de données** | Suppression/Modifi-cation de données | Loi Godfrain 05 I 1998 | Code pénal Art. 323 al.1 | 1an d'emprisonnement + 15 000 € d'amende |
| | Altération de fonctionnement | | Art. 323-1 al.2 | 2ans d'emprisonnement + 30 000€ d'amende |
| | Entrave au fonctionnement | | Art. 323-2 | 3ans d'emprisonnement + 45 000 € + d'amende |
| **Les infractions aux cartes bancaires** | | LSQ A5 XI 2001 Art.35-39 et 40 | Code Monétaire et Financier | 7ans d'emprisonnement |
| **Interceptions** | Régime des interceptions des correspondances émises par voie de télécommunication | Loi Perben II | Code de procédure Pénale Art. 706-95 | Autorisation par le juge des libertés, à la requête du Procureur, pour une durée de 15 jours renouvelables une fois |
| | Violation de correspondance (interception illégale) | Ordonnance n°2000-916 du 19/9/2000 | Code Pénal Art. 226-15 et 432-9 | 1an d'emprisonnement+ 15 000€ d'amende (3ans et 45000€ si auteur dépositaire autorisé publique ou exploitant de réseau de télécom) |

[89] Voir toutes les infractions définies selon la législation européenne dans le rapport sur la cybercriminalité-Annexes, « protéger les internautes », février 2014, P.45. Ainsi que les peines qui leurs sont attribuées, PP.86-129.

| | | | | |
|---|---|---|---|---|
| **Escroquerie en ligne** | L'escroquerie par l'utilisation frauduleuse de numéros de cartes de paiement sur Internet et les escroqueries en général | | Code Pénal Art. 313-1 | 5ans d'emprisonnement + 375 000€ d'amende |
| **Atteinte aux personnes** | Usurpation d'identité | | Code pénal Art.434-23 | 5ans d'emprisonnement+ 75 000€ d'amende |
| | Atteinte à la vie privée | | Art.226 al.1&2 | 1an d'emprisonnement et 45 000€ d'amende |
| | Dénonciation calomnieuses | | Art.226-10 | 5ans d'emprisonnement + 45 000€ d'amende |

**Source :** Etabli sur la base des données sur les infractions et les peines dans le rapport annexes de lutte contre la cybercriminalité, « protéger les internautes », Février 2014.

Chaque Etat de l'Union est tenu d'adopter les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes[90] :

- **Article 16** – Conservation rapide de données informatiques stockées- *: « à ordonner ou imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de pertes ou de modifications ».*
- **Article 18** – Injonction de produire- : *« à ordonner : i) à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ; et ii) à un fournisseur de service offrant des prestations sur le territoire, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services ».*
- **Article 19** – Perquisition et saisie de données informatiques stockées – *« à perquisitionner ou à accéder d'une façon similaire : i) à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et ii) à un support du stockage permettant de stocker des données informatiques » […] « à*

[90] Voir la convention du Conseil de l'Europe relative à la cybercriminalité, sur ce lien : http://www.senate.be/www/?MIval=/publications/viewPub.html&COLL=S&LEG=5&NR=1497&VOLGNR=1&LANG=fr

*saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé ».*

- **Article 20** - Collecte en temps réel des données relatives au trafic- : *« à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire » […] « les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique* » (ou à obliger un fournisseur de services à le faire ou à prêter son concours et son assistance pour le faire ).
- **Article 21** – Interception de données relatives au contenu- : « *en ce qui concerne un éventail d'infractions graves » […] « à collecter ou à enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique* » (ou à obliger un fournisseur de services à le faire).

### II- La réponse des Etats-Unis :

Les Etats unis sont considérés comme un modèle en matière de lutte contre les cyber-attaques pour 44% des sondés, néanmoins ils sont considérés comme l'un des 3 pays les plus vulnérables aux cyber-attaques sur les infrastructures critiques dans leurs secteurs, suivie par la Chine et la Russie.

Les pays souvent cités comme sources d'attaques sont également parmi les plus touchés (voir le tableau ci-dessous)

**Tableau n°9 : Cibles des attaques**

| rang | Pays | Nombre d'attaques | Part du total(%) |
|---|---|---|---|
| **1** | Etats- Unis | 143 | 20,5 |
| **2** | Brésil | 87 | 12,4 |
| **3** | Philippines | 64 | 9,2 |
| **4** | Chine | 52 | 7,4 |
| **5** | Malaisie | 37 | 6,3 |
| | Autres | 309 | 44,2 |

**Source :** ATLAS, 2011

### a) La coopération Internationale dans la lutte contre la cybercriminalité :

Face à ce phénomène, les Etats-Unis se sont positionnés comme leader dans la mise en place d'une stratégie de coopération internationale renforcée dans le domaine de la cybercriminalité. Hillary CLINTON, Eric HOLDER, 82$^{éme}$ procureur général des Etats Unis et Howard SMICHDT, coordinateur Cybersécurité de l'administration OBAMA, ont tous les trois présenté un document intitulé : « **International strategy of cyber-espace : Property,**

**Security and Opennes, in a Networked World** »[91] qui présente, selon eux, les priorités en matière de sécurisation d'Internet et de lutte contre la cybercriminalité.

Il est précisé, dans le rapport[92], que les Etats-Unis souhaitent construire un environnement international qui assure l'ouverture des réseaux à de nouvelles innovations, garantissant la sécurité des supports de travail, pour gagner la confiance des internautes. Le président OBAMA souhaite construire et maintenir un environnement dans lequel des normes de comportements guideront les actions des Etats, d'entretenir des partenariats et garantir la primauté du droit[93].

A cet égard, les Etats Unis s'efforcent de bâtir une coopération internationale entre acteurs publics et privées. Parmi les actions émanant de cette coopération :

- ✓ **Ouverture d'un bureau de lutte contre la cybercriminalité** en Estonie (un pays qui a été victime de plusieurs attaques informatiques ces dernières années) où ils offriront des séances de formation afin d'aider les forces de l'ordre de l'Estonie, de la Lettonie et Lituanie à combattre les crimes informatiques mais aussi le blanchiment d'argent, etc.
- ✓ **Les Etats Unis comme leader et défenseur** d'un Internet libre, ouvert et sécurisé[94].
- ✓ **Création du Cyber command** aux USA et sa certification opérationnelle en novembre 2010, qui est un système de défense qui agit pour la protection des réseaux et infrastructures vitales.

### b) Qualification pénale[95] :

Les Etats- Unis ont déterminé, au niveau fédéral, certaines infractions spécifiques, qui sont citées comme suit :

- ✓ L'obtention d'informations relatives à la sécurité nationale, est punie de 10 à 20 ans d'emprisonnement ;

[91] Pour plus de détails concernant la stratégie destinée au Cyberespace, voir le lien suivant : https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[92] Idem.

[93] ENDERLIN Clément, op-cit, P.104.

[94] Dans le rapport, le président des Etats Unis prévoit le recours à la légitime défense en cas d'attaques informatiques sur des infrastructures vitales pour l'économie : *« lorsque c'est justifié, les Etats-Unis répondent aux actes hostiles dans le cyber espace comme nous le ferons pour n'importe quelle autre menace sur notre pays. Tous les Etats possèdent un droit inhérent à la légitime défense […] Nous nous réservons le droit d'utiliser tous les moyens nécessaires, diplomatiques, informationnels, militaires et économiques, le cas échéant et conformément au droit international applicable, afin de défendre notre nation, nos alliés, nos partenaires et nos intérêts »*.

[95] LegiGlobe, L'accès francophone aux droits, « La cybercriminalité (Brésil, Espagne, Etats-Unis, Royaume Unis, Pays-Bas, Chine, Allemagne) », P.3. Voir le lien suivant : http://legiglobe.rf2d.org

- ✓ L'accès à un ordinateur et l'obtention d'information sans autorisation, est puni de 1 à 5 ans d'emprisonnement ;
- ✓ L'accès illégal à un ordinateur du gouvernement est puni d'un an d'emprisonnement ;
- ✓ L'accès à un ordinateur en vue de commettre une escroquerie et d'acquérir des informations, est puni de 5 ans d'emprisonnement ;
- ✓ L'endommagement intentionnel d'un ordinateur en transmettant une donnée, est puni de 1 à 10 ans d'emprisonnement.
- ✓ L'endommagement par négligence ou imprudence après avoir eu accès intentionnellement à un ordinateur, est puni de 1 à 5 ans ;
- ✓ Les dommages et pertes causés par négligence après avoir accéder intentionnellement à un ordinateur est puni d' 1 an ;
- ✓ Le trafique de mot de passe est puni d'1 an ;
- ✓ L'extorsion par l'intermédiaire d'un ordinateur est punie de 5 ans d'emprisonnement.

**c) Les polices spécialisées** :

les Etats-Unis ne font pas l'objet d'une centralisation des réponses au sein d'un service de police ou d'une juridiction unique, un nombre important de services d'enquête y sont chargés de lutter contre les différents aspects de la cybercriminalité, au travers du **FBI** ; C'est le plus important service de police judiciaire et de contre espionnage. Ses trois priorités sont :

- L'intrusion dans les réseaux informatique ;
- L'usurpation d'identité ;
- Les fraudes.

Le FBI a mis en place plusieurs structures administratives spécifiques qui puissent répondre aux spécificités de ce type de délinquance, parmi elles :

- La « **Cyber Division** » : réorganisée en 2012, se concentre sur la sécurité des réseaux.
- **IC3** *(Internet Crime Complaint Center)* : c'est un centre de gestion des plaintes des victimes d'infraction liées à Internet (il s'agit de l'équivalent de PHAROS en France).
- La **NCFTA** *(National Cyber Forensics Training Alliance) :* créée en 1997, c'est un centre d'analyse des menaces sur Internet qui rassemble les services de polices, les entreprises concernées par la sécurité informatique et les universités. Son rôle est de faire remonter les menaces et de diffuser les risques identifiés à l'ensemble du secteur privé. Il mit en place la « CIRFU » *(Cyber Initiative and Ressource Fusion*

*Unit),* en collaboration avec « IC3 », qui est une plate-forme de dialogue entre les pouvoirs publics et le secteur privé et qui a pour rôle la recherche de menaces, l'orientation des enquêtes vers les services appropriés et l'échange entre acteurs privés.

- Le « **Department of Homeland Security** » : a été créé, suite aux attentats du 11 septembre 2001, dans un objectif de coordination des agences fédérales et il a pour mission la protection des frontières. Pour élargir et développer ses compétences sur la cybercriminalité, elle a trois unités rassemblées dans le *Cyber Crime Center* et qu'on cite :

  - ***« Computer Forensics Unit »:*** c'est une unité de personnels spécialisés qui comporte un réseau de techniciens judiciaires spécialisés ayant un rôle de conseil pour les services de terrain et d'assistance dans certaines opérations d'extraction de données.

  - ***« Cyber Crimes Unit » :*** c'est un service, d'enquêtes, spécialisé qui réalise des opérations d'infiltration pour identifier des infractions de fraude, de contrefaçon ou de contrebande douanière. Il dispose de pouvoir de réquisition administrative qui lui permet d'obtenir rapidement des informations des opérateurs téléphoniques et fournisseurs d'accès à internet, notamment en matière d'import/export de marchandises prohibées ou de contrebande.

  - ***« Child Exploitation Unit » :*** est une unité exclusivement chargée des infractions commises sur mineurs et identifiées grâce à Internet (la pédopornographie, les atteintes sexuelles en contactant des mineurs sur les réseaux sociaux). Ce service gère une base de données de toutes les adresses IP qui ont été ciblées, afin de déterminer des objectifs à partir des informations transmises.

**d) La politique de prévention** :

La politique de prévention de la cybercriminalité est une priorité que le président OBAMA a souligné dans son programme et qui se focalise sur les 3 axes suivants : réduction du risque, réduction de la vulnérabilité et réponse aux intrusions.

**d-1) La réduction du risque :** Elle se fera par le développement de campagnes de sensibilisation du public qui implique la formation des citoyens américains en matière de cybersécurité, la mise en place d'un partenariat avec le secteur privé et d'une coopération internationale.

**d-2) La réduction de la vulnérabilité :** Elle se fera par la protection du « cyber espace[96] ». Les Etats-Unis ont connu plusieurs échecs dans leur lutte contre la cybercriminalité (arrêt d'usines électriques, coupures électriques dans les villes, processeurs de paiement compromis et transactions bancaires frauduleuses depuis 130 automates dans 49 villes pendant 30 secondes, pertes systémiques, touchant la propriété intellectuelle) engendrant des milliards de dollars de perte. La« cybersécurité » est ainsi devenue une priorité nationale.

**d-3) La réponse aux intrusions :** Elle suppose le développement de liens importants avec le secteur privé notamment dans le rapport des infractions dont ils ont été victimes. Les victimes commerciales ont un intérêt réel à rapporter aux services de police judiciaire les infractions liées à la cybercriminalité (mais les victimes se montrent réticentes à le faire en raison de la répercussion de cette publicité sur leur clientèle).

**Conclusion**

Les cibles de la cybercriminalité n'épargnent aucune catégorie de victimes potentielles, depuis les particuliers eux-mêmes, utilisateurs d'Internet, jusqu'au monde de l'entreprise et les services de l'Etat[97]. La stratégie de lutte suivie par les Etats en Europe comme aux Etats Unis touche à deux points de vue essentiels politique et économique. D'abord, du point de vue politique, l'efficacité de la sécurité tend à favoriser les démarches d'externalisation des services et de la sécurité des systèmes et des informations. Elle peut néanmoins induire une dépendance ce qui peut constituer un risque à la souveraineté d'un Etat qui ne doit pas être dépendant pour leur gestion stratégique et opérationnelle de leur sécurité et cela en imposant le respect des normes de sécurités, de disposer de la sécurité en mode natif (par défaut) de

[96] Dans la « National Security Presidential Directive » n/54 c'est comme le réseau interdépendant d'infrastructures technologiques de l'information, réseau qui comprend Internet, les réseaux de télécommunication, les systèmes informatiques ainsi que les processeurs intégrés et les régulateurs dans les industries concernées.

[97] Rapport sur la cybercriminalité « protéger les internautes », 2012, P.30.

manière compréhensible, transparente et contrôlable, etc. Du point de vue économique[98], la sécurité ne permet pas de gagner de l'argent, mais elle évite d'en perdre. La valeur économique de la sécurité est à appréhender dans toute sa dimension sociétale et tient compte des impacts des nouvelles technologies pour les individus, les organisations et les nations et ne peut se réduire à des coûts d'installation et de maintenance.

[98] Rapport de l'UIT, « Guide sur la cybersécurité pour les pays en développement, P.16.

**CONCLUSION**

La cyber- menace est classée au troisième rang des risques, juste après la guerre et les attaques terroristes. L'espionnage qui émane, parfois, d'entreprises concurrentes, le piratage d'un site ou un déni de service, plus encore, des détournements de données livrées au public pour des tentatives de déstabilisation ou à des fins de propagande[99].

Aujourd'hui, certains États plus touchés que d'autres (comme les Etats Unis et l'Europe) ont compris les enjeux de la cybersécurité et investissent fortement dans ce domaine. Seulement, il y'a de grandes entreprises et des institutions qui adoptent une approche encore trop timorée et réductrice face à l'évolution des menaces. Certaines ont su avancer, car elles ont été durement touchées par un incident quelconque. Chaque acteur du cyberespace doit prendre conscience des risques même s'il est difficile d'avoir une idée claire de la stratégie à mettre en place et à suivre face à des menaces qui sont en constante évolution.

Avec la multiplication des attaques, les révélations et les actions des États dans leur cyber-défense, s'offre une opportunité sans pareil pour maitriser le sujet de la cybercriminalité en profondeur. Certains Etats, comme l'Algérie, ne sont plus à fonction de sensibiliser, elles sont souvent « en attente »! Il est alors grand temps de leur apporter une démarche claire et simple pour protéger les clients et le patrimoine des entreprises et institutions financières.

[99] Abdelaziz Derdouri, Cybersécurité : Etats des lieux en l'Algérie, 2014, (Article du 19 Décembre), voir sur le lien : http://www.ssri.dz/la-cyber-securite-etat-des-lieux-en-algerie/

# - CHAPITRE III -

## Introduction

L'expansion rapide des technologies de l'information et de la communication (TIC) dans les dix dernières années est devenue un vrai problème dans les pays qui visent à accélérer la modernisation de leur économie en développement et essayent de combler le fossé numérique avec les pays développés.

L'Algérie est touchée par cette évolution. Ces autorités ont reconnu l'importance des technologies de l'information et de la communication et visent à transformer le pays en une société de l'information. Ainsi elles font donc un effort pour diffuser les TIC de manière cohérente et continue pour combler le fossé qui sépare l'Algérie de ses voisins en ce qui concerne l'utilisation d'Internet, de la téléphonie fixe et de la téléphonie mobile[1].

En Algérie les revenus du secteur des TIC représentent environ 1% du PIB[2]. Selon le rapport de la conférence des Nations Unies sur le commerce et le développement (CNUCED), ayant trait au développement de la société d'information, à travers l'investissement dans les projets logiciels, l'Algérie aura déboursé 4586 millions de dollars en total en 2011, dans les technologies de l'information et de la communication[3]**.**

Le développement des nouvelles technologies de l'information et de communication (TIC) et la ruée vers la modernisation des infrastructures en Algérie, a fait naitre un nouvel espace « Le cyber espace », où circulent des flux d'informations numériques et où s'effectue toutes sorte de transactions et prestations électroniques qui accueillent des comportements illicites, et là, un phénomène nouveau est né « La cybercriminalité ».

**S**elon le rapport de Microsoft Security Intelligence[4] (SIRv16), l'Algérie est la cible principale de cyber attaques, parmi ces attaques, le piratage informatique. L'Organisation Business Software Alliance a révélé que le taux de piratage des logiciels (tous logiciel confondus) en Algérie a atteint 84% en 2011, ce qui la classe premier pays arabe en piratage[5].

Dans le rapport de Microsoft Security Intelligence l'Algérie est à la troisième position dans le monde, juste avant le Pakistan et l'Indonésie. Selon le même rapport, 49% des ordinateurs en

[1] Rym Bouchelit, « Les perspectives d'E-banking dans la stratégie E- Algérie 2013 », thèse de doctorat en sciences économiques, université Abou Bekr Belkaid, Tlemcen, 2014-2015, page 106.
[2] Nadia Chettab, « Economie, TIC et bonne gouvernance en Algérie », papiers imprimés, Université Badj Mokhtar, Annaba, page 4.
[3] Rapport de la CNUCED, 2014.
[4] Revue N'tic, juin 2014, Algérie, page 22.
[5] Idem, page 20.

Algérie ont détecté une menace de ce type au premier trimestre de l'année 2013 contre plus de 59% des machines au deuxième trimestre. Le taux de cyberattaque reste élevé sur le reste de l'année 2013, avec plus de 47%des ordinateurs algériens qui ont fait face à une attaque au troisième trimestre et plus de 55% au quatrième trimestre. Sur l'ensemble de l'année passée, ce sont plus de 40% des ordinateurs, équipés de Microsoft, qui ont été infectés par un logiciel malveillant. Soit près de un sur deux[6].

L'évolution technologique a incité la majorité des pays du monde à mettre en place des dispositifs appropriés aux différentes utilisations de l'outil informatique (comme les données personnelles, signature numérique, cybermarché, etc.). Entre temps, de nouvelles formes de criminalité ont évolué dans le cyber espace incitant donc l'Algérie à se doter d'un arsenal juridique et à adopter des lois spécifiques relatives à la prévention et à la lutte contre les infractions liées aux TIC, celle en 2009, venu compléter celle de 2004 en modifiant et complétant le code pénal. Dans ce chapitre nous analyserons d'abords, le degré d'introduction des TIC en Algérie, en allons plus loin au niveau du secteur bancaire, ensuite on donnera une idée sur l'ampleur du phénomène de cybercriminalité dans notre société pour enfin, démontrer les outils de protection et de sécurité au niveau macroéconomique c.à.d. pour l'Etat algérien et au niveau microéconomique du secteur bancaire et ce par l'étude et l'analyse d'un questionnaire élaboré par nos soins.

## Section 01 : L'Algérie face au phénomène de cybercriminalité

L'Algérie fait partie des pays qui s'intéressent le moins aux technologies d'information et de communication, mais ces dernières années le pays essaie de rattraper son retard en multipliant les réformes et les initiatives d'investissement dans le secteur des TIC. L'implication de ce dernier dans la compétitivité et la croissance et le développement économique est très limitée, malgré l'usage lent mais plus généralisé d'Internet et des moyens de télécommunication cela n'a pas empêché le développement des délits liés à leurs usages. Dans un premier point nous essaierons de voir l'état des lieux des TIC sur le territoire algérien au travers de trois (03) indicateurs, puis de démystifier la situation de l'Algérie face à la cybercriminalité.

[6] Revue N'tic, juin 2014, Algérie , page 22.

## I- Etat des lieux en matière de TIC en Algérie

Selon le rapport de l'Union Internationale de Télécommunication (UIT), sur la société d'information et la pénétration du haut débit dans le monde, l'Algérie ne brille pas par son développement, en 2014 elle squatte toujours la même place qu'en 2012 et 2013 c'est-à-dire la 114ème place, il compté parmi les 5 pays du monde arabe à avoir un indice de développement très faible aux coté du Soudan, la Mauritanie, le Yémen et Djibouti. Egalement, d'après le rapport de The Global Information Technology, établie par le World Economic Forum (WEF)[7], l'Algérie gagne 9 places par rapport à l'an passé et prend la 120ème, suivant un classement sur leur capacité à utiliser les TIC pour améliorer leur compétitivité, leur croissance et la prospérité des citoyens. Ce rebond en 2015 est dû au fait que le secteur algérien des technologies de l'information et de la communication s'était d'abord engagé, au cours de ses réformes précédentes avec le soutien de la Banque mondiale, dans une réforme du secteur des postes et des télécommunications (en l'an 2000). Parmi les principales réussites[8], on site:

-l'adoption d'une déclaration de politique des télécommunications pro-libérale en 2000 ;

- la promulgation de la nouvelle Loi sur les Postes et Télécommunications (Loi 2000-03) du mois d'août 2000 ;

- l'établissement d'une entité réglementaire indépendante (ARPT[9]) opérationnelle depuis mai 2001 ;

- la transformation d'Algérie Telecom et d'Algérie Poste en entreprises commerciales, l'octroi à Orascom Telecom Algérie (OTA) en juillet 2001 de la seconde licence GSM pour 737 millions de dollars US[10].

### I.1. Le degré d'introduction :

Pour bien situer la place de l'Algérie dans le développement du secteur des TIC, nous allons démontrer si la société algérienne, s'est approprié les outils TIC, cela par l'étude de certains indicateurs que sont : 1.1) Internet ; 1.2) La téléphonie (fixe et mobile) ; 1.3) la poste.

[7] Le rapport, « The Global Information Technology », Soumitra Dutta (Cornell University), Thierry Geiger, (World Economic Forum), Bruno Lanvin (INSEAD), 2015, page 119, accessible sous format PDF : http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf

[8] The World Bank, « Fondations for the development of information and communication technologies in Algeria", report No. 25841, Avril 2003, page 15.

[9] ARPT : Autorité de Régulation de la poste et des Télécommunications.

[10] Rym Bouchelit, op-cit, page 121.

### I.1.1) Internet :

Internet a fait son entrée en 1991 par le biais de l'Association Algériennes des Utilisateurs d'UNIX et la collaboration de l'Association des Scientifiques Algériens (ASA). On recense 800 administrations connectées en 1999, dont 100 dans le secteur de l'université, 50 dans le secteur médical, 500 dans le secteur de l'économie et 150 dans d'autres secteurs. L'utilisation du réseau Internet connait en Algérie un essor indéniable depuis la fin des années 90, soutenu par la baisse des prix des micro-ordinateurs et par la généralisation de leur utilisation tant par les ménages que les institutions.

Selon les statistiques de l'Union Internationale de télécommunication et du site Internet world statistique[11], en juin 2014, l'Algérie et au nombre de 6 669 927 d'usagers a Internet ce qui représente un taux de pénétration de 17.2% dans le pays, qui est très faible si on le compare à ses voisins maghrébins tel le Maroc où le taux est de 61,3% ou en Tunisie qui est de 46,2%.

**Tableau n° 10**: Nombres d'internautes et taux de pénétration d'Internet

| Année | Nombre d'usagers | Population | Taux de pénétration (%) |
|---|---|---|---|
| 2000 | 50 000 | 31 795 500 | 0.2 |
| 2005 | 1 920 000 | 33 033 546 | 5.8 |
| 2007 | 2 460 000 | 33 506 567 | 7.3 |
| 2008 | 3 500 000 | 33 769 669 | 10.4 |
| 2009 | 4 100 000 | 34 178 188 | 12.0 |
| 2010 | 4 700 000 | 34 586 184 | 13.6 |
| 2012 | 5 230 000 | 37 367 226 | 14 |
| 2013 | 6 404 264 | 38 813 722 | 16.5 |
| 2014 | 6 669 927 | 38 813 722 | 17.2 |

Source : http://www.internetworldstats.com/stats1.htm et www.ons.dz

En 2014, le nombre d'usagers a atteint les 6.669.927 utilisateurs, selon l'ex ministre les TIC, Moussa BENHAMADI, les usagers d'Internet sont représentés par les abonnés à l'ADSL[12]. C'est grâce a cette technique d'accès haut débit via ADSL que l'accès Internet s'est généralisé

[11] http://www.internetworldstats.com

[12]Moussa Benhamadi, « Algérie et la Société de l'Information », voir le lien : www.webreview.dz/IMG/pdf/information-3.pdf. B. Abdelkader, « Le ministre des p'tic avance ses chiffres », disponible sur le site suivant : www.carrefourdalgerie.com/archive/pdf/2013/05/18-05-2013.pdf

en Algérie, son lancement en 2003, après la convention signée par EEPAD (le fournisseur de service Internet) et Algérie Télécom, à partir des lignes téléphoniques classiques[13]. L'année 2011 a été marquée par le programme de développement de l'accès à Internet, de qualité et surtout sécurisé et cela par la généralisation du raccordement par fibre optique qui remplace les câbles en cuivre avec un budget de 80 milliards de dinars[14].

Malgré les efforts consentit par l'Etat Algérien, le développement du réseau Internet reste limité, avec un taux de pénétration relativement faible de 17,2% comparativement à certains pays du Maghreb. L'Algérie reste un pays consommateur passif des technologies d'Internet elle ne se limite qu'à certaines fonctions basiques à l'instar de la correspondance électronique (mailing) et de la communication (chat, téléphone via Internet), la recherche d'information via les moteurs de recherche et le téléchargement des softwares, etc. L'Algérie est pratiquement absente du réseau mondial du Web, avec seulement 1400 sites dont 800 sont actifs, l'Algérie est en retard par rapport a certains pays comme le Maroc avec 6000 sites, 4000 pour la Tunisie, et 800000 pour la France. Selon les statistiques du CERIST, le nombre de nom de domaines « .dz » en Algérie est de 2380[15].

### I.1.2. La téléphonie (fixe et mobile) :

Le groupe Algérie Télécom occupe une place prépondérante dans le marché de la téléphonie fixe. On dispose d'un réseau terrestre de fibre optique qui totalise 15000 km en 2003 et passe a 50000 km déployé à mi 2013 ; l'accès WLL (Wireless Local Loop) c'est une technique sans fil qui offre des services au niveau des zones urbaines, rurales et suburbaines ; 4425 Publiphones gérés par Algérie Télécom et 212040 lignes KMS (kiosques Multiservices) exploitées par des promoteurs privés[16]. Le marché de la téléphonie est essentiel vu la croissance exponentielle du nombre d'abonnement, malgré la stabilité du nombre d'opérateurs et prestataires qui y interviennent. Au plan institutionnel et économique, le développement de l'Internet est encore plus faible car d'après l'ONU, l'Algérie est classé 148ème place en 2014 en ce qui concerne les services en ligne.

[13] Lamri Douidi ; Chabane Khentout et Mahieddine Djoudi, « Place de l'Algérie dans le monde des TIC », page8. Manifest.univ-ouargla.dz/documents/Archive/…/Douidi.pdf
[14] Rym, op-cit, page 132.
[15] Idem, page 135.
[16] UIT, (2009), « présentation du groupe Algérie Télécom », 7ème réunion sur les indicateurs des télécommunications TIC mondiales, Le Caire, Egypte, Mars, p4.

I.1.2.1. Téléphonie FIXE :

Algérie télécom a mobilisé les services de la téléphonie fixe. Les investissements ont augmenté et se font remarqué par l'a augmentation du nombre d'abonnés et du taux de densité de la téléphonie fixe.

a) Nombre d'abonnés à la téléphonie fixe :

Le tableau ci-dessous nous révèle l'évolution du nombre d'abonnés de 2000 à 2013.

**Tableau n°** 11: représentant du nombre d'abonnés à la téléphonie fixe (2000- 2013)

| **Année** | **Nombre d'abonnés** |
|---|---|
| 2000 | 1 761 000 |
| 2005 | 2 572 000 |
| 2007 | 3 113 325 |
| 2010 | 2 922 731 |
| 2013* | 3 317 000 |

Source : Etablie à partir des données d'Algérie Télécom, 12/2013, par Mohamed Amine Kessouri. « les indicateurs de Télécommunication/ TIC : Etats des lieux en Algérie », 11ème réunion sur les indicateurs Télécom/TIC, Mexique. Note : * : Chiffre du troisième trimestre de 2013

Pour 2013, l'année a été marquée par 3,317 millions d'abonnés par rapport a l'année précédente, il y'a eu une évolution de 2,41%. Algérie Télécom est actuellement le seul opérateur de la téléphonie fixe, son concurrent « Lacom[17] » a cessé ses activités en fin 2008.

b) Densité téléphonique :

Le tableau ci-dessous illustre la densité de la téléphonie fixe d'une période allant de 2000 à 2013, selon les chiffres d'Algérie Télécom le taux de pénétration de la téléphonie fixe a enregistré une augmentation de 2000 à 2007 d'un taux de 9, 1% pour réaliser une baisse en 2010 qui atteint 8,05%.

[17] C'est le second opérateur téléphonique fixe en Algérie qui avait commencé son activité en Février 2006.

**Tableau n°** 12: représentation de la densité Téléphonique fixe en Algérie (2000- 2013)

| **Année** | **Densité** |
|---|---|
| 2000 | 5, 90% |
| 2005 | 7 ,90% |
| 2007 | 9,10% |
| 2010 | 8,05% |
| 2013 | 8,75% |

Source : Algérie Télécom 12/2013, par Mohamed Amine Kessouri. « les indicateurs de Télécommunication/ TIC : Etats des lieux en Algérie », 11ème réunion sur les indicateurs Télécom/TIC, Mexique.

L'augmentation est moins importante que celle de la téléphonie mobile, pour des raisons telles que la demande, l'octroi de licences de nouveaux opérateurs, la concurrence.

I.1.2.2. Téléphonie MOBILE :

L'Algérie un connu un vrai « boom » du nombre d'abonnés à la téléphonie mobile qui se répartissent selon les trois opérateurs GSM[18] que sont Djezzy[19], Mobilis[20], Ooredoo[21] et qui se livrent une rude concurrence. La téléphonie mobile a connu l'introduction effective des services de télécommunications mobile 3G[22] dont les 3 opérateurs présents sur le marché ont reçu la licence de les exploiter le 2 décembre 2013 et de lancer leur commercialisation le 15 décembre 2013. C'est donc l'occasion de communiquer quelques chiffres sur ce nouveau sous segment du marché mobile qui représente le segment essentiel du marché des télécommunications de par son chiffre d'affaires et du nombre d'abonnés qu'il compte.

a) Le nombre d'abonnés au réseau GSM[23] :

Le tableau ci-dessous résume le nombre d'abonnés au réseau GSM répartis selon les opérateurs du marché de la téléphonie en 2012 et 2014.

[18] **Global System for Mobile** Communications (**GSM**) est une norme numérique de seconde génération pour la téléphonie mobile. Le réseau GSM est idéal pour les communications de type « voix » (téléphonie). Le réseau étant commuté, les ressources ne sont allouées que pour la durée de la conversation.

[19] OTA, détenu par 96,8% par Orascom Télécom Algérie. Lancement de la 3G en 2013.

[20] ATM, premier opérateur de téléphonie mobile. Filiale de l'opérateur téléphonique Algérie Télécom, il a eu le monopole du marché du cellulaire jusqu'en 2001.

[21] WTA, a démarré ses activités commerciales sous le nom de marque Nedjma et récemment connu sous le nom de Ooredoo le 25 Aout 2004. C'est un opérateur multimédia avec des promotions agressives telles : les minutes gratuites à l'activation, des appels gratuits pendant les soirées, et le lancement du réseau commercial HSPA en 2013 sous le label 3G++.

[22] **La troisième génération (3G)**, elle désigne une génération de normes de téléphonie mobile. C'est une technologie mobile permettant à un téléphone de recevoir un débit bien supérieur aux technologies précédentes, que l'on appelle GSM, et ses applications sont t la visiophonie (voix + vidéo lors d'appels) les besoins en bande passante ont considérablement augmenté (on pourrait définir "*bande passante*" par la capacité d'une antenne d'émettre et recevoir des informations).

[23] Bilan annuel de l'ARPT, l'observatoire du Mobile-Autorité de régulation, 2014, Algérie, page 5.

**Tableau n° 13**: le nombre d'abonné à la téléphonie mobile (2012 /2014)

| | **ATM** | **OTA** | **WTA** | **Total** |
|---|---|---|---|---|
| 2012 | 10 622 884 | 17 845 669 | 9 059 150 | 37 527 703 |
| 2014 | 10 815 000 | 17 887 000 | 8 556 000 | 37 250 000 |

Source : établie sur la base de données de l'observatoire du Mobile-Autorité de régulation (ARPT), 12/2013. Et l'opérateur avant audit de l'ARPT.

On remarque que c'est l'opérateur OTA (Djezzy) qui domine avec 17.887.000 abonnés en 2014 avec une part de marché de 47,55% contre ATM (Mobilis) qui pour sa part a enregistré un nombre de 10.815.000 abonnés avec 28,31% de part de marché, enfin WTA (Ooredoo) avec 8.556.000 d'abonnés a une part de 24,14% de part de marché. Nous constatons alors que c'est Djezzy qui tient la place de leader au réseau GSM.

b) Nombre d'abonnés au réseau 3G (en millions):

Après le lancement de la 3G en décembre 2013, le nombre d'abonnés a atteint les 8 millions en une année (fin 2014) et c'est l'opérateur Mobilis (ATM) qui en est le leader en Algérie avec 3,639 millions d'abonnés.

**Tableau n°** 14: Le nombre d'abonnés à la 3G (en millions)

| | **ATM** | **OTA** | **WTA** | **Total** |
|---|---|---|---|---|
| 2014 | 3, 639 | 0,985 | 3,607 | 8,231 |

Source : le bilan 2014 de l'ARPT.

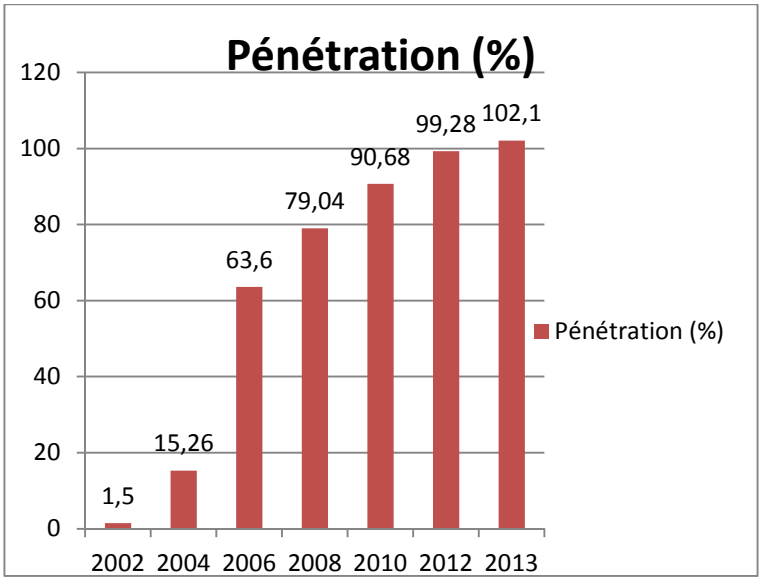
Selon le bilan annuel de l'ARPT, les chiffres ci-dessus démontrent que le parc abonnés à la 3G a enregistré le 30 novembre 2014 une baisse d'environ 277 703 millions d'abonnés par rapport à l'année 2012 et de 1 360 millions par rapport à 2013.

c) Taux de pénétration :

Le marché des télécommunications mobile enregistre une forte croissance. L'histogramme ci-dessous illustre l'évolution du taux de pénétration de la téléphonie mobile. A la fin de l'année 2013 le taux de pénétration atteint les 102 %[24].

[24] Mohamed Amine Kessouri. « Les indicateurs de Télécommunication/ TIC : Etats des lieux en Algérie », 11ème réunion sur les indicateurs Télécom/TIC, Mexique, rapport d'Algérie Télécom, 2013, Algérie, page 16.

**Figure n° 6**: représentation du taux de pénétration de la téléphonie mobile (2002-2013)




Source : Etablit a partir des données du rapport de l'ARPT 2014.

Les taux de la pénétration mobile sont très élevés par rapport aux taux de la pénétration de la téléphonie fixe. Il atteint les 102,1% en 2013.

d) La télé-densité mobile :

Le tableau ci-dessous répartie la densité de la téléphonie mobile par le taux de pénétration de la GSM et le taux de pénétration de la 3G, il est représenté par le nombre d'abonnée par 100 habitants. Le pourcentage enregistré de la densité GSM atteint 94,3 en 2014 contre 20,8% de la densité 3G.

**Tableau n°15** : Densité de la téléphonie mobile (2014)

| | |
|---|---|
| Population (en millions) | 39 500* |
| densité en GSM | 94,3% |
| densité 3G | 20,8% |
| Télé- densité globale | 115,1% |

Source : bilan 2014, de l'ARPT. Note :* chiffre estimé par l'Office National des Statistiques.

Le taux global atteint en 2014 est de 115,1%, soit 115 abonnés pour 100 habitants contre 110,21% en 2013.

**I.1.3. La poste** :

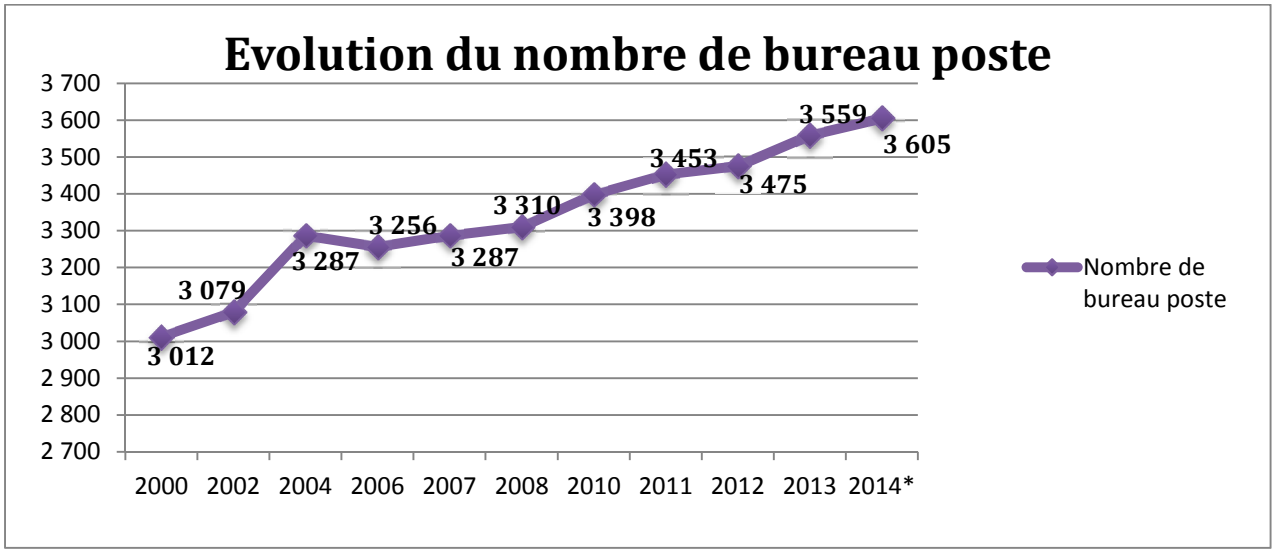
Algérie post pourrait devenir un vecteur essentiel pour la transmission des TIC particulièrement pour la diffusion de point d'accès Internet. Cela pourra contribuer à réduire la fracture numérique, notamment pour les communautés rurales et permettrait ainsi l'accès à de nombreux services gouvernementaux[25]. Parmi ces services : les paiements, les retraits, les virements. Surtout avec le lancement du service Internet e-ccp d'Algérie CCP qui permet la consultation en ligne, la commande de chéquier[26], la généralisation de la CIB (carte inter bancaire) qui éviterait les chaines au moment des retraits de salaires des pensions de retraite et des bourses d'étudiants.

C'est notre troisième indicateur, qui s'effectue sur Algérie Poste et dont le chiffre d'affaire réalisé durant l'année 2013 atteint les 25,2 milliards de dinars, contre 25,8 milliards de dinars en 2012, ce qui fait une diminution de 2,33%. De plus le chiffre d'affaires généré par l'activité postale est estimé à 8,2% en 2013. L'analyse s'effectuera sur la base de deux points : le nombre de bureaux de postes ; densité postale

I-1-3-1-Le nombre de bureaux de postes :

Le tableau ci-dessous représente l'évolution du nombre de bureau de poste sur le territoire national de l'an 2000 à 2014.

**Figure n°7** : représentation de l'évolution du nombre de bureau de poste en Algérie (2000-2014*)




Source : Etablie sur la base des données d'Algérie Télécom, 12/2013. Note : (*) au premier semestre de 2014.

[25] Rym Bouchelit, op-cit, page 126.
[26] Il s'effectue sur le site : Ccp.post.dz

Le nombre de bureau de poste en Algérie, évolue de façon Graduelle mais lente. En 2000, le nombre de bureau de poste a été de 3 012, puis il atteint 3 287 bureaux en quatre (4)ans, ensuite le nombre se rétrograde légèrement à 3 256 en 2006 pour réaliser une évolution qui atteint 3 494 bureaux de poste au premier semestre de 2013.

D'après le bilan de l'ARPT, le nombre total de bureaux de poste sur le territoire national au 1er semestre 2014 a atteint le chiffre de 3605 contre 3559 à la fin de 2013, soit une progression de **1,3%**[27]. Parmi le nombre de bureaux existants, on retrouve que 3489 bureaux qui activent réellement, soit plus de **96,8%**[28], contre 3451 à la fin 2013 dont 1000 sont reliés parle réseau MEGAPAC[29]. Alors il n'y a que 38 bureaux qui ont ouvert leurs portes aux clients durant le 1er semestre 2014. Les services financiers postaux génèrent plus de la moitié des revenus postaux et représentent approximativement 75% des activités des bureaux de poste[30].

I-1-3-2- La densité postale :

D'après le bilan de l'ARPT, on recense au premier semestre 2014, que la densité postale est de 1 bureau pour 10 570 habitants alors qu'elle était de 1 bureau pour 10 502 habitants à la fin 2013. L'opérateur Algérie Poste dispose de huit (08) centres CCP/CNEP MANDAT, qui sont répartis à travers le territoire national. Au mois de juin 2014, l'opérateur gérait a approximativement 17,5 millions de comptes CCP contre 17 millions à fin 2013, ce qui fait une progression de 3%[31].

**I.2. Les TIC dans le secteur bancaire Algérien :**

Le système bancaire à fin 2011, se compose de vingt sept (27) banques et établissements financier, ayant toutes leur siège social à Alger. D'abord six (6) banques publiques dont l'activité contribue à hauteur de 50% à la formation du PIB national, elles sont très centrés sur l'économie nationale et peu vulnérable aux chocs externe. Quatorze (14) banques privées et sept (7) établissements financiers (voir annexe n°7).

Le secteur bancaire algérien a enclenché une vague de modernisation et ce par la mise en place de nouveaux réseaux qui nécessite de gros investissement pour l'acquisition des

[27] Bilan de l'ARPT, 2014, Algérie, page 3.
[28] Idem.
[29] Mohamed Kessouri, op-cit, 2013, page 7.
[30] The World Bank, op-cit, 2013, page 56.
[31]Idem, page 4.

technologies de l'information et de communication. Cette modernisation reposerait sur l'efficacité du réseau de télécommunication qui est le support principal du réseau de monétique, contribuant ainsi à faciliter le fonctionnement des échanges (intra et inter bancaires) et à traiter les opérations de paiement[32].

La modernisation des infrastructures bancaire (c.à.d. le système de paiement) nécessite :

- Une infrastructure qui permet une efficacité, rapidité et sécurité dans le traitement des opérations (interbancaire et de marché) et le développement du système de paiement de gros montant réel et de masse.
- Modernisation du système d'information de la banque d'Algérie qui puisse appuyer le système de paiement et le traitement des opérations de politique monétaire, couverture de change, etc.

Le système bancaire algérien repose sur un système de règlement brut en temps réel et gros montant, dénommé RTGS (ARTS[33]), aussi sur un système de télé- compensation des instruments de paiement de masse qui est géré par le Centre Interbancaire de Pré compensation[34]. Seulement ces deux systèmes nécessitent une mise a niveau du système d'information des banques mis en place durant l'année 2005.

### I.2.1. Le système d'information en Algérie

L'Algérie a reçu de la Banque africaine de développement (BAD) un don en vue du financement du « Projet de Renforcement d'appui à la supervision de la mise en œuvre des plans de modernisation des systèmes d'information des banques publiques »[35].

Ce projet vise à renforcer les capacités des structures du Ministère des Finances, et notamment de la Direction des Banques Publiques et du Marché Financier (DBPMF) qui relève de la Direction Générale du Trésor (DGT), en vue d'améliorer le suivi des plans de modernisation des systèmes d'information (SI) des six banques publiques algérienne afin

[32] BEKHTI Madjid, "Politique de lancement d'un nouveau produit : enjeux des NTIC dans le secteur bancaire algérien, étude de cas: le comportement des clients bancaires avec le multicanal", mémoire de Magister en Marketing, Université de Béjaia, 2013, page 11.

[33] ARTS : Algeria Real Time Settlement.

[34] ATCI : Algérie Télé- compensation Interbancaire.

[35] Banque africaine de développement (BAD), « Règles et Procédures pour l'utilisation des Consultants **»,** édition Mai 2008 révisé en juillet 2012, pp2. Pour plus d'information, s'adresser à Salima BEDRANI, directrice d'Etudes – Coordinatrice du Projet Ministère des Finances, Direction Générale du Trésor, au mail: salima.bedrani@mf.gov.dz

qu'elles se dotent de systèmes d'information performants. Parmi les acquisitions que le projet comporte on distingue[36]:

- Les services de Cabinet de consultants pour les missions :

(i) d'Appui au renforcement des capacités de supervision ; (ii) d'Appui à l'étude d'évaluation (Audit) de la solution « DELTA[37] » ; et (iii) d'Etude de faisabilité relative à Société Service Informatique bancaire et à la mutualisation des infrastructures informatiques-Data center seront acquis par la méthode fondée sur la qualité technique et le coût, en utilisant la demande de propositions type appropriée.

- Les services d'audit financier seront acquis par voie de consultation sur la base de liste restreinte et la méthode d'évaluation sera celle basée sur les Qualifications des Consultants (SQC).

### I.2.2. Le système de paiement en Algérie

Pour être plus compétitive et assuré sa place dans cette mondialisation. L'Algérie a adopté des technologies plus modernes qui incorporent de nouveaux services bancaires tels : Une consultation en ligne par les clients de leurs comptes bancaires, les cartes bancaires, les guichets et distributeurs automatiques,

**a) RTGS[38]** (système de règlements bruts en temps réel de gros montants) ou ARTS :

C'est un système de paiement où s'effectuent les paiements de gros montants ou de paiements urgents. Le ARTS algérien est un système endogène des banques centrales qui le gèrent et l'administrent (de façon automatisé) pour leur compte et pour les opérations interbancaires des paiements par ordres de virement. Et ces derniers sont effectués dans le système un par un et en temps réel (ils ne sont pas compensés). Les paiements**,** dans le système, sont irrévocables et cela pour assurer la libre utilisation des fonds reçus par un participant pour l'exécution de ses propres opérations. Dans le cas d'un paiement par erreur, le participant

[36] Banque africaine de développement (BAD), « Règles et Procédures pour l'utilisation des Consultants **»,** édition Mai 2008 révisé en juillet 2012, pp2.

[37] DELTA : est un logiciel conçu pour réaliser les opérations de banque (de retrait, virements), les opérations de commerce extérieur (crédoc, remise documentaire), autre (comptabilité, gestion de la trésorerie), ce logiciel est généralisé dans toutes les agences et différentes directions comme un bon outil de gestion bancaires

[38] Banque d'Algérie, « Chapitre VI : modernisation de l'infrastructure du système bancaire», Rapport 2009, page 114. Voir le lien (pour télécharger) : https://www.google.dz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CBwQFjAA&urhttp%3A%2F%2Fwww.bank-of-algeria.dz%2Fpdf%2Fchapitre_VI.pdf&ei=NJ9kVfXeLOG7ygPLtoDYCQ&usg=AFQjCNE8hLUTDeVuN-a-L-r45r4eMH554w&sig2=a9HnPFbySdUiTa7PqMn6xA&bvm=bv.93990622,d.bGQ

concerné doit demander au participant qui a réceptionné le virement, de le lui renvoyer pour corriger l'erreur.

Concernant les ordres de virement, les participants utilisent le format de message SWIFT. Ces derniers et en plus du système de transmission, sont généralement utilisés par les banques Centrales, pour assurer la fiabilité et la sécurité des paiements.

Le système RTGS dispose d'une plate-forme de secours à chaud qui prend en charge les opérations en cas de problème. Il est également recommandé qu'il soit doté d'une plate forme de secours à froid (système de secours à distance) qui assure l'archivage des données historiques qui portent sur le paiement et prend en charge les paiements en cas de difficultés (sinistre, séisme,…).

Il est a noté que c'est le premier système de paiement de gros montant opérationnel en Afrique du nord. Aussi, lors de la phase de lancement du système, la banque d'Algérie à requis la mobilisation personnelle, des responsables des banques et d'Algérie Poste, pour la supervision des opérations de paiement et éviter le risque opérationnel inhérent pour leur institution et pour le système bancaire[39].

**b) ATCI[40] (**Algérie Télé- Compensation Interbancaire**)** ou la télécompensation :

En 2004, La banque d'Algérie a créé une filiale avec les banques, le Centre de Précompensation Interbancaire (CPI). Cette filiale a pour mission d'assurer la réalisation du système de télé- compensation, et une fois en place elle assurera son fonctionnement en tant qu'opérateur du système. Pour répondre alors au besoin du processus de modernisation du système de paiement en Algérie et complémenter le système RTGS, Elle mi en place un système de télé- Compensation des paiement par chèque, prélèvements, virements, retraits et paiements par carte bancaire. Sa réalisation s'était poursuivie tout au long de l'année 2005 ket son fonctionnement a été au premier semestre 2006. Parmi les caractéristiques de ce système :

- ✓ Il calcule à la fin de chaque journée de compensation, les soldes multilatéraux nets des participants et les déverse au système de RTGS ;
- ✓ Auto protégé à travers la détermination de limites maximales autorisées de soldes débiteurs qu'il contrôle en permanence, et dans le cas où le solde approcherait la

[39]Banque d'Algérie, op-cit, rapport 2009, page 118.
[40]Idem, page120.

limite autorisée il envoie alors des messages d'alerte à l'administrateur du système et aux participants concernés **;**

- ✓ Sécurisé contre les risques de fraude (les échanges se font par le transfert de fichiers cryptés et scellés) ;
- ✓ Sécurisé contre le risque opérationnel à travers des sites de secours à chaud et à froid ou distant ;
- ✓ Automatisé et dématérialisé qui repose sur les échanges de transactions électroniques dématérialisées (exemple : chèques et effets).

Avec la réalisation du système de télécompensation, une amélioration a été attendu en matière de paiement de masse, de la réhabilitation des moyens de paiements scripturaux classiques tel le chèque, … au développement des moyens de paiement modernes comme la carte bancaire.

**b-1) Les moyens de paiements scripturaux**

Parmi les moyens de paiement scripturaux, on distingue le chèque, le virement, l'avis de prélèvement :

**b-1-1) Le chèque[41]** : il représente 90% de l'ensemble des autres moyens scripturaux. L'essentiel des chèques émis sont des chèques de retrait, En dépit de son utilisation massive en Algérie, le chèque souffre d'un déficit d'image préjudiciable à sa popularité[42]. Puis avec le système de télécompensation, il y'eu un concept de dématérialisation, autrement dit, la numérisation des chèques, pour un enregistrement électronique dans ce système. Les chèques sont alors comptabilisés sous le progiciel DELTA[43], qui a été adopté par le système bancaire algérien, il intègre[44] :

- Le flux financier/ enregistrement informatique ;
- L'image scannée du chèque ;
- La vignette : circulante ou non.

Trois éléments distinguent les opérations de traitement[45] :

- ➢ Les chèques de moins de 50 000DA, (dit M1) sont payés par la banque tirée sur le seul enregistrement de l'image numérisé ;

[41] Il est régis par l'instruction de banque d'Algérie n°05695 du 25/ 01/1995 et les dispositions des articles 472 et suivants du code de commerce, modifiés par la loi 05/02 du 06 février 2005 ; le règlement Banque d'Algérie n° 92/03 du 22/03/1992 plus l'instruction 71/92 du 24/11/1992 ; enfin les normes définies par le comité de normalisation (ABEF).

[42] Hassam Fodil, « Le système bancaire algérien », Edition l'Economiste d'Algérie, Alger, 2012, page 115.

[43] DELTA : est un Progiciel de Gestion Intégrée des opérations bancaires du guichet au siège, pour les banques ou filiales implantées outre-mer (Afrique, Océanie, Moyen Orient et Europe de l'Est).

[44] Hassam Fodil, op-cit, 2012, page 135.

[45] Hassam Fodil, op-cit, 2012, page 136.

- Les chèques dont le montant est compris entre 50 000 et 200 000 DA (dit M2), sont scannés et transmis en complément de l'enregistrement numérisé par la banque du client bénéficiaire à la banque du tireur via un réseau d'échange d'images et de valeurs (REIV). Les vignettes M1 et M2 sont transmises à la banque dans un délai de rejet de trois (03) jours.
- Les chèques a montant supérieur a 200 000DA (dit M3), sont scannés et l'image est transmise en complément de l'enregistrement numérisé et dans ce cas la vignette circulante est transmise via une messagerie traditionnelle.

**b-1-2) Le virement[46]** : il se définit comme un simple paiement de banque à banque. Le RIB[47], est indispensable au bénéficiaire lors de l'émission d'un ordre de virement. C'est un moyen de préparer la bancarisation la plus large des salariés qui s'appuierait sur de nouveaux instruments électroniques de paiements, telle la carte bancaire. Ce mode de paiement est sécurisé et attrayant, car le délai d'imputation sur le compte du client bénéficiaire est court. Seulement, l'indisponibilité d'une plateforme qui permet l'insertion des opérations dans un procès automatisé et qui génère des fichiers fiables et normalisés c.-à-d. l'absence d'un système d'Echange de Données Informatisées (EDI) qui relierait les entreprises et les administrations aux banques.

**b-1-3) l'avis de prélèvement[48] :** Il est émis par un créancier qui demande à sa banque de prélever un montant sur le compte du débiteur. Le RIB et le document autorisant le prélèvement sont remis au créancier au préalable. Le prélèvement concerne les abonnés aux services publics : téléphone, électricité, eau,… etc.

**b-2) La monétique[49] :** Les banques algériennes font partie d'un réseau de monétique interbancaire, qui est géré par la SATIM[50] qui rassemble : BNP Paribas, Société Général, Housing Bank, HSBC, Natixis, BNA, CNEP, BEA, etc. A l'exception d'Algérie Poste et de la

[46] Hassam Fodil, op-cit, page 118.
[47] Le Relevé d'Identité Bancaire (RIB), il a été introduit en Algérie sur arrêté de la banque d'Algérie, en 2005. Il se définit comme un document regroupant les informations nécessaire à l'identification du client. Le RIB est présenté à chaque émission de paiement.
[48] Hassam Fodil, op-cit, page 121.
[49] Hassam Fodil, « Le système bancaire algérien », Edition l'Economiste d'Algérie, Alger, 2012, page 125.
[50] La Société d'Automatisation des Transactions Interbancaire et de Monétique (SATIM), elle a été créée en 1995 à l'initiative de la communauté bancaire. Elle rassemble actuellement 17 adhérents dans son réseau monétique interbancaire : 16 Banques dont 07 banques publiques et 09 banques privées ainsi qu'Algérie Poste. (al baraka, société générale Algérie, BNP paribas, NATIXIS, Housing BANK, BNA, BEA, CNEP, BDL, CNMA, CPA, BADR, Algérie Post).

BADR qui gèrent leurs propres DAB. Le Crédit Populaire d'Algérie (CPA) fut la première banque à lancer une carte de retrait « CPA CASH » ; qui offre un service de base qui est le retrait auprès des agences de la banque dotées d'un distributeur automatique de billets (DAB). L'innovation est intervenue dès 2001/2002 avec le lancement par la Banque Nationale d'Algérie (BNA) d'une carte interbancaire (CIB) ; elle permettait d'effectuer des retraits en espèces (a un plafond autorisé) auprès de l'ensemble des agences de la BNA dotées d'un DAB et des autres banques affiliées au Réseau Monétique Interbancaire[51] (RMI).

**b-2-1) La carte bancaire :** En Algérie on distingue depuis 1999 la distribution de la carte de retrait voyant sa fonction réduite elle laisse place, en 2005, à la distribution de la CIB.

**b-2-1-1) La carte de retrait :** la première période de vie de la carte bancaire entre 1999 et 2002, elle servait en moyenne à effectuer moins de quatre transactions. Durant l'an 2000, le nombre de cartes distribuées dépasse le nombre d'opérations effectuées[52] , d'après la SATIM il y'a 3,56 transactions effectuées sur chaque carte sur une année. Le nombre de carte a évolué de 73,36% contre un volume de transactions de 29,62%.

**Tableau n° 16**: Evolution de la carte de retrait en Algérie

| **Années** | **1999** | **2000** | **2001** | **2002** |
|---|---|---|---|---|
| **Cartes en circulation** | 63 489 | 110 066 | 139 223 | 173 131 |
| **Evolution (%)** | - | 73,36 | 26,49 | 24,36 |
| **Transactions effectuées par cartes** | 247 336 | 320 635 | 501 338 | 666 184 |
| **Evolution (%)** | - | 29,62 | 56,36 | 32,88 |

Source : données de la SATIM

Le marché de la carte de retrait s'est révélé régressif, après une forte émission en 1999 et 2000, la circulation de la carte suit une rythme fléchit en 2002. Selon HASSAM Fodil, la carte de retrait n'a guère bénéficié d'une promotion massive[53].

**b-2-1-2) La Carte Interbancaire (CIB)** : c'est une carte de paiement & de retrait, sa distribution a été dès 2005 et bénéficie d'une validité de 2 ans. Elle est octroyée moyennant une cotisation réglée annuellement par le client à sa banque. Le coût de transaction de

[51] Le réseau monétique interbancaire a été mis en place en 1996, sous la gestion de la SATIM. Les principaux adhérents sont les banques, établissements financiers et Algérie post. Il assure la fonction d'interbancarité des opérations de retrait par porteurs de cartes, de mise a disposition des DAB aux adhérents, préparation et transfert de flux financiers destinés aux opérations de précompensation des transactions DAB.
[52] Idem, page 127.
[53] Idem, page 130.

paiement est gratuit, alors que le retrait est facturé de 10DA-15DA[54], aussi bien en intrabancaire qu'en interbancaire. Elle est délivrée à tous salariés à revenu mensuel régulier et supérieur à 12 000DA. Elle permet à son titulaire d'effectuer des retraits sur les DAB/GAB et de régler des achats auprès des commerces affiliés au réseau monétique interbancaire tels les hôtels, les restaurants, les magasins, les pharmacies, …etc.

On distingue dans le système bancaire algérien deux types de cartes interbancaires, la « carte Classic » et la « carte Gold » :

❖ **La carte Classic** : elle propose des services de paiement et de retrait auprès de tous les automates appartenant aux banques et établissements participants participant au RMI. Les critères d'attribution de cette carte sont arrêtés par chaque banque à sa convenance.

❖ **La carte Gold** : elle obéit aux mêmes principes d'attribution, mais offre des fonctionnalités supplémentaires ainsi que des plafonds de retrait et paiement plus élevés.

**Figure n °8:** CIB Classic[55]


**Figure n°9:** CIB Gold[56]


La CIB est délivrée, pour chaque client détenteur d'un compte chèque, automatiquement (voir l'annexe n°06). Elle peut être émise exceptionnellement sur la demande du client. En cas de perte ou de vol, le client peut faire opposition sur la CIB, et cette dernière sera directement bloquée et peut être renouvelée au bout de six mois. La création de la CIB varie entre 200DA et 500DA pour la **Classic** et de 250DA à 600 DA pour la **Gold**, mais on distingue également des établissements qui proposent la création de la CIB gratuitement. Le tableau ci-dessous nous résume les tarifs de l'émission de et du retrait de la carte CIB par banque :

[54] Le différentiel de 5DA représente la commission interbancaire due par la banque émettrice à la banque acquéreur.
[55] SATIM sur (www.satim.dz)
[56] Idem.

**Tableau n° 17**: Les tarifs de l'émission de la CIB et aux opérations de retrait

| Banque | Prix de Création de la CIB | | Commission sur retrait | |
|---|---|---|---|---|
| | Classic | Gold | DAB de la banque | DAB confrère |
| **BNA** | 300.00 | 500.00 | 23.40 | 29.25 |
| **BEA** | 350.00 | 600.00 | 10.00 | 15.00 |
| **BDL** | 400.00 | 250.00 | 11.70 | 25.00 |
| **BADR** | 500.00 | 500.00 | 11.70 | 35.00 |
| **CPA** | 300.00 | 500.00 | 11.70 | 17.00 |
| **CNEP** | 300.00 | 600.00 | 10.00 | 15.00 |
| **SGA** | 250.00 | 450.00 | 20.00 | 25.00 |
| **BNP Paribas** | 200.00 | 400.00 | Gratuite | 54.00 |
| **NATIXIS** | Gratuite | | 29.25 | 29.25 |
| **AGB** | Gratuite | | gratuite | 29.25 |

Source : SATIM, 2011

Le marché de la carte bancaire a enregistré une amélioration qui se traduit par une évolution assez importante du nombre de carte CIB en circulation, Le nombre de carte en circulation a évolué de 38,61% durant les deux dernières années, comme le montre le tableau suivant :

**Tableau n °** 18: le nombre de carte CIB en circulation 2000-2013

| Années | Nombre de carte en circulation |
|---|---|
| 2000 | 110 066 |
| 2001 | 139 223 |
| 2002 | 173 131 |
| 2003 | 199 266 |
| 2008 | 339 374 |
| 2009 | 569 558 |
| 2010 | 783 311 |
| 2011 | 850 008 |
| 2012 | 1 178 243 |
| 2013 | 1 287 330 |

Source : document de la SATIM

**b-2-2) Les DAB/GAB** :

Le DAB[57] est un Distributeur Automatique de Billets de banque en self-service il permet les retraits d'espèces. Le GAB[58], le Guichet Automatique de Banque, est un automate multifonction qui permet à la fois le retrait et d'autres opérations bancaires et répondant à des normes fonctionnelles, techniques, sécuritaires et ergonomiques. Parmi les avantages qu'ils procurent, on trouve :

-Retrait d'espèces ;-Consultation de solde, -Consultation et impression de l'historique de compte, -Virement compte à compte avec contrôle planché et plafond, -Dépôt de chèque avec ou sans choix de compte, -Dépôt d'espèces avec ou sans choix de compte,-Demande de chéquier, -Demande de RIB.

Le DAB est le seul instrument disponible en Algérie, le tableau ci-dessous nous énumère son évolution de 2009 à 2013, avec le taux de disponibilité des DAB et le nombre de transaction de retrait :

**Tableau n°** 19: Evolution du DAB en Algérie (2008-2013)

| Années | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |
|---|---|---|---|---|---|---|
| Nombre de DAB | 544 | 572 | 636 | 647 | 543 | 534 |
| Taux de disponibilité | - | 84,69% | 83,01% | 84,31% | 86,83% | 86,83% |
| Nombre de transaction de retrait | | 2 615 168 | 3 765 579 | 5 718 663 | 4 582 279 | 2 656 365 |

Source : document fourni par la direction du système d'information de la SATIM, 2014.

Le nombre de transaction de retrait est de 2 656 365, ce chiffre a évoluer de 1,57% entre 2009 et 2013, malgré que le réseau de DAB couvre 86,83% du marché bancaire algérien, on conclu que le nombre de transactions de retrait effectuées représente une quantité négligeable par rapport aux capacités disponible[59].

[57] Comité français d'organisation et de normalisation bancaire, référence déjà cité, p4

[58] Comité français d'organisation et de normalisation bancaire, Terminologie bancaire et financière multilingue, 2003, P20

[59]TEBIB HANA, « la monétique et le e-citoyen en Algérie durant la période 2005-2013 : la contrainte culturelle cas des clients de la banque extérieur d'Algérie et de la banque de l'Agriculture et du développement Rural », dans la Revu des Sciences Humaines, Université Mohamed Khider Biskra, N°34, Mars 2014. pp91-115.

**b-2-3) Les TPE** : Le Terminal de Paiement Electronique, est un équipement, installé chez les commerçants, il permet au porteur de la carte CIB d'effectuer différents types de transactions (achat, remboursement, paiement de facture,...). Pour l'heure, plus de 2900 TPE sont en service à travers l'ensemble du territoire national, chez les pharmaciens, les gérants de grandes et petites surfaces de distribution, des hôtels et des restaurants. À noter que le coût de la transaction de paiement par carte CIB est nul pour le porteur, alors que la redevance du commerçant pour sa banque domiciliataire est de 1,5% du montant de la transaction. Ce taux est identique pour toutes les banques.

De manière sécurisée, rapide et performante. Le nombre de TPE ne cesse de croitre, le tableau ci-dessous nous présente l'évolution du nombre de TPE de 2008 à 2013.

**Tableau n°20** : Le nombre de TPE

| Année | **2008** | **2009** | **2010** | **2011** | **2012** | **2013** |
|---|---|---|---|---|---|---|
| **TPE** | 1 984 | 2 639 | 2 946 | 3 047 | 2 956 | 2 904 |

Source : document de la SATIM, 2014.

Le réseau qui essaie de couvrir les besoins de la population, est le Réseau Monétique Interbancaire (RMI) qui est sans cesse en développement et c'est la SATIM, qui en assure la bonne marche grâce à la connexion des DAB, et à son exploitation technique. Elle œuvre au développement et à l'utilisation des moyens de paiement électronique en toute sécurité.

**c) L'E- Banking** :

L'e-banking en Algérie a été l'œuvre d'une véritable évolution du secteur des finances en Algérie. Dans l'attente d'une mise en service de plateforme de paiement en ligne, deux des banque algériennes : La BADR (en 2004) et le CPA(2008), et récemment la BNA, ont proposé quelques uns de leurs services en ligne à travers le E-Banking. Désormais, les clients de ces banques peuvent consulter leurs comptes sans se rendre à leur agence bancaire. Selon la formule adoptée, l'usage du e-banking peut se matérialiser via quatre canaux. Il s'agit de l'internet, les messages au cellulaire (sms), le fax et enfin le téléphone.

La souscription à ces services est conditionnée par la signature d'un contrat. Dans une première phase, le service e-banking se limite à la consultation du solde du compte et le suivi des opérations comme les virements et les retraits. Il est également possible d'imprimer les relevés de compte et procéder à l'identification d'une transaction précise. L'abonnement à ce service est symbolique. Il est à raison de 100DA par mois et par compte pour les clients particuliers et à 800 DA pour les clients professionnels avec les mêmes conditions. Quant aux SMS et FAX, il est proposé de les recevoir par mois à la date souhaitée par le particulier

concerné. Ce service est facturé au même tarif pour les entreprises mais à raison d'une fois par semaine. La tarification est de 50 DA par mois et par compte pour les SMS et 200 DA par mois et par compte pour le FAX[60].

Pour le moment, la **CPA** est à sa première phase dans l'e-banking, il ne propose que la consultation des comptes à distance. Le service e-banking de la **BADR**[61], destiné aux particuliers et aux professionnels, le service en ligne vous permet de :

- ✓ Gérer l'ensemble de vos comptes depuis votre ordinateur, 7 jours/7, 24h/24, et aussi souvent que vous le souhaitez ;
- ✓ Consulter toutes vos opérations : historique sur 30 jours ;
- ✓ Effectuer une recherche et trouver l'opération qui vous intéresse ;
- ✓ Effectuer l'abonnement en ligne ;
- ✓ Télécharger vos relevés aux formats Excel, PDF ou CSV ;
- ✓ Créer des fusions de soldes si vous êtes un professionnel ;
- ✓ Consulter le cours des Devises ;
- ✓ Recevoir des messages personnels en provenance de votre Banque.

Malheureusement, dans l'e-banking, les banques algériennes accusent un retard, par rapport aux services que propose par exemple la **BNP Paribas** en ligne, cette dernière permet :

- Un accès illimité et gratuit : le site est accessible 24/24, sans abonnement et sans frais de connexion (hors coût du fournisseur d'accès Internet).
- Des virements unitaires gratuits entre vos comptes consultables sur BNPPARIBAS.NET. La création gratuite de virements permanents. Pour les moins de 25 ans, tous les virements sont gratuits.
- La possibilité de commander des chéquiers et d'éditer des RIB en ligne.
- Une utilisation simple : en quelques clics, effectuer des opérations courantes
- Un accès sécurisé : réaliser ces opérations en toute sécurité grâce à un numéro client et un code secret.

## II- Cybercriminalité en Algérie

Le développement des nouvelles technologies a ouvert une brèche aux comportements illicites, la cybercriminalité en plein boom, l'escroquerie et l'arnaque deviennent massives, le tableau suivant nous résume en type et en nombre les infractions cybercriminels en Algérie.

[60] A. Naima, « Automatisation du secteur bancaire et sécurisation des transactions : de la monnaie fiduciaire à la monnaie électronique », INSAG, Ingénieur commercial, 2010, page 107. Voir le lien : http://www.memoironline.com/10/12/6337/Automatisation-du-secteur-bancaire -et-securisation-des transactions-de-la-monnaie-fiduciaire--la.html

[61] Au travers de son site : **http://ebanking.badr.dz/fr/**

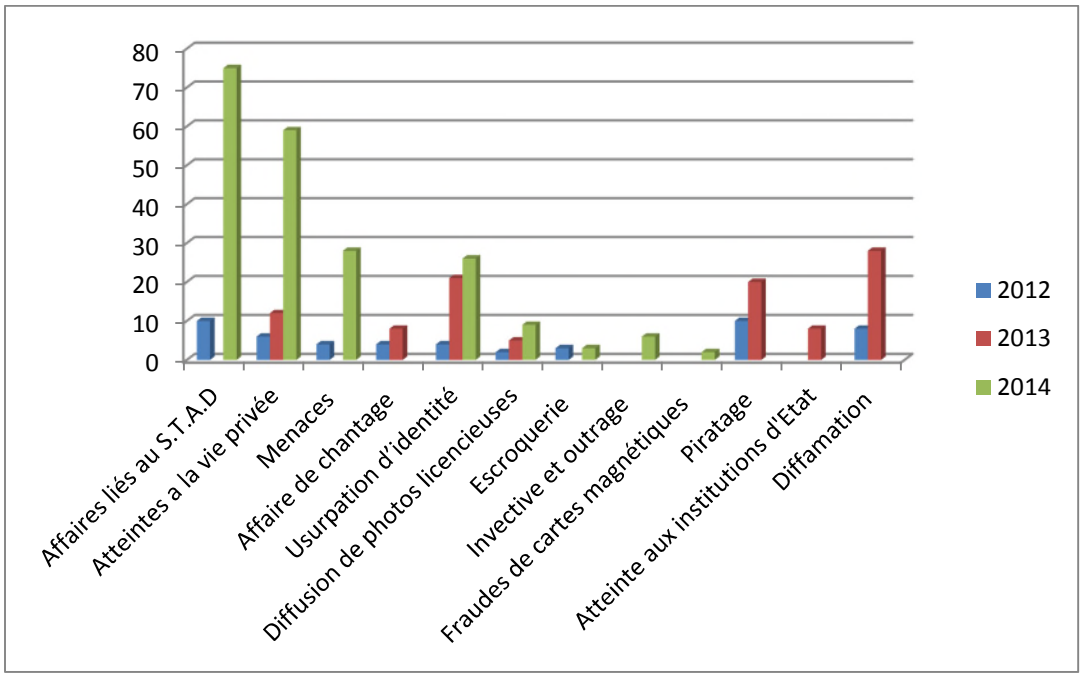
**Tableau n°21** : Evolution des infractions cybercriminels entre 2011-2014

| Années | 2012 | 2013 | 2014 |
|---|---|---|---|
| Affaires liés au système de traitement automatique de données (S.T.A.D) | 10 | | 75 |
| Atteintes à la vie privée | 6 | 12 | 59 |
| Menaces | 4 | | 28 |
| Affaire de chantage | 4 | 8 | |
| Usurpation d'identité | 4 | 21 | 26 |
| Diffusion de photos licencieuses | 2 | 5 | 9 |
| Escroquerie (via Internet) | 3 | | 3 |
| Invective et outrage (via Internet) | | | 6 |
| Utilisation illégale de cartes magnétiques | | | 2 |
| Piratage | 10 | 20 | |
| Atteinte aux institutions de l'Etat | | 8 | |
| Diffamation | 8 | 28 | |
| **Total** | **51** | **102** | **208** |

Source : Etablie a partir des données de la DGSN (direction général de la sureté national)

L'analyse de l'évolution de chaque infraction à travers trois années consécutives 2012, 2013, 2014 est représentée dans la figure qui suit :

**Figure n°10**: Evolution des infractions cybercriminelles en Algérie




Source : Rapport DGSN

On recense 51 infractions cybercriminels en 2012 et 208 en 2014. Le chiffre a quadruplé en deux ans. Les principales menaces enregistrées en 2014, sont : les atteintes au STAD, à la vie privée menace via Internet et l'usurpation d'identité. L'Algérie ne connait pas une grande criminalité technologique par rapport a d'autre pays, et on est loin des pirateries et fraude de carte bancaires et comptes postaux, même s'il a été révélé récemment qu'un groupe de malfaiteurs aurait réussi à obtenir les codes et les numéros de cartes de clients par un procédé qui consistait à placer des micro-caméras afin d'enregistrer le code et le numéro des cartes lors de l'utilisation de ces machines. A partir de ces informations récoltées, ils ont fabriqué des puces et ont ainsi vidé les comptes des clients ciblés à partir d'autres wilayas[62]. Certes, nos services électroniques ne sont pas assez développés ou quasiment inexistants (comme le e-commerce, le e-santé ou le e-administration). Néanmoins, cela ne doit pas empêcher l'Algérie de se doter d'outils pour se prémunir une fois la technologie introduite car ça reste un phénomène inévitable.

**II-1- Les cyber-attaques contre l'Algérie**

Des institutions algériennes ont été victimes de plusieurs cyber-attaques dont les responsables sont des hackers aux motivations politiques. D'autres attaques plus sophistiquées, ayant pour

[62] Nordine Douici, « l'alerte est donnée au niveau national, des cartes bancaires piratées à Béjaia », el Watan, le 30.05.2015.

but l'espionnage, et qui émane de nations qui ont ciblé notre pays (comme les Etats-Unis). Des compagnies comme *Microsoft*, *Kaspersky*, *The Norman Malware Cleaner*, *Trendmicro*, *Seculert*, *Lookout* et le rapport de septembre 2014 de *l'Europol*, confirment l'appréhension quant à l'état du cyber espace en Algérie. Du troisième trimestre 2013 au deuxième trimestre 2014, l'Algérie est passé de la 8ème place à la 3ème place des pays les plus infectés dans le monde. Avec un pourcentage de 52,05%[63].

**Tableau n° 22:** Les pays avec le plus haut risque d'infection

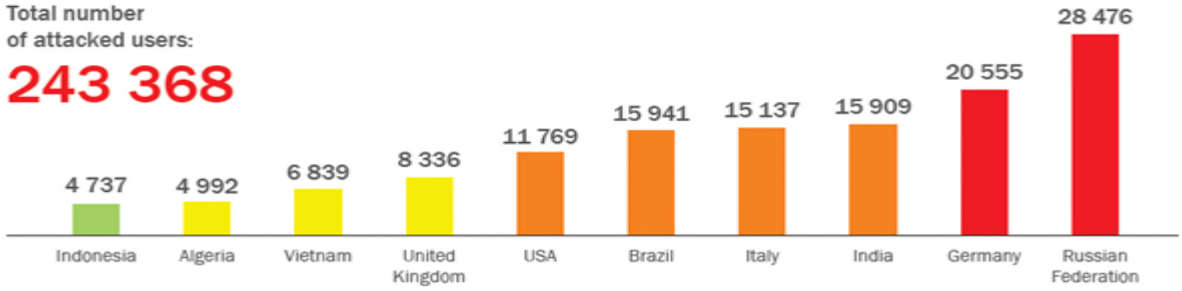
| | Pays | Pourcentage |
|---|---|---|
| 1 | Vietnam | 58,42% |
| 2 | Mongolie | 55,02% |
| 3 | Algérie | 52,05% |
| 4 | Yémen | 51,65% |
| 5 | Bangladesh | 51,12% |
| 6 | Pakistan | 50,69% |
| 7 | Népal | 50,36% |
| 8 | Afghanistan | 50,06% |
| 9 | Irak | 49,92% |
| 10 | Egypte | 49,59% |

Source : www.ssri.dz

Le secteur financier algérien ne semble pas échapper et est victime de ce phénomène au moment où il fait justement des efforts pour rattraper son retard afin de se moderniser et s'ouvrir plus. Durant le mois de septembre 2014, les utilisateurs ci-dessus figurent parmi les plus ciblés dans le monde par les cyber-attaques, dont l'Algérie avec 4992 attaques recensées.

[63] Les informations bien en détail cité dans le lien suivant : http://www.ssri.dz/la-cyber-securite-etat-des-lieux-en-algerie/

**Figure n°** 11: Le nombre d'attaques cybercriminels en 2014.




Source : www.ssri.dz

L'Algérie est victime de, plus de 4000 attaques en ce qui concerne l'année 2014. Parmi ces attaques on recense des cas de piratage de sites de journaux tel « Le quotidien d'Oran » et le « Tous sur l'Algérie (TSA) », des intrusions dans les fichiers de la Banque d'Algérie et des Douanes nationales (à Oum El bouaghi), d'autres attaques relatives au vol informations, d'atteinte à la vie privée et bien d'autres. Comme cité dans la figure n°11, ci-dessus.

### II-2-les Institution chargées de la réglementation

Des institutions sont chargé de la réglementation numérique et du système d'informations, leur objectifs se définis dans la prospérité du secteur des Tic mais également a maintenir un contrôle et une surveillance en son sein. Parmi elles on site :

**Tableau n°** 23: Entités Algériennes de réglementation

| Institutions | Présentation et mission |
|---|---|
| ARPT | L'Autorité de régulation de la poste et des Télécommunications, Accès aux réseaux large bande et Radiodiffusion. Veille à la protection du consommateur à la sécurité informatique et a la certification électronique, analyse les différents outils et logiciels de sécurité (en cryptographie), tire le meilleur partie de son système d'information dont les systèmes de pilotage et de production |
| MPCIT | Ministère chargé de la poste et des technologies de l'information et de la communication. Autorité gouvernementale qui est responsable des initiatives politiques liées au secteur des TIC en Algérie. Il est chargé du suivi et du contrôle de l'activité de liés aux TIC et à la poste. Autorité de cybersécurité. Depuis peu, elle contrôle la signature et la certification électronique (loi 15-04 du 1 février 2015). |
| CERIST | Régulateur national responsable des contenus numériques et centre de recherche sur l'information scientifique et technique. Le centre a pu s'ouvrir et développer des solutions à |

| | |
|---|---|
| | certains problèmes relatifs à la société de l'information et par la même favoriser sa promotion. |
| TDA[64] | Régulateur national de la Radiodiffusion numérique, chargé de la gestion de l'émission et de la diffusion par voie de terre et par satellite les programmes de radio et Télévision. |
| | Cellule de traitement du renseignement financier est un organe spécialisé, indépendant, chargé de recueillir, de traiter, d'analyser et d'échanger avec les organismes homologues étrangers des renseignements financiers dans le but de contribuer à la détection, prévention et la dissuasion du recyclage de fonds et de financement des activités terroristes en Algérie. Elle mobilise quatre services : Le service Enquêtes et Analyses ; le service documentation et bases de données ; le service de la coopération ; le service juridique. |

Source : Elaboré par nous même sur la base des données des sites : www.mf-ctrf.gov.dz; www.**arpt**.dz; www.cerist.dz; www.mptic.dz .

### III- La mise à niveau du cadre juridique national : *cause ou conséquence*

Avec les nouvelles formes de criminalité qui sont apparues et ont évolué dans le cyber espace, l'Algérie se devait de se doter d'un arsenal juridique et d'adopter des lois spécifiques relatives à la prévention et à la lutte contre les infractions liées aux TIC, il y'eu d'abord la loi n° 04-15 du 10 novembre 2004 qui venu apporté les premiers articles de lutte contre ces nouvelles infractions puis la loi n° 06-23 du 20 décembre 2006 venu compléter celle de 2004 en modifiant et complétant le code pénal. En plus de la loi de 2009 et celle de 2014. Un tableau résume par type d'infraction et les incriminations dans le code pénal algérien voir dans l'annexe n°2.

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[65]. En plus du cadre juridique, duquel elle s'est dotée, l'Algérie doit contourner le phénomène de cybercriminalité et se lancer dans la confiance numérique et la protection des données personnelles[66] **:** a l'instar des autres pays du Maghreb, l'Algérie dispose d'une politique publique pour la confiance numérique. Cette politique est basée principalement sur la mise en place d'un dispositif juridique de protection contre la cybercriminalité et les

[64] TDA : Télédiffusion Algérie
[65]Ali El AZZOUZI, « la cybercriminalité au Maroc », édition Ali el AZZOUZI, Casablanca, 2010, page 103.
[66]Rachid JANKARI, « Les technologies de l'information au Maroc, en Algérie et en Tunisie », vers une filière euromaghrébine des TIC ? », Consultant à l'Institut de Prospérité Economique du Monde Méditerranéen, Etudes & Analyse, vers une filière euromaghrébine des TIC, Octobre 2014, page 19, 20.

infractions qui touchent les systèmes d'information. En 2004, le pays a adopte une série de mesures pour lutter contre la cybercriminalité. Il s'agit de :

• la promulgation de la **loi 04-15 du 10 novembre 2004** relative aux atteintes des systèmes de traitement automatise de données (STAD) ;

• l'installation du Centre de lutte et de prévention contre la cybercriminalité de la gendarmerie nationale ainsi que la mise en place d'autres laboratoires spécialises et des brigades spécialisées de la direction de la sûreté nationale. **La loi 09-04 du 5 aout 2009** relative à la prévention et à la lutte contre les infractions liées aux TIC est un autre texte fondateur dans le domaine de la confiance numérique. Elle concerne les infractions portant atteinte au système de traitement automatise de données telles que définies par le code pénal ainsi que toute autre infraction commise ou dont l'exécution est facilitée par un système informatique ou un système de communication électronique. Cette loi prévoit d'ailleurs la possibilité d'effectuer des opérations de surveillance des communications électroniques et la perquisition des systèmes informatiques dans le cas de la protection de l'ordre public et les besoins d'enquêtes ou d'informations judiciaires en cours. Dernièrement la loi n°15-04 du 1er Février 2015 relative à la signature et à la certification électronique, voir l'annexe n°1.

**Conclusion** :

L'Algérie ne prend pas conscience des conséquences que pourrait engendrer la cybercriminalité, il est extrêmement important pour un pays d'envisager les différents scénarios lui permettant d'assurer la continuité des services critiques. Notre pays, n'y échappera pas et c'est dans cette perspective, que le développement d'outils de sécurité ont été identifiés en incitant d'abord à la prévention et à la promotion d'une culture de sécurité, en plus d' un renforcement des droits du cyber-utilisateurs devant offrir une sécurité juridique déterminante. Dans le cadre de la prévention et de la promotion de la culture de la confiance numérique, le ministère de l'Enseignement supérieur et la Recherche à lancer un portail *www.wikayanet.dz* dédié à la diffusion de l'information auprès du grand public et des professionnels sur la cybersécurité. Il fournit des informations et des alertes sur les virus informatiques et les menaces relatives aux systèmes d'information.

Pour étudier de plus prés ce phénomène nous avons procéder à une analyse par questionnaire au niveau des banques dans la section 02.

## Section 2 : Evaluation des banques Algériennes face au phénomène de cybercriminalité : Etude et analyse par questionnaire

Les mises à jour du système bancaire en termes de TIC que se soit au niveau du système d'information, qu'au niveau du système de paiement, ils ont pour objectif de moderniser les outils et les infrastructures bancaires et cela a été suivi de l'apparition de risques numériques aussi bien internes qu'externes rassemblés sous le concept de cybercriminalité. Cette section comprendra des éléments méthodologiques relatifs à la présentation du questionnaire puis il sera question d'une analyse des résultats de l'enquête.

### I- Méthodologie et présentation de l'enquête

Pour évaluer son effet sur le système bancaire et la part de ce dernier dans la sécurité et la contra attaque, nous avons mené une enquête du mois d'Avril au mois de Juin 2015, dans le cadre d'un travail de recherche, le questionnaire est divisé en quatre (4) parties. La première partie intitulé « questions relatives aux technologies de l'information et de la communication de la banque », qui nous permet de saisir le degré d'introduction des Tic et son impact sur les banques. La deuxième partie qui s'intitule « questions relatives aux moyens de paiement », se penche sur la situation de la monétique. La troisième partie qui s'intitule « questions relatives au système d'informatique », nous permet l'évaluation de leur degré d'informatisation. Enfin, La quatrième partie s'intitulant « questions relatives aux risques numériques et à la sécurité informatique », s'intéresse aux risques auxquels fait face la banque et aux efforts déployés, aux outils et dispositifs utilisés pour y faire face et les gérer.

### II- Analyse et interprétation des résultats de l'enquête :

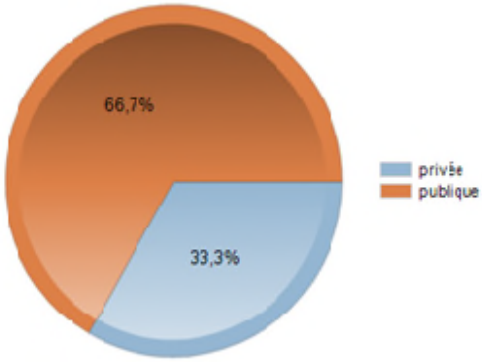
L'analyse des résultats de ce questionnaire nous a révélé l'*importance de l'impact sur l'usage des TIC ; le développement insuffisant de la monétique ; un système de sécurité centralisé pas assez présent*. Par ailleurs il est a noté que certaines questions n'ont pas eu de réponses, nous allons donc nous contenter d'analyser et de conclure en fonction des banques qui ont répondues. Sur un échantillon bien choisi, notre questionnaire (voir annexe n°7) n'a été accepté que par neuf (9) banques. Le traitement statistique des réponses a été effectué grâce au logiciel **Sphinx IQ**, en plus de l'analyse des questions ouvertes qui sera enrichi des entretien tenu auprès des différents responsables, une diversité d' informations que nous essayerons d'étayer dans cette présente section.

**Tableau n° 24**: Echantillon de banque répondant au questionnaire

| Dénomination sociale de la banque | Banques répondantes |
|---|---|
| BNA | OUI |
| BEA | OUI |
| BDL | NON |
| CPA | OUI |
| BADR | OUI |
| CNEP-Banque | OUI |
| EL Baraka | NON |
| BNP-Paribas | NON |
| CITY Bank | NON |
| NATIXIS Bank | OUI |
| CAB | NON |
| EL Rayan Bank | NON |
| BMG | NON |
| ABC Bank | OUI |
| Société Générale Algérie | OUI |
| Arab Bank PLC | NON |
| Trust Bank | OUI |
| Acro Bank | NON |
| Algeria Golf Bank | NON |
| Housing bank | NON |
| **Total** | **9/ 20** |

Source : Etablit par nous-mêmes.

**Figure n°12** : Répartition par Statut Social

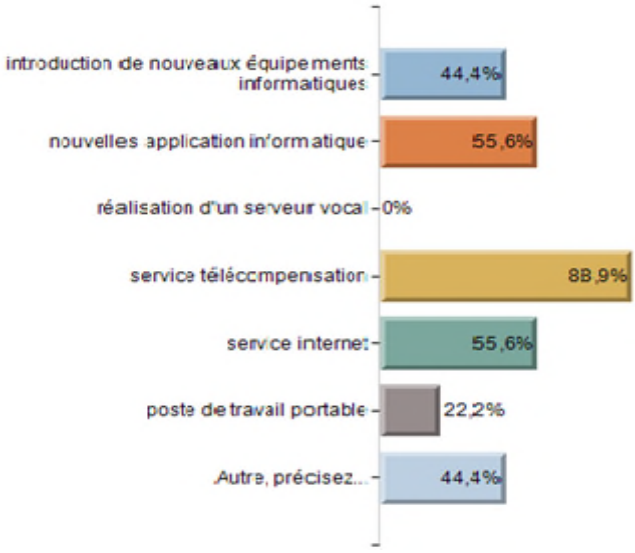



Source : notre enquête

Comme le montre le tableau ci-dessus, le nombre de réponse n'a été que de neuf (9) sur un total de 20 banques. Elles sont réparties à 66,7% Publiques et à 33,3% Privées, ce qui fait trois (3) banques privées et six (6) banques publiques de notre échantillon répondant. Comme le démontre la figure n°12.

**II-1- Importance de l'impact de l'usage des Tic :** Les banques intègrent sans cesse de nouvelles technologies d'informations et de communication dans leur système et dans leurs fonctions. Le tableau ci-dessous nous démontre parmi les modalités citées lesquels sont intégrées dans leur système.

**Figure n° 13**: Les TIC dans les banques Algériennes




Parmi les services introduit, 88,9% c'est le service télécompensation, ce qui fait huit (8) banque sur neuf (9), viennent après les applications informatiques, tel le SGBD ; le système client serveur et le service Internet, avec 55,6% (c.à.d. Cinq banques sur neuf), et quatre banques sur neuf ont introduit de nouveaux équipements informatiques (ce qui fait 44,4%), le reste dont 22,2% dispose de poste de travail portables (deux banques

Source : établit à partir du logiciel sphinx IQ

sur neuf). Les Autres technologies proposées par les banques sont représentées comme suit : un système de gestion des opérations bancaires (concernant l'ABC Bank) ; une nouvelle organisation commerciale des agences (CNEP-Banque) ; une clé de stockage de données permettant la continuité de l'activité dans le cas de l'inaccessibilité au site (Natixis). Les Tic présentent un impact sur la productivité qui est à une échelle très importante pour la banque, mais également sur le mode interne de travail. Les réponses a cette dernières ont été les suivantes :

**Tableau n°25** : impact sur le mode interne du travail

| | Nb | % obs. |
|---|---|---|
| rapidité et fiabilité | 9 | 100,0% |
| amélioration, efficacité et précision | 8 | 88,9% |
| réduction des contraintes | 3 | 33,3% |
| réduction du risque | 6 | 66,7% |
| suppression des taches | 4 | 44,4% |
| Autre, précisez... | 1 | 11,1% |
| **Total** | 9 | |

Source : notre enquête

La majorité des réponses des banques déterminent que l'impact des Tic réside dans la rapidité et la fiabilité des opérations, l'efficacité et la précision et enfin dans la réduction du risque. Ainsi grâce aux technologies de l'information les banques peuvent effectuer plusieurs

opérations par jour et le temps moyen pour le traitement est rapide et efficace comme va le démontré le tableau suivant :

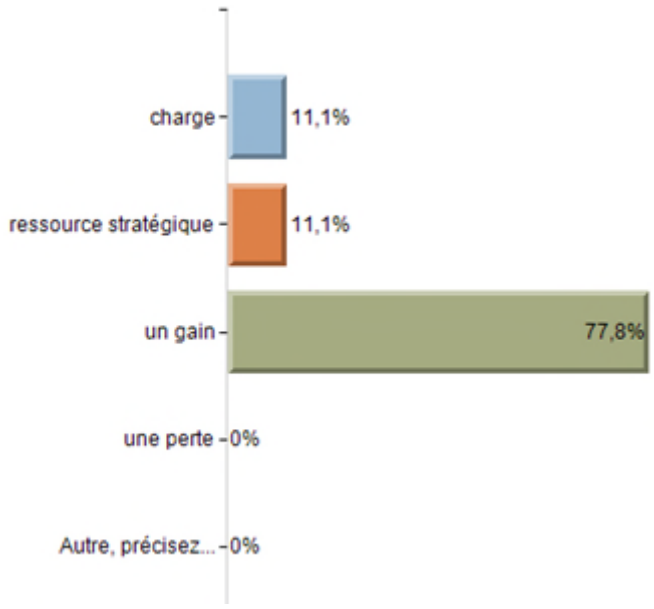
**Tableau n°** 26: le nombre d'opérations par jour et le temps moyen consacré au traitement

| | ABC | BADR | BEA | BNA | CNEP | CPA | NATIXIS | SGA | TRUST |
|---|---|---|---|---|---|---|---|---|---|
| Nbr opérations /jr | 20 | 200 | 2000 | 500 | - | 200 | 160 | 30 | - |
| Temps moyen (min) | 2 | 1 | 10 | 2 | 2 | 2 | 2 | 2 | - |

Source : notre enquête

Les banques publiques enregistrent un nombre important d'opérations effectuées par jour et en majorité le temps consacré au traitement ne dépasse pas les 2 minutes excepté pour la BEA qui prend 10 minutes.

**Figure n°14**: Importance des Tic




Le point de vue des banques au sujet des Tic a été déterminé comme étant globalement une source de gain à 77,8%, ce qui représente sept (7) banques sur neuf, et a 11,1% comme étant une charge et cela s'explique par l'investissement qui suit son installation dans l'entretien et la maintenance du matériel, comme dans la formation des employés pour s'adapter aux Tic et à la maitrise des outils.

Source : notre enquête

L'avènement d'Internet a bousculé les stratégies des banques, néanmoins cette technologie n'est pas suffisamment exploitée. Malgré l'absence d'information, les banques estiment être connectées au réseau. Le tableau ci-dessous, nous montre les premières connexions Internet des banques :

**Tableau n°** 27: Les connexions Internet

| Dénomination | ABC | BADR | BEA | BNA | CNEP | CPA | NATIXIS | SGA | TRUST |
|---|---|---|---|---|---|---|---|---|---|
| Connexion Internet | 2001 | 2013 | - | - | - | - | 2006 | 2008 | 2002 |

Source : notre enquête

La connexion entre agences s'effectue donc par voie d'ADSL à 33,3% comme le montre le tableau suivant:

**Tableau n° 28**: connexion dans les agences

| | Nb | % obs. |
|---|---|---|
| ligne téléphonique simple | 1 | 11,1% |
| ligne téléphonique numérique | 0 | 0,0% |
| cable de télédistribution | 0 | 0,0% |
| adsl | 3 | 33,3% |
| Autre, précisez... | 6 | 66,7% |
| **Total** | 9 | |

Source : notre enquête

Pour ceux qui disposent d'une connexion Internet, ce canal est exploité pour les modalités suivantes :

**Tableau n° 29**: utilisation d'Internet

| | Nb | % obs. |
|---|---|---|
| téléchargement de fichier | 3 | 33,3% |
| telechargement de logiciel | 2 | 22,2% |
| recherche d'information | 7 | 77,8% |
| consultation de mail | 7 | 77,8% |
| echange de fichiers avec les clients | 5 | 55,6% |
| diminution des couts | 3 | 33,3% |
| présentation de la banque | 4 | 44,4% |
| Autre, précisez... | 2 | 22,2% |
| **Total** | 9 | |

Source : notre enquête

Mais d'après nos entretiens, certaines banques ne sont pas connecté a Internet comme la CNEP et la CPA qui usent de l'intranet estimant que c'est pour assurer la sécurité des données de la banque, même réponse pour la Trust Bank, les agences ne sont pas connecté a Internet par mesure de sécurité ils communique par voie de ligne spéciale en plus du WiMax (il s'agit d'un standard de réseau sans fil, il fourni une connexion à haut débit. Elle fourni un accès haut débit aux zones non couvertes par les technologies filaires classiques comme les lignes ADSL ou ligne spécialisé T1). Un système de ligne satellite utilisé par Société Générale et Natixis.

Pour le tableau n°30, l'utilisation d'Internet est surtout pour la recherche d'information et la consultation des mails. Concernant la rubrique Autre de 22,2%, on cite 11,1% qui utilisent Internet pour le système EDI (Echange de Données Informatisées) dans le traitement des ordres de salaires par exemple. Les 11, 1% restant utilisent Intranet.

Pour la plupart de ces banques, les lignes de connexion introduites ce sont faites au travers de partenariats avec des opérateurs téléphoniques ou Algérie Télécom à défaut des technologies de communication :

**Tableau n°30** : Partenariat avec un opérateur téléphonique ou Algérie Télécom

| | Nb | % cit. |
|---|---|---|
| oui | 5 | 55,6% |
| non | 4 | 44,4% |
| Total | 9 | 100,0% |

Source : notre enquête

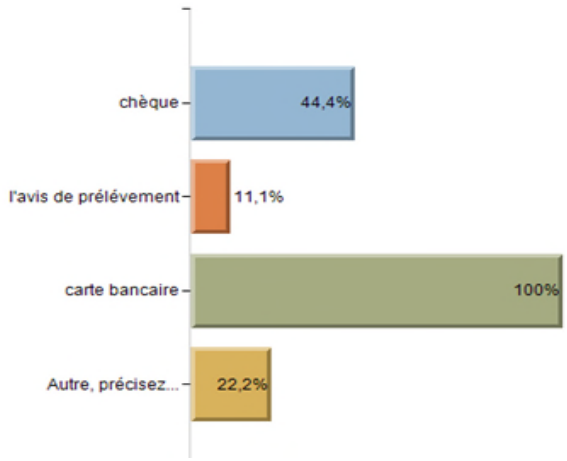
On remarque seulement cinq banques sur neuf (NATIXIS, Trust Bank, BNA, ABC) affirment avoir collaboré avec Algérie Télécom pour l'introduction de ligne ADSL, ou ligne spéciale de connexion ou juste pour les systèmes d'alarmes, d'appels. A l'exception de Société Générale où le partenariat s'est fait avec l'opérateur « DJEZZY » et pour NATIXIS (en plus d'Algérie Télécom) elle collabore avec France Télécom.

Les technologies de l'information et de communication détiennent une grande place au niveau des banques, considéré comme une source de gain, dans la rapidité et la fiabilité des opérations, dans la réduction des risques et pour la concurrence, même si leur exploitation n'est pas assez suffisante surtout en ce qui concerne certains canaux stratégiques comme celui d'Internet qui reste un atout incontournable pour les banques algériennes.

### II-2- Développement insuffisant de la monétique

La prise en charge de la monétique s'est concrétisée avec la mise en place de la SATIM « Société d'Automatisation des Transactions Interbancaires et de Monétique », en mars 1995, elle a été crée pour contribuer au développement de la monétique en Algérie même si l'utilisation de certain instruments comme la carte de retrait ne constitue pas un fait nouveau vu qu'elle a été introduite en Algérie en 1989, et en 1990 quelques banques comme la BEA, CPA, BNA disposaient déjà de carte bancaire. Parmi les moyens de paiements les plus automatisé les banques répondent a 100% pour la carte bancaire.

**Figure n° 15:** Moyens paiement plus automatisé




En 2006 une nouvelle forme de carte bancaire a été mise au point qui est la CIB (Carte Inter Bancaire), en plus des autres types de carte que chaque banque propose à ses clients.

Source : notre enquête par sphinx IQ

Dans le tableau ci-dessous, on résumera la date de mise en circulation de la carte bancaire avant et après la création de la SATIM, en plus des différents types de cartes proposées par chacune.

**Tableau n°** 31: Système de carte bancaire (date et type)

| | ABC | BARD | BEA | BNA | CNEP | CPA | NATIXIS | SG | TRUST |
|---|---|---|---|---|---|---|---|---|---|
| Carte bancaire avant la SATIM | - | 1994 | 1989 | 1989 | - | 1989 | - | - | - |
| Carte CIB | 2006 | 2000 | | 2004 | - | 2000 | 2006 | 2010 | 2006 |
| Autres types de cartes | | Carte CRB ; carte BADR TAWFIR ; Carte de crédit (2011) | carte carburant ; Master Card (prochaine ment) | Carte Visa Internati onal | Carte d'épargne | | | | Master card (2014) |

Source : notre enquête

Le tableau nous fait remarqué la disponibilité de la carte CIB auprès des banques, elle a pour fonction le retrait et le paiement mais elle ne fait fonction de retrait vu l'inexistence de GAB et le nombre moindre de TPE disponibles. Pour que les titulaires de cartes bancaires puissent

bénéficier de la totalité des services proposées par ces dernières, les banques doivent coordonner ce développement avec d'autres acteurs tel les commerçants, …etc.

**Tableau n°** 32: Nombre de DAB

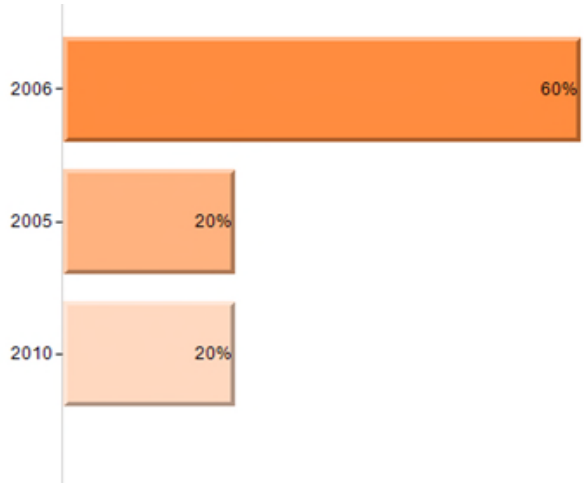
| | ABC | BARD | BEA | BNA | CNEP | CPA | NATIXIS | SOCIETE GENERALE | TRUST Bank |
|---|---|---|---|---|---|---|---|---|---|
| Nombre d'agences | 24 | 300 | 150 | 205 | 209 | 154 | 26 | 70 | 14 |
| Nombre de DAB | 24 | 121 | - | - | 209 | 100 | 26 | 70 | 14 |

Source : notre enquête

Le développement des DAB est faible comme le montre le tableau ci-dessus, pour les banques privées il y'a un DAB pour chaque agence. Et concernant les GAB (guichet automatique bancaires), ils sont quasiment inexistant, on retrouve quelques banques qui en dispose comme la BNA qui l'a introduit récemment, ils affichent de nouvelles fonctionnalités, à savoir la remise de chèques et le versement d'espèce.

Concernant l'automatisation de chèque précédemment évalué dans la figure n°, à 44,4%, elle s'est faite en 2006, et la majorité l'an introduite a cette date excepté certaine la figure suivante nous montre le pourcentage d'introduction en trois (3) années distinctes comme cité dans les réponses des neuf banques, 2005, 2006, 2010.

**Figure n°16**: date d'automatisation du chèque




Source : notre enquête par le logiciel sphinx IQ

Malgré les multiples réformes adoptées, et qui ont pour but de dématérialiser le système de paiement, le développement de la monétique reste insuffisant et cela pourrait s'expliquer par le manque de confiance des particuliers dans ces instruments et cela doit être l'une des

fonctions de la banque inclut dans sa démarche marketing de prévenir, d'inciter et de mettre en confiance les clients en leurs charge.

### II-3- Un système de sécurité centralisé et pas assez présent.

Un bon système de sécurité passe par un développement du système informatique, car ce dernier nous permet une bonne gestion de l'information qui devient de plus en plus automatisé. Dans ce dernier axe nous verrons les outils, dispositifs et les services prêt a affronter les risques inhérents du numériques et a les gérer.

a) Le système informatique

Le SI est développé à 100%, c'est-à-dire que toutes les banques ont investie dans le développement de celui-ci. Selon les réponses des banques, la stratégie de développement du SI a été effectuée sous quelques critères que nous avant déterminé et que les banques, selon leur choix, ont cité :

**Tableau n°** 33: Pourquoi développer le système informatique

| | Nb | % obs. |
|---|---|---|
| realisation d'economie d'echelle | 2 | 22,2% |
| assurer une plus large diffusion des produits | 4 | 44,4% |
| modernisation | 7 | 77,8% |
| Autre, précisez... | 2 | 22,2% |
| **Total** | 9 | |

Source : notre enquête

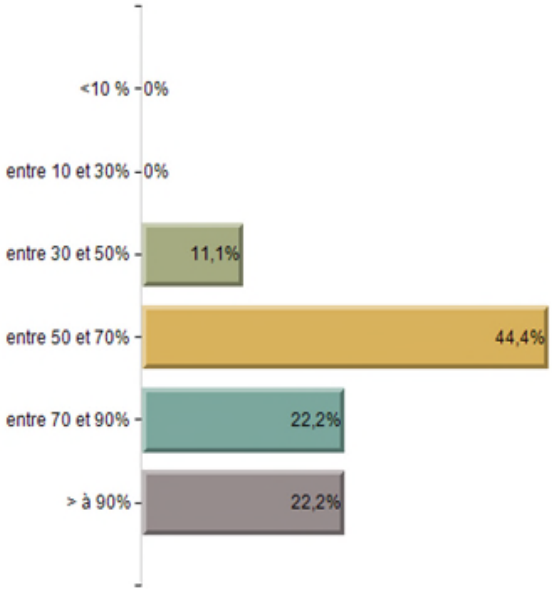
D'autres banques ont ajouté le critère de sécurité comme étant un facteur primordial qui les a orientés vers le développement du SI. Les banques ont connu alors un processus d'informatisation à 55,6% graduel à vitesse plutôt moyenne, ce qui fait 5/9 banques.

**Tableau n°34** : Processus d'informatisation

| | nombre | % d'observations |
|---|---|---|
| Graduel et rapide | 3 | 33,3% |
| Graduel à vitesse plutôt moyenne | 5 | 55,6% |
| Graduel mais lent | 1 | 11,1% |
| Total | 9 | 100,0% |

Source : notre enquête

**Figure n°17**: Taux d'informatisation des banques



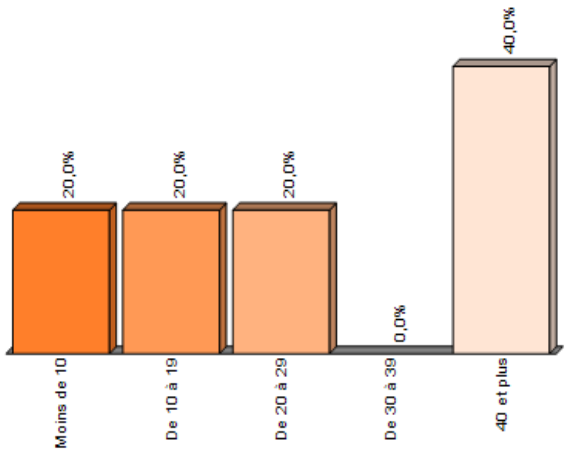

L'estimation en pourcentage de l'informatisation au niveau des neuf banques interrogées, est fréquente selon trois (3) modalités :

- Entre 50 et 70% (pour CNEP, BADR, ABC, NATIXIS) ;
- Entre 70 et 90% (pour la BNA, Société Générale) ;
- >à 90% (pour Trust Bank, CPA).

Source : notre enquête

**Figure n° 18**: Budget de l'informatisation (%)

Le budget consacré à l'informatisation varie d'une banque a une autres mais cette question jugée sensible n'a pas retenue de réponse, nous avons donc proposé de donner une estimation annuel pour les dépenses investit dans l'informatisation, comme affiché sur la figure n°18.




Source : notre enquête

Un Total de réponse de cinq (5) banque sur neuf (9), le budget annuel destiné a l'informatisation (en équipements et logiciels) se répartit comme suit :

-BADR : 3% de son budget total est investit dans l'informatisation ;

- BNA : investit 20% du budget total dans l'informatisation

- ABC Bank: le budget varie de 30 à 50% ;

- Société Générale : avec 60% de son budget total.

Avec un taux de réponses des banques égales a 88,89%. Les dépenses informatiques ont enregistré un taux de croissance annuel plutôt en hausse pour 87,5% soit 7 banques sur 9. Et 12,5% en baisse pour une banque (Trust Bank qui juge être assez bien équipé pour freiner ses dépenses). Après avoir reçu les pourcentages du budget liés a l'informatisation nous allons examiner si la performance et le contrôle du système informatique, ils y sont a leur niveau, les banques affirment suivre de prés la performance de leur système, Le contrôle de la performance du SI s'effectue selon les modalités citées dans le tableau suivant.

**Tableau n° 35**: déroulement du contrôle du système

| | Nb | % obs. |
|---|---|---|
| annuellement | 0 | 0,0% |
| semestriellement | 0 | 0,0% |
| trimestriellement | 0 | 0,0% |
| mensuellement | 6 | 66,7% |
| Autre, précisez... | 3 | 33,3% |
| **Total** | **9** | **100,0%** |

Source : notre enquête par Sphinx IQ

On note 66,7% des banques effectue un contrôle mensuel à leur système et expliquent que le contrôle est effectué au niveau de la Direction Générale avec le système help DESK (selon Trust Bank) qui est :

Un centre d'assistance ou « hotline », c'est un service qui est chargé de répondre aux demandes d'assistance émanant des utilisateurs. Ceux-ci entrent en contact avec le help desk dans le but de trouver une réponse à un problème technique informatique, tant logiciel que matériel. Les utilisateurs peuvent joindre le centre d'assistance :

- ✓ par email ;
- ✓ par téléphone ;
- ✓ sur le site Internet de l'entreprise. L'utilisateur peut résoudre lui-même son problème via des documents et notices. On parle alors de mode libre-service.

Les banques disposent de deux directions nationales de contrôle (selon la CPA) au niveau de la BA (Banque d'Algérie) :

-la direction du traitement informatique ;

-la direction des études et réalisation informatique ;

Pour les 33,3% qui précisent que le déroulement au niveau du contrôle est suivi au jour le jour, des visites préventives, contrôle aléatoire ou occasionnel.

Pour savoir si les banques sécurisent assez bien leur réseau nous avons procéder a un entretien des responsables, ainsi selon les réponses récoltées : -la Direction Générale (DG) contrôle le

système ; -Avec le système help Desk la direction générale contrôle et suivie la banque ;-pour certaines c'est l'utilisation d'Intranet qui leur confère la sécurité absolue ; -dispose de moyens nécessaire comme les logiciels et antivirus performants mis en place par la direction du traitement informatique en plus des programmes d'exploitation ;-les lecteurs CD et flash-disk sont inactifs sur les ordinateurs des employés (débranchés) ; -dispose d'un système d'alerte pour la détection de risque ou de menace.

Le nombre d'informaticien intervenant aux banques est présent au niveau des directions nationales et régionales par contre il est faible au niveau des agences, Le pourcentage d'informaticien dans l'effectif total de la banque :

**Tableau n° 36** : Pourcentage d'informaticien

| | ABC | BARD | BEA | BNA | CNEP | CPA | NATIXIS | SOCIETE GENERALE | TRUST Bank |
|---|---|---|---|---|---|---|---|---|---|
| Nbr d'informaticien / effectif total | 9% | 10% | | 2% | 30% | 2% | | | 3% |

Source : notre enquête

Pour la CNEP, le nombre d'informaticien représente une grande part dans l'effectif de la banque, cela prouve le degré d'investigation de la banque dans le contrôle du système et la sécurité. Contrairement à la BNA, CPA et la Trust Bank qui ne représente que 2% à 3% du total du personnel. Ils se répartissent comme suit :

**Tableau n° 37**: répartition du personnel informaticien

| | ABC | BARD | BEA | BNA | CNEP | CPA | NATIXIS | SGA | TRUST |
|---|---|---|---|---|---|---|---|---|---|
| Cadres | | 20% | - | 100% | 100% | 100% | 60% | - | - |
| Agents de maitrise | | 40% | - | - | - | - | 30% | - | - |
| Agents d'exécution | | 40% | - | - | - | - | 10% | - | - |

Source : notre enquête

Dans la majorité des banques, la plus grande part du personnel informaticien est représentée par des cadres. Pour la CNEP, BNA, CPA, les informaticiens sont à 100% des cadres.

Avec tous les critères ci-dessus qui nous ont démontré le bon équipage de la banque, une bonne mise au point du système informatique, et le personnel bien cadré et formé, nous allons d'abord analyser la situation de la banque concernant les infractions auxquels elle a pu faire face, des cas de piratage, de spam et des fraudes de carte bancaire pour ensuite indiquer

les dispositifs mis au point par les banques et même au niveau des agences pour y remédier, du moins les gérer.

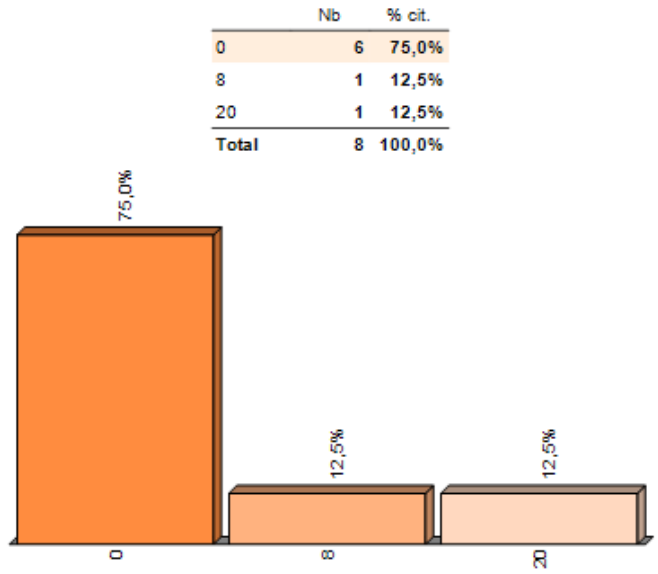
b) Les risques numériques :

**Tableau n°** 38: Les infractions liées au TIC

| | ABC | BADR | BEA | BNA | CNEP | CPA | SGA | NATIXIS | TRUST |
|---|---|---|---|---|---|---|---|---|---|
| Infractions (%) | 20% | 8% | - | - | - | - | 0% | - | 0% |

Source : établit par nous même

**Figure n° 19**: taux d'infraction liés aux TIC




Source : notre enquête sur le Sphinx IQ

Certaines banques sont plus atteintes par des infractions touchant aux technologies d'informations et de communication en leur sein, que d'autres. Avec un taux de réponse de 88,89%, c'est à dire six (6) banques sur neuf (9) jugent que le pourcentage est de 0%, contre 20% et de ABC pourcentage très élevé si on prend en considération le degré d'informatisation et de protection employé. Pour la BADR il est de 8%.

**Tableau n°** 39: Banques victime de piratage

| | ABC | BADR | BEA | BNA | CNEP | CPA | SGA | NATIXIS | TRUST |
|---|---|---|---|---|---|---|---|---|---|
| OUI | | | | | | | | | |
| NON | + | + | + | + | + | + | + | + | + |

Source : notre enquête

Les banques interrogées affirment ne pas avoir été victime cas de piratage. Concernant les infections informatiques, le tableau suivant nous montre quelle banque a déjà fait face à des cas de SPAM :

**Tableau n° 40:** banques **v**ictime de spamming

| | ABC | BADR | BEA | BNA | CNEP | CPA | SGA | NATIXIS | TRUST |
|---|---|---|---|---|---|---|---|---|---|
| OUI | | + | | | | | + | | |
| NON | + | | + | + | + | + | | + | + |

Source : notre enquête

Des plaintes ont été reçues par deux banques, de la part des clients, ayant été victime de spamming, La BADR et Société Générale. Le pourcentage estimé par la BADR est de 2%, et pour Société générale, il est de 1%.

Fraude de carte bancaire :

Les banques interrogées affirment ne jamais avoir fait face a ce type de délit cybercriminel, excepté la BADR qui déclare des cas de fraude de cartes bancaires et cas d'usurpation de numéros de cartes bancaires, estimé à 5% pour l'année actuelle.

Falsification de chèque :

Sur l'échantillon interrogé, six banques ont répondu oui au cas de falsification de chèque mais seulement trois d'entre elles ont estimé l'ampleur, Société Générale à 1% et la BADR à 2%, Trust Bank à hauteur de 5%, la CPA déclare avoir fait face a un seul (1) cas, et ABC à deux (2) cas.

**Tableau n°41** : Les falsifications de chèques

| | ABC | BADR | BEA | BNA | CNEP | CPA | SGA | NATIXIS | TRUST |
|---|---|---|---|---|---|---|---|---|---|
| OUI | + | + | | + | | + | + | | + |
| NON | | | | | + | | | + | |
| Estimation/an | | 2% | | | | | 1% | | 5% |

Source : notre enquête

Le dépouillement des résultats ont été traité par le logiciel Sphinx IQ, la falsification de chèque est l'infraction la plus répandue. Le tableau suivant nous démontre les résultats **:**

**Tableau n° 42**: résultat des cas portant sur la falsification de chèque

| | Nb | % cit. |
|---|---|---|
| oui | 6 | 75,0% |
| non | 2 | 25,0% |
| Total | 8 | 100,0% |

Source : notre enquête par le logiciel Sphinx IQ

c) Outils et procédures de sécurité :

Pour prendre connaissance de la protection et des efforts employé par la banque pour gérer ces risques nous avons la question suivante : - Les systèmes employés pour la sécurité sont ils suffisamment efficace ?

**Tableau n°43**: efficacité de la sécurité du système

| | Nb | % cit. |
|---|---|---|
| oui | 6 | 75,0% |
| non | 2 | 25,0% |
| Total | 8 | 100,0% |

Source : notre enquête

Pour les 75% qui ont dit OUI, l'efficacité réside dans la centralisation du système vers la Direction Générale qui prends en charge les anomalies et qui dispose d'une meilleure surveillance pour les agences ; de plus ces dernières sont rattachées à la division des risques et de contrôle permanant qui se fait au niveau de la direction générale. Pour mesurer cette sécurité nous avons cherché à savoir s'il existait un système de détection de fraude au niveau de chaque banque (de notre échantillon interrogé):

**Tableau n°44** : système de détection de fraude

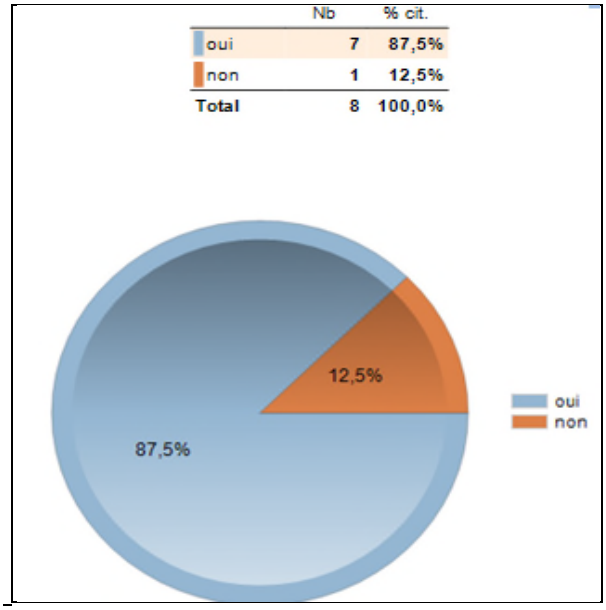
| | Nb | % cit. |
|---|---|---|
| oui | 8 | 88,9% |
| non | 1 | 11,1% |
| Total | 9 | 100,0% |

Source : notre enquête

Parmi les banques interrogées 88,9% ont dit OUI, à l'existence d'un système de détection de fraude contre 11,1% de réponses négatives (une banque sur les neuf). D'après les entretiens

effectué auprès des banques : c'est au niveau de la direction de l'inspection générale ; c'est un service nommé « service contrôle » au niveau de la DG ; le système DELTA ; AML (Anti Money Laundering), voir le processus dans l'annexe n°3**.** En fonctions des réponses des banques nous avons déterminé des critères que certaines banques (la CNEP, SOCIETE GENERALE, CPA) jugent frauduleux et qui incite l'appel aux autorités pour une enquête auprès du niveau centrale qu'est la DG : le certificat de vie ; la signature ; la somme a retiré ou a viré (pour la Société générale par exemple : une somme de 1.000.000 pour un particulier, et 4.000.000 pour un commerçant est passible d'une enquête) ; la procuration (falsifications). A coté du piratage et de fraude de carte bancaire, il y'a le phénomène de blanchiment d'argent qui a pris beaucoup d'ampleur au niveau de la BNA et de la BEA, alors nous avons cherché a savoir au travers de notre enquête quels sont les Dispositif de lutte contre le blanchiment d'argent et qui suit le financement du terrorisme:

**Figure n°20** : les banques qui intègrent un dispositif de lutte contre le blanchiment d'argent




Source : Etablit avec le logiciel Sphinx IQ

Sur les huit banques répondantes, sept banques ont répondu « OUI » à la disposition d'outils de lutte contre le blanchiment d'argent avec un pourcentage de 87,5%, contre une seule réponse négative. Selon les réponses des banques les dispositifs sont :

**i)** La banque centrale charge la direction de la conformité ;

**ii)** les fiches « PEP[67] » au niveau des agences. Ces fiches constituent un ensemble de questions que le client doit remplir et c'est en fonction des réponses que le banquier pourra détecter et jugé si une personne est suspecte ; KYC[68], SIRON[69];

**iii)** Un matériel spécialisé pour la détection de faux billets.

En plus des dispositifs et service conçu et organisés au niveau des directions générales et nationales, les agences disposent d'outils de protection de données et matériels leur permettant d'avoir un accès fiable et sécurisé a leur données et dans l'application de leur taches mettant ainsi en confiance la clientèle et veillant a leur réputation. Selon notre enquête, et parmi les modalités citées ci-dessous, quelles sont celle dont dispose l'établissement ?

[67] Un **PEP** ( personne politiquement exposées) a été ainsi considéré comme une personne « à risque » du point de vue du blanchiment de capitaux et les établissements de crédit sont tenus d'identifier les PEP parmi leur clientèle dès l'ouverture de compte. Pour ce faire, il existe 2 méthodes d'identification :

- Méthode déclarative : Les établissements de crédit modifient les formulaires que doit remplir tout nouveau client lors d'une ouverture de compte, pour faire figurer des questions portant par exemple sur la détention d'un mandat politique, ou l'exercice d'une fonction judiciaire. C'est sur la base de ces informations que l'établissement de crédit qualifie le client comme PEP ou non.
- Méthode interrogative : Les établissements de crédit souscrivent un abonnement spécifique auprès d'un fournisseur de listes PEP. Ces listes sont intégrées dans les dispositifs de contrôle par filtrage et génèrent des alertes lors de rapprochement avec les clients de l'établissement de crédit.

[68] Le **KYC** (Know Your Customers) est une fiche signalétique d'informations sur le client personne physique ou morale. Elle permet a la banque d'établir une relation personnalisée avec sa clientèle afin de mieux cerner son activité. C'est un ensemble de processus que l'établissement de crédit met en œuvre pour assurer à la fois une connaissance approfondie de ses clients, mais également un suivi régulier de la clientèle car l'établissement de crédit dispose, par nature, d'une clientèle habituelle. A l'opposé, une clientèle occasionnelle définit toute personne qui ne rentre en contact avec un fournisseur que dans le cadre d'une transaction isolée (même si la personne effectuera d'autres transactions dans le futur). La relation cesse dès l'achèvement de la transaction. Les obligations de conformité envers les clients bancaires peuvent se scinder en 2 groupes, selon que l'on se place dans le temps au cours de la relation commerciale:

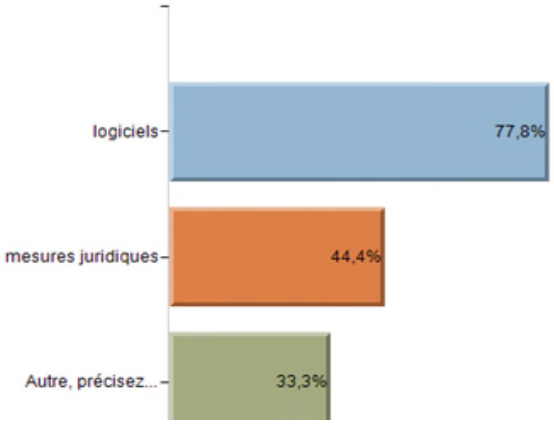
- Le processus de connaissance des clients lors de l'entrée en relation,
- Le suivi régulier des clients pendant toute la durée de la relation commerciale.

[69] **Siron.AML**, est un système de lutte contre le blanchiment d'argent et les fraudes, identifie, évalue et surveille continuellement. Il facilite l'analyse de risque complète, l'intégration des domaines lors de l'évaluation de risque ainsi que la documentation et implémentation sécurisée et non modifiable des mesures et contrôle pour la minimisation de risque, parmi ses fonctions :

- ✓ couverture extensive de toutes les exigences légales contrôle complet de client et leurs transactions, capacité multi-mandat et surfaces multilingues ;
- ✓ modules standard et possibilités d'extension flexibles ;
- ✓ scénarios de contrôle « Best Practice »en vue du blanchiment d'argent à partir d'une multitude d'installations de client ;
- ✓ Intégration simple dans les systèmes de banque via des interfaces de données standardisées et flexibles ;
- ✓ documentation sous forme sécurisée, non modifiable à 100%.

**Figure n°21** : Outils de protection de matériels et données bancaires

| | Nb | % obs. |
|---|---|---|
| logiciels | 7 | 77,8% |
| mesures juridiques | 4 | 44,4% |
| Autre, précisez... | 3 | 33,3% |
| **Total** | 9 | |




Source : notre enquête, traité a partir du logiciel Sphinx IQ.

En plus des logiciels (d'alarme, de gestion des risques) et mesures juridiques, 33,3% des banques disposent d'outils de protection de matériel et de donnée tels que :

- Les Antivirus, parmi les banques interrogées certaine ce sont permise de dévoilé les Antivirus installé et utilisé auprès de leur établissement dans le tableau ci-dessous :
  **Tableau n°45 :** Type d'Antivirus

| | ABC | BADR | BEA | BNA | CNEP | CPA | SGA | NATIXIS | TRUST |
|---|---|---|---|---|---|---|---|---|---|
| Type d'Antivirus | McAfee | - | - | - | - | McAfee | Symantec | - | McAfee |

Source : notre enquête

- Les Codes d'accès, spécifique pour chaque poste de travail, et qui ne sera détenu que par l'utilisateur de ce dernier (procédure de sécurité appliquée qu'à Société Générale) ;
- L'inactivité des lecteurs Flash-disk et des lecteurs CD (par mesure de sécurité) cette application on la trouve dans Trust Bank comme dans la Société Générale ;
- Système DELTA (c'est un logiciel conçu pour réaliser les opérations de banque (de retrait, virements), les opérations de commerce extérieur (crédoc, remise documentaire), autre (comptabilité, gestion de la trésorerie), ce logiciel est généralisé dans toutes les agences et différentes directions comme un bon outil de gestion bancaires).

En dépit des instruments matériels et logiciels, des services et directions responsables de la surveillance, du traitement et de la gestion des infractions numériques, la sécurité reste insuffisante. Elle ne doit pas s'arrêter la, il est du devoir de l'Etat de soutenir ces dispositifs de sécurité bancaires en apportant une réelle politique judiciaire et fournissant ainsi un arsenal législatif qui puisse réprimer la cybercriminalité.

**Conclusion**

La cybercriminalité n'est pas en expansion en Algérie vu le retard de l'introduction des technologies de l'information et du développement insuffisant de la monétique, néanmoins le phénomène est imprévisible et couteux, il pourrait faire perdre aux banques des sommes colossales a travers les fraudes liés aux cartes bancaire, aux distributeurs automatiques et au falsification de chèque, détournement et blanchiment d'argent.

La sécurité est un enjeu majeur pour le bon fonctionnement d'un pays et pour l'avenir de la banque et sa pérennité. En revanche, elle reste sous-estimée en Algérie surtout au niveau des banques. Certes, à nos jours, les infractions cybercriminels que subissent nos institutions se comptent sur le bout des doigts, néanmoins le phénomène reste grandissant dont les pertes seraient inestimables et où le risque numérique conduit au risque de réputation.

## CONCLUSION

L'Algérie a suivi une stratégie de modernisation des secteurs et infrastructures, pour un cadre technologique, innovant des services de télécommunication aux services Internet, du paiement électronique et E-banking. Comme la plupart des pays, cette dématérialisation a fait naitre une nouvelle forme de criminalité insidieuse, invisible et transnationale qui constitue une menace sérieuse pour les institutions, les entreprises, d'où la nécessité d'un dispositif de lutte et de prévention[70]. En dépit des démarches de lutte poursuivie par notre Etat et nos institutions, nombreux sont les professionnels et les juristes qui estiment que le dispositif actuel pour la lutte contre la cybercriminalité est insuffisant. Ils plaident pour la mise en place d'un office de lutte contre la criminalité liée aux TIC et la création d'une agence nationale de la sécurité des systèmes d'Information (SSI). L'Algérie doit élaborer une bonne stratégie, pour faire face aux cyber-menaces il faut passer d'abord, par une prise de conscience, l'éducation, la formation et le soutien des internautes, le renforcement du partenariat public-privé, la coopération et un meilleur encadrement de ces interlocuteurs (les opérateurs de communication), une meilleure organisation de l'Etat, renforcement des moyens juridique que des ressources humaines. L'harmonisation des normes techniques a donc permis la mondialisation des technologies et des services, seulement elle devrait également conduire à l'harmonisation des législations nationales (ce qui pourrait être une bonne initiative pour l'Algérie). Comme l'ont démontré les négociations de la convention du conseil de l'Europe sur la cybercriminalité, le droit national évolue beaucoup plus lentement que les techniques.

[70] Association des expert judiciaires et de la wilaya d'Oran (A.E.J.O), « Aperçu de la cybercriminalité en Algérie », 29/05/2012, http://expertise-judiciaire.hautetfort.com/archive/2012/05/29/cybercriminalite-en-algerie.html, consulté le 9/06/2015.

# CONCLUSION GENERALE

Internet sera omniprésent, elle deviendra bientôt aussi accessible et à moindre coûts que l'électricité. Les internautes seront connectés en permanence via leur téléphone mobile et leur ordinateur portable. Ils seront plus disposés à adopter les nouveaux services sur le Web. Ainsi, le cyberespace fera partie intégrante de la vie quotidienne de tout à chacun. Malgré le fait que nos entreprises et institutions financières ne sont pas suffisamment orientées vers les transactions et les services électroniques, ceci ne doit pas empêcher l'Algérie de se doter de stratégie cyberdefense et de cybersécurité pour se protéger contre la cybercriminalité, une fois ces technologies introduites, car il s'agit d'un phénomène inévitable.

On assiste à un véritable engouement pour la cybercriminalité. La convergence de la criminalité perpétrée dans le monde réel vers la criminalité numérique dans le cyberespace sera de plus en plus appréciée par les délinquants. Ainsi, le blanchiment d'argent, l'escroquerie, la fraude, le piratage, l'espionnage 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. »[1]. Certaines recommandations ont été proposées ci-dessous, parmi elles on cite :

❖ **Investigation et répression**[2] : il est important pour l'Etat d'avoir une connaissance précise du phénomène. Cela suppose le recours à des outils statistiques fiables mais surtout une collaboration étroite entre différentes organisations publiques et privées. L'investigation nécessite un travail d'ensemble ; la police et la gendarmerie sont des acteurs essentiels mais également les fournisseurs d'accès à l'internet et des cybercafés dont l'implication devra être plus grande. Cette recommandation implique le recours à des organisations avancées en la matière, comme l'Europe (cas 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[3].

[1] Ali EL AZZOUZI, op-cit, P.150.
[2]Idem, P.103.
[3]Voir le chapitre 02, dans « stratégie de lutte contre la cybercriminalité ». Source : le Club de la sécurité de l'information français, http://www.clusif.fr

❖ **La coopération internationale :** En juillet 2013, l'Algérie est devenue membre du Groupe Egmont[4] et a signé 17 protocoles d'entente et accords d'échange d'informations avec des homologues d'Afrique, du Moyen-Orient et d'Europe et a élaboré des projets d'amendement du Code Pénal pour mettre certains délits en conformité avec la norme, a élargi les obligations de vigilance à l'égard de la clientèle et étendu les mesures préventives à l'ensemble des institutions financières[5].

❖ **Promotion de technologies de paiement modernes:** les espèces restent le moyen de paiement prédominant en Algérie, cela revient aux questions liées à la fiabilité des réseaux qui contribuent à une faible acceptation de ces moyens modernes. La poursuite du développement des TIC apportera aux moyens de paiement modernes un potentiel de croissance rapide.

❖ **Modernisation de la centrale des risques :** la Banque d'Algérie, devra communiquer suffisamment d'informations aux banques pour qu'elles procèdent à une évaluation exhaustive des risques. Le système souffre d'une couverture restreinte, de la qualité insuffisante des données, de données historiques limitées et d'un système informatique obsolète[6].

❖ **Promotion d'une culture de sécurité :** quel que soit les mesures de sécurité mises en place, elles n'auront de sens que si elles sont accompagnées par la promotion d'une véritable culture de sécurité. Il s'avère alors important de développer et soutenir cette culture de sécurité dans la société. Pour y parvenir, l'Etat, devra s'engager dans[7] : a) La sensibilisation et la communication sur la SSI ; b) Des formations sur la SSI destinées à des élèves ingénieurs ; c) Des formations destinées à des professions juridiques ; d) Des chartes de sites marchands et de E-banking.

**a) La sensibilisation et la communication sur la SSI** : L'Etat doit lancer des campagnes de sensibilisation et de communication sur la sécurité des systèmes d'information ; organiser des séminaires et workshop annuels sur la cybercriminalité et donner une image sur ce qui se fait dans plusieurs pays, pour nous permettre de saisir des messages importants sur les différents thèmes liés à la cybercriminalité.

---

[4] Le Groupe Egmont est un forum qui réunit les cellules de renseignement financier du monde entier et dont le but est de faciliter la coordination, la coopération internationale et l'échange d'informations.

[5] Rapport du FMI, « Algérie, évaluation de la stabilité du financier », No. 14/161, juin 2014, P.27. En 2013, le GAFI a encouragé l'Algérie à prendre de nouvelles mesures, notamment à : prévoir la criminalisation adéquate du financement du terrorisme ; à établir et appliquer un cadre juridique adéquat permettant d'identifier, de retracer et de geler les avoirs terroristes ; dans le but de protéger le secteur financier de l'Algérie contre un usage abusif et de sortir du processus de surveillance. Voir le lien :
https://www.imf.org/external/french/pubs/**ft**/scr/2014/cr14161f.pdf

[6] Idem, P.33.

[7] Ali AZZOUZI, Op-cit, P.147.

**a) Des formations sur la SSI destinées à des élèves Ingénieurs** : Proposer des formations spécialisées en SSI à destination des étudiants de l'enseignement supérieur, permettra à des professeurs et experts en sécurité de dispenser des formations en mettant en valeur leurs connaissances. Parallèlement, on devrait penser à mettre en place un programme de réhabilitation des hackers[8], leur recrutement serait un point positif pour bénéficier de leurs services pour une meilleure protection (ce concept existe aux Etats-Unis et au Royaume-Uni).

**b) Des formations destinées à des professions juridiques** : l'Etat doit créer des passerelles entre l'univers informatique et celui des juristes avec les avocats, les magistrats, les policiers et gendarmes. Pour que les cyberenquêteurs appliquent la loi, il faut d'abord qu'ils soient sensibilisés à la lutte contre la cybercriminalité grâce à des formations spécifiques est indispensables.

**c) Des chartes de sites marchands et d'E-Banking** : La mise en place de chartes par l'Etat conférera aux institutions financières (banques), de meilleurs pratiques en termes de sécurisation de sites de commerce électronique et de services bancaires en ligne. Ainsi, contribuer à renforcer la confiance des citoyens.

**d) La sécurité des moyens de paiement** : Recourir à des moyens cryptographiques pour sécuriser le paiement en ligne accompagné de textes législatifs qui préciseront les responsabilités des différentes parties en cas d'utilisation frauduleuse des instrument de paiement (cartes bancaires qui sont actuellement indisponibles dans le code Pénal).

Pour une meilleure sécurité informatique : *entre stratégies appliquées et objectifs ;*

Nous avons sélectionné certaines entreprises spécialisées dans le contrôle et la performance du système d'information et de la sécurité informatique.

### 1. SunGard[9]

SunGard, 380ème entreprise américaine en 2010 et fournisseur de solutions informatiques intégrées pour les institutions financières. Cette entreprise [10] devrait être d'une grande opportunité pour l'Algérie. Si l'Etat pouvait s'ouvrir à l'implantation de cette entreprise, cette dernière pourra apporter des solutions informatiques à notre secteur financier, et constituer une bonne muraille à l'Algérie, mais aussi une grande offre d'emploi pour le chiffre toujours croissant d'ingénieurs informatiques algériens.

[8] Idem
[9] Rachid JANKARI, op-cit, 2014, page 57.
[10] Elle s'est Implantée en 2011, en Tunisie, le centre est classé troisième centre mondial après celui de la Chine et de l'Inde, source : Rachid JANKARI, op-cit, 2014, P. 57.

### 2. Méditerranée informatique industrie service[11] (M2I Services)

M2I Services[12], Sarl de droit algérien, qui se positionne sur quatre segments d'activités : *le multimédia, les réseaux télécoms, la sécurité* et *les systèmes d'information inshore* et *offshore*. L'entreprise dispose d'un portefeuille de partenariat avec plusieurs éditeurs et constructeurs internationaux (Gold partner Microsoft Gold, Prefereed partner HP, APC, Fortinet, Cisco et Juniper Elite) et développe ses activités principalement dans le domaine des services et notamment de l'assistance à l'intégration et à la bonne gouvernance des systèmes d'information.

### 3. Comparex[13]

Le groupe allemand Comparex, est actif dans les domaines *des logiciels*, de *la sécurité informatique*, de *la bureautique*, de *la communication* et de *la virtualisation*. Il a ouvert une filiale en Algérie en 2009[14]. « Comparex Algérie »[15] est un intégrateur de solutions informatiques, notamment du software, et technologiques. Il compte avec plus d'une quarantaine d'ingénieurs informaticiens, tous algériens. La filiale algérienne représente une large gamme de produits d'éditeurs internationaux tels que Microsoft, Citrix, VMware, Adobe, Symantec, McAfee, Hitachi, IBM et EMC.

Dans ce modeste travail, nous avons présenté de manière générale le concept de Cybercriminalité dans l'économie mondiale puis, déterminé l'état des lieux de l'Algérie dans l'évolution si grandissante de ce phénomène démesuré et inévitable. Pour conclure, nous avons voulu apporter un ensemble de recommandations qui pourrait être soit des projets à exploiter ou des stratégies préalablement mise en place mais qui demande une actualisation et plus de soutien de la part de l'Etat. Ce travail constitue pour nous un préalable pour le lancement d'un autre projet de recherche sur la cybercriminalité, son impact sur notre économie et la nécessité de mise en place d'une cybersécurité.

---

[11] Idem, P.50.

[12] Créée en 1997, M2I Services a réussi à devenir le premier pourvoyeur d'expertise dans ce domaine dans le pays, M2I Services à une croissance régulière et constante de +20% de son chiffre d'affaires. L'objectif pour 2013 est d'attendre les 400 millions de dinars et 30% des parts du marché. Elle compte parmi ses effectives plus de 30 ingénieurs certifiés.

[13] Idem, P.49.

[14] A ouvert en Algérie en partenariat avec l'entrepreneur Djaoued Salim Allal, en 2009. En 2011, il a enregistré un chiffre d'affaires d'un peu moins de 500 millions de dinars (+ 50% par an).

[15] C'est une entreprise qui s'appuie sur le centre d'assistance multi-éditeurs de la maison mère et son académie de formation, Comparex est également revendeur grands comptes de Microsoft pour la zone Europe,Moyen-Orient et Afrique. Chaque année, l'entreprise organise le « Comparex technology day » où elle réunit des représentants des entreprises et des administrations afin de les sensibiliser aux nouvelles technologies et notamment à la virtualisation.

# - LA LISTE DES ANNEXES -

# Annexe 01



Art. 18. — Est puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 100.000 DA à 500.000 DA, tout titulaire d'un certificat électronique qui continue à l'utiliser tout en sachant que ledit certificat est arrivé à échéance ou révoqué.

Art. 19. — La présente loi sera publiée au *Journal officiel* de la République algérienne démocratique et populaire.

Fait à Alger, le 11 Rabie Ethani 1436 correspondant au 1er février 2015.

Abdelaziz BOUTEFLIKA.

———★———

**Loi n° 15-04 du 11 Rabie Ethani 1436 correspondant au 1er février 2015 fixant les règles générales relatives à la signature et à la certification électroniques.**

———

Le Président de la République,

Vu la Constitution notamment, ses articles 119, 120, 122, 125 et 126 ;

Vu l'ordonnance n° 66-155 du 8 juin 1966, modifiée et complétée, portant code de procédure pénale ;

Vu l'ordonnance n° 66-156 du 8 juin 1966, modifiée et complétée, portant code pénal ;

Vu l'ordonnance n° 75-58 du 26 septembre 1975, modifiée et complétée, portant code civil ;

Vu l'ordonnance n° 75-59 du 26 septembre 1975, modifiée et complétée, portant code de commerce ;

Vu la loi n° 84-17 du 7 juillet 1984, modifiée et complétée, relative aux lois de finances ;

Vu la loi n° 88-01 du 12 janvier 1988 portant loi d'orientation sur les entreprises publiques économiques ;

Vu la loi n° 90-21 du 15 août 1990, modifiée et complétée, relative à la comptabilité publique ;

Vu la loi n° 2000-03 du 5 Joumada El Oula 1421 correspondant au 5 août 2000, modifiée, fixant les règles générales relatives à la poste et aux télécommunications ;

Vu l'ordonnance n° 03-03 du 19 Joumada El Oula 1424 correspondant au 19 juillet 2003, modifiée et complétée, relative à la concurrence ;

Vu la loi n° 04-02 du 5 Joumada El Oula 1425 correspondant au 23 juin 2004, modifiée et complétée, fixant les règles applicables aux pratiques commerciales ;

Vu la loi n° 04-04 du 5 Joumada El Oula 1425 correspondant au 23 juin 2004 relative à la normalisation ;

Vu la loi n° 04-08 du 27 Joumada Ethania 1425 correspondant au 14 août 2004, modifiée et complétée, relative aux conditions d'exercice des activités commerciales ;

Vu la loi n° 08-09 du 18 Safar 1429 correspondant au 25 février 2008 portant code de procédure civile et administrative ;

Vu la loi n° 09-03 du 29 Safar 1430 correspondant au 25 février 2009 relative à la protection du consommateur et à la répression des fraudes ;

Vu la loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication ;

Après avis du Conseil d'Etat ;

Après adoption par le Parlement ;

**Promulgue la loi dont la teneur suit :**

## TITRE I

## DISPOSITIONS GENERALES

### Chapitre 1er

### Objet

Article 1er. — La présente loi a pour objet de fixer les règles générales relatives à la signature et à la certification électroniques.

### Chapitre 2

### Définitions

Art. 2. — Il est entendu par :

**1- Signature électronique** : données sous forme électronique, jointes ou liées logiquement à d'autres données électroniques, servant de méthode d'authentification.

**2- Signataire** : personne physique qui détient des données de création de signature électronique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente.

**3- Données de création de signature électronique** : données uniques, telles que des codes ou des clés cryptographiques privés, que le signataire utilise pour créer une signature électronique.

**4- Dispositif de création de signature électronique** : matériel ou logiciel destiné à mettre en application les données de création de signature électronique.

**5- Données de vérification de signature électronique** : des codes, des clés cryptographiques publiques ou d'autres types de données, qui sont utilisées pour vérifier une signature électronique.

**6- Dispositif de vérification de signature électronique** : matériel ou logiciel destiné à mettre en application les données de vérification de signature électronique.

**7- Certificat électronique** : document sous forme électronique attestant du lien entre les données de vérification de signature électronique et le signataire.

**8- Clé cryptographique privée** : chaîne de chiffres détenue exclusivement par le signataire et utilisée pour créer une signature électronique, cette clé est liée à une clé cryptographique publique.

**9- Clé cryptographique publique** : chaîne de chiffres mise à la disposition du public afin de lui permettre de vérifier la signature électronique, elle est insérée dans le certificat électronique.

**10- Autorisation** : désigne le régime d'exploitation de services de certification électronique et se matérialise par le document officiel délivré au prestataire de manière personnelle lui permettant de commencer la fourniture effective de ses services.

**11- Tiers de confiance** : personne morale qui délivre des certificats électroniques qualifiés ou éventuellement fournit d'autres services en matière de certification électronique au profit des intervenants dans la branche gouvernementale.

**12- Prestataire de services de certification électronique** : personne physique ou morale qui délivre des certificats électroniques qualifiés et fournissant éventuellement d'autres services en matière de certification électronique.

**13- Intervenants dans la branche gouvernementale** : institutions et administrations publiques, établissements publics tels que définis par la législation en vigueur, institutions nationales autonomes, autorités de régulation, intervenants dans les échanges interbancaires, ainsi que toute personne ou entité qui de par sa nature ou mission fait partie de la branche gouvernementale.

**14- Titulaire de certificat électronique** : personne physique ou morale à laquelle un prestataire de services de certification ou un tiers de confiance a délivré un certificat électronique.

**15- Politique de certification électronique** : ensemble des règles et procédures organisationnelles et techniques liées à la signature et à la certification électroniques.

**16- Audit** : vérification de la conformité par rapport à un référentiel.

### Chapitre 3

### Principes généraux

Art. 3. — Sans préjudice de la législation en vigueur, nul ne peut être contraint d'accomplir un acte juridique signé électroniquement.

Art. 4. — Le document signé électroniquement est conservé dans sa forme d'origine. Les modalités de conservation du document signé électroniquement sont définies par voie réglementaire.

Art. 5. — Toutes les données et informations à caractère personnel recueillies par les prestataires de service de certification électronique, les tiers de confiance et les autorités de certification électronique ainsi que les bases de données qui les contiennent doivent être hébergées sur le territoire national et ne peuvent être transférées en dehors de celui–ci que dans les cas prévus par la législation en vigueur.

## TITRE II

## DE LA SIGNATURE ELECTRONIQUE

### Chapitre 1er

### Principes d'assimilation et de non-discrimination de la signature électronique

Art. 6. — Une signature électronique a pour fonction d'authentifier l'identité du signataire et de manifester l'adhésion de ce dernier au contenu de l'écrit sous forme électronique.

Art. 7. — La signature électronique qualifiée est une signature électronique qui satisfait aux exigences suivantes :

1- être réalisée sur la base d'un certificat électronique qualifiée,

2- être liée uniquement au signataire,

3- permettre l'identification du signataire,

4- être conçue au moyen d'un dispositif sécurisé de création de signature électronique,

5- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif,

6- être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée.

Art. 8. — Seule la signature électronique qualifiée est assimilée à une signature manuscrite, qu'elle soit le fait d'une personne physique ou morale.

Art. 9. — Nonobstant les dispositions de l'article 8 suscité, une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice au seul motif qu'elle :

1. se présente sous forme électronique, ou

2. ne repose pas sur un certificat électronique qualifié, ou

3. n'est pas créée par un dispositif sécurisé de création de signature électronique.

### Chapitre 2

### Des dispositifs de création et de vérification de la signature électronique qualifiée

Art. 10. — Le dispositif de création de la signature électronique qualifiée doit être sécurisé.

Art. 11. — Le dispositif sécurisé de création de signature électronique est un dispositif de création de signature électronique qui satisfait aux exigences suivantes :

1- il doit, au moins, garantir, par les moyens techniques et les procédures appropriées, que :

## Annexe 02

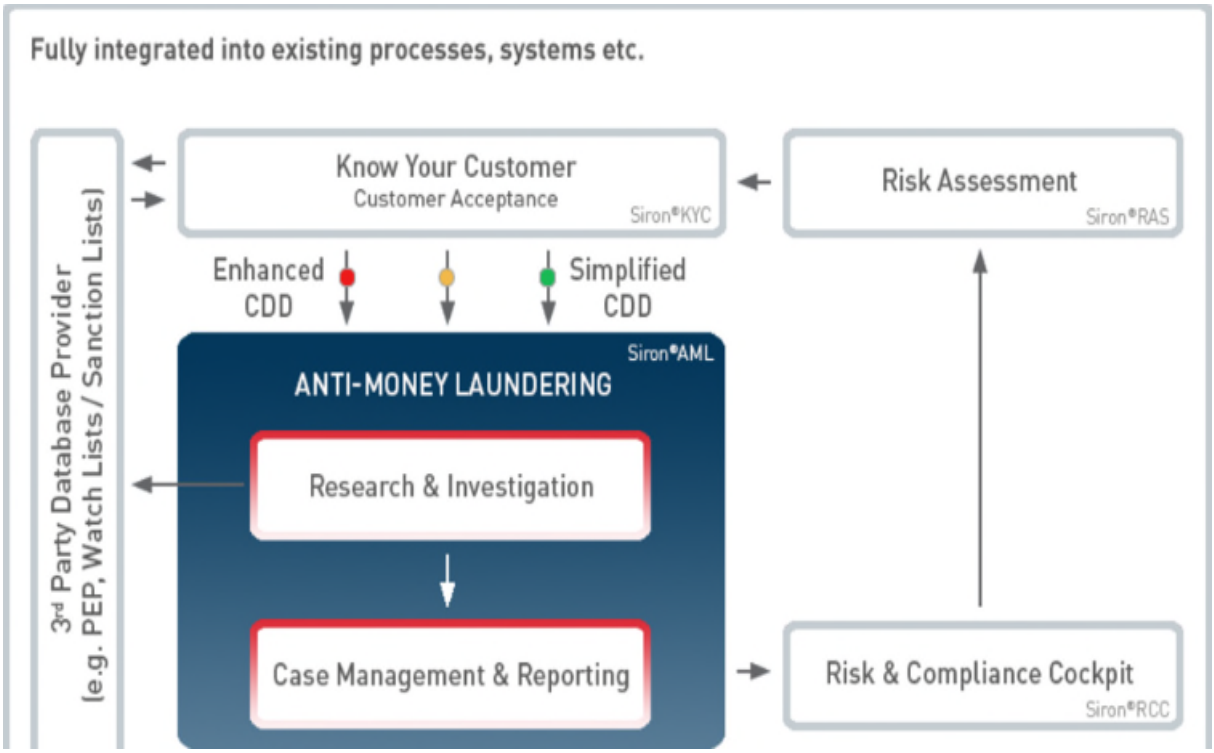
| Type d'infraction | Titre et chapitre du code pénal | Articles du code pénal | la peine |
|---|---|---|---|
| Atteinte au système de traitement automatisé de données (S.T.A.D) | loi n° 04-15 du 10 novembre 2004 (Le chapitre III du titre II du livre III, a été complété en vertu de la loi n° 04-15 du 10 novembre 2004(JO n° 71, p.10), par une section VII bis, intitulé "Des atteintes aux systèmes de traitement automatisé de données" comportant les articles de 394 bis à 394 noniès. | Art. 394. | -Puni d'une peine d'emprisonnement de trois (3) mois à un (1) an et d'une amende de cinquante mille (50.000) DA à cent mille (100.000) DA (pour un accès frauduleux dans le système) ;<br>-Peine est doublée (résultant de la suppression ou la modification de données contenues dans le système) ;<br>-Peine est de six (6) mois à deux (2) ans d'emprisonnement et d'une amende de 50.000DA à 150.000DA (pour altération du fonctionnement du système) ;<br>-puni d'un emprisonnement de deux (2) mois à trois (3) ans et d'une amende de 1.000.000 DA à 5.000.000DA (pour la conception, la diffusion, la révélation et la commercialisation des données stockées et traitées et transmises par le système) ;<br>-Punie d'une amende qui équivaut à cinq (5) fois le maximum de l'amende prévue pour la personne physique (pour une personne morale qui commet une des infractions ci dessus) ; |
| Trahison et espionnage | loi n° 06-23 du 20 décembre 2006(JO n° 84, p.16) | Art. 61.<br>Art. 62.<br>Art. 63.<br>Art. 67. | Puni de la réclusion à temps, de cinq (5) à dix (10) ans. |
| Financement du terrorisme ou d'une organisation terroriste (Actes terroristes ou | loi n°14-01 du 04 février 2014 | Art. 87. | la réclusion à temps de dix (10) à vingt (20) ans. Et d'une amende de 100.000 DA à 500.000 DA |

| | | | |
|---|---|---|---|
| subversifs) | | | |
| Contrefait et falsification de certificats, livrets, cartes, passeports, et autres documents administratifs | la loi n° 06-23 du 20 décembre 2006 | Art. 222. | Puni d'emprisonnement de six (6) mois à trois (3) ans et d'une amende de 1500 DA à 15000 DA. |
| Usurpation d'identité ou usage irrégulier de fonctions, de titres ou de noms[1] | la loi n° 06-23 du 20 décembre 2006(Modifié par la loi n° 06-23 du 20 décembre 2006 (JO n° 84, p.18) rédigé en vertu de l'ordonnance n° 66-156 du 8 juin 1966) | Art. 247. | Puni d'une amende de 500 DA à 5000 DA |
| Menaces | | Art. 284.<br><br><br><br>Art. 285. | Puni d'emprisonnement de deux (2) ans à dix (10) ans et d'une amende de 500 DA à 5000 DA.<br>Puni d'emprisonnement d'un (1) à trois (3) ans et d'une amende de 500 DA à 2500 DA |
| Atteinte portées à l'honneur, à la considération et à la vie privée[2] | Ajouté par la loi n° 06-23 du 20 décembre 2006 (JO n° 84, p.19) | Art. 303. Du code Pénal | Puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de cinquante mille (50.000) DA à trois cent mille (300.000) DA.<br>(Le pardon de la victime met fin aux poursuites pénales) |
| Diffamation | la loi n° 06-23 du 20 décembre 2006 | Art. 298. | Punie d'un emprisonnement de deux (2) à six (6) mois et d'une amende de 25.000 DA à 50.000 DA ou de l'une de ces deux peines seulement. (pour un particulier) ; punie d'un emprisonnement d'un (1) mois à un (1) an et d'une amende de 10.000 DA 100.000 DA ou de l'une de ces deux peines (pour un groupe |

| | | | |
|---|---|---|---|
| | | | de personnes)<br>(Le pardon de la victime met fin aux poursuites pénales) |
| Escroquerie et falsification de chèque | la loi n° 06-23 du 20 décembre 2006 ((JO n° 84, p.22) | Art. 375. | puni d'un emprisonnement d'un (1) à dix (10) ans et d'une amende dont le montant ne saurait être inférieur à celui du chèque ou de l'insuffisance. |
| Blanchiment de capitaux | la loi n° 06-23 du 20 décembre 2006 (JO n° 71, p.9) | Art. 389. | Puni d'un emprisonnement de cinq (5) à dix (10) ans et d'une amende de un million (1.000.000) de DA à 3.000.000 DA ; et puni d'un emprisonnement de dix (10) à vingt (20) ans et d'une amende de 4.000.000DA à 8.000.000DA, (commis de façon habituelle ou dans le cadre d'une organisation criminelle). |

Source : établit par nos soins sur la base du code pénal de l'année 2015.

## Annexe 03




Source : directive de l'UE concernant le blanchiment d'argent, et fraudes recommandations FATF. http://www.tonbeller.com/fr/

## Annexe 04




**FOUNDATION INTERNATIONALE BILL GATES**
**DIRECTION DE LA PROMOTION DE L'INTERNET ET DU JEUX**
**LA DIRECTION DE LOTERIE CRISTAL INTERNATIONALE BILL GATES**
**Loterie Américaine pour la promotion de l'Internet partout dans le monde**

**Réf. Nombre : 22/756/4007**
**Numéro de lot : 497 00 1527-AB66**
**Numéro de gain : AB 164C**

**Monsieur/Madame**

**Nous sommes heureux de vous informer du résultat des programmes internationaux de gagnants de loterie tenus il y a deux jours de cela à notre siège sis à New York.**
**Votre adresse d'E-mail attachée au billet le numéro 9570015948-6410 avec le numéro de série 3648042- 510 a dessiné des numéros chanceux 4-14-66-71-07-36 qui en conséquence gagne dans la 1ère catégorie avec quatre autres personnes, vous avez été donc approuvés pour percevoir la somme forfaitaire hors taxe de 100.000 Euro (Cent Mille euro).**
**FELICITATIONS !!!!!!!!!!!!!!!!!!!!!!!!!!!!**
**En raison du mélange vers le haut de quelques nombres et noms, nous demandons de gardez l'information confidentielle de votre gain jusqu'à la fin de vos réclamations et que les fonds vous soit remis.**
**Cela fait partie de notre protocole de sécurité pour éviter double réclamation et abus sans garantie de ce programme par quelques participants.**
**Tous les participants ont été tirés par un logiciel de pointe de vote d'ordinateur tiré parmi plus de 20.000.000 compagnies et de 30.000.000 adresses d'e-mail d'individu de partout dans le monde.**

**Ce programme promotionnel de l'Internet a lieu chaque trois ans.**
**Cette loterie a été favorisée et commandité par Monsieur BILL GATES, président du plus grand logiciel du monde ( Microsoft ), nous espérons qu'avec une partie votre de gain vous participerez à la promotion de l'Internet chez vous car cela fait partie également de la promotion de Monsieur BILL GATES.**
**Suite à plusieurs obstacles pour certains gagnants de rentrer en possession de leur gain, directement avec le siège à new York, nous avons cotiges à déléguer quelque agence partout dans le monde depuis deux années. Cette fois ci en Afrique de l'ouest plus précisément en Cote d'Ivoire. (Abidjan) Notre STANDARD CHARTERED BANK représentative à Abidjan débitera immédiatement le processus pour débloquer vos fonds dès que vous entrerez en contact avec elle.**
**Pour les réclamations de votre gain, entrer en contact par courrier avec SVP Notre représentant officiel de justice Maître: CAMARA GILLES de l'agence de confiance globale, Charge de la légalisation des dossiers des lauréats qui ne peuvent se rendre ici a notre siège.**
**Contact Direct l'avocat : e-mail :** cabinet.camaragilles@yahoo.co.uk

**Défendre vos intérêts au point de vu juridique auprès de Maître: CAMARA GILLES afin d'éviter certaines erreurs, nous vous rappelons de citer à Maître: CAMARA GILLES, par courrier électronique ou par téléphone les informations Comportant :**

1) **Votre Nom et Prénoms**
2) **Adresse Complète**
3) **N° De Téléphone,**
4) **N° réf, N°de lot et N°de gain**

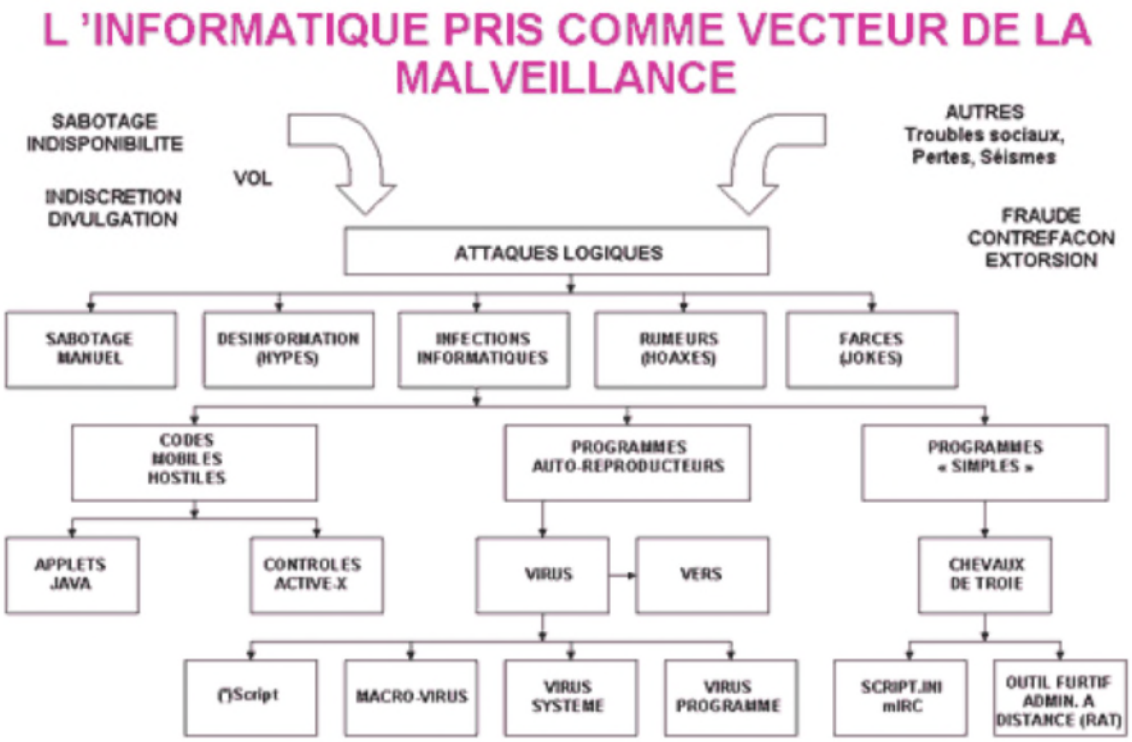
**Ainsi Qu'une Copie De Votre Carte Nationale D'identité Ou Passeport.**
**Après Quoi Il Vous Sera Expliqué dans les moindres détails Comment Entrer En Possession De Votre Gain.**
**Se rappeler que le lot doit être réclamé avant plus de deux semaines, après quoi tous les fonds non revendiqués seront reversés à certains Organisme Internationaux de Santé et de Médecine.**
**En outre, s'il devrait y avoir n'importe quel changement d'adresse informez notre agent aussitôt que possible. Recevez les félicitations une fois de plus de nos membres de personnel et nous vous remercions de faire partie de notre programme promotionnel.**

**Note : Quiconque sous l'âge de 18 ans est automatiquement éliminé.**

**Madame ISABELLE CHEVALIER / Directrice des Opérations**

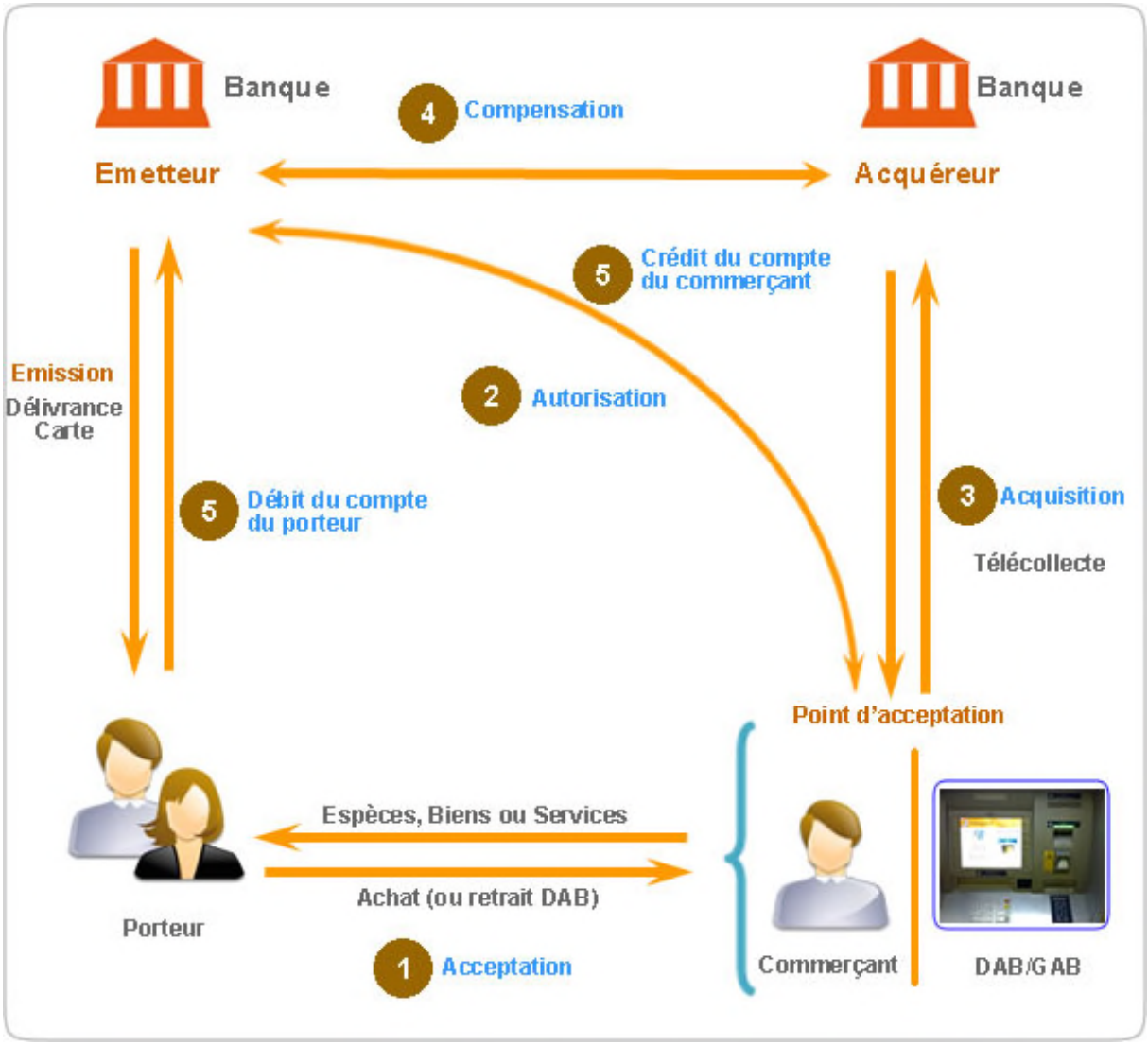

Bill Gates

## Annexe 05



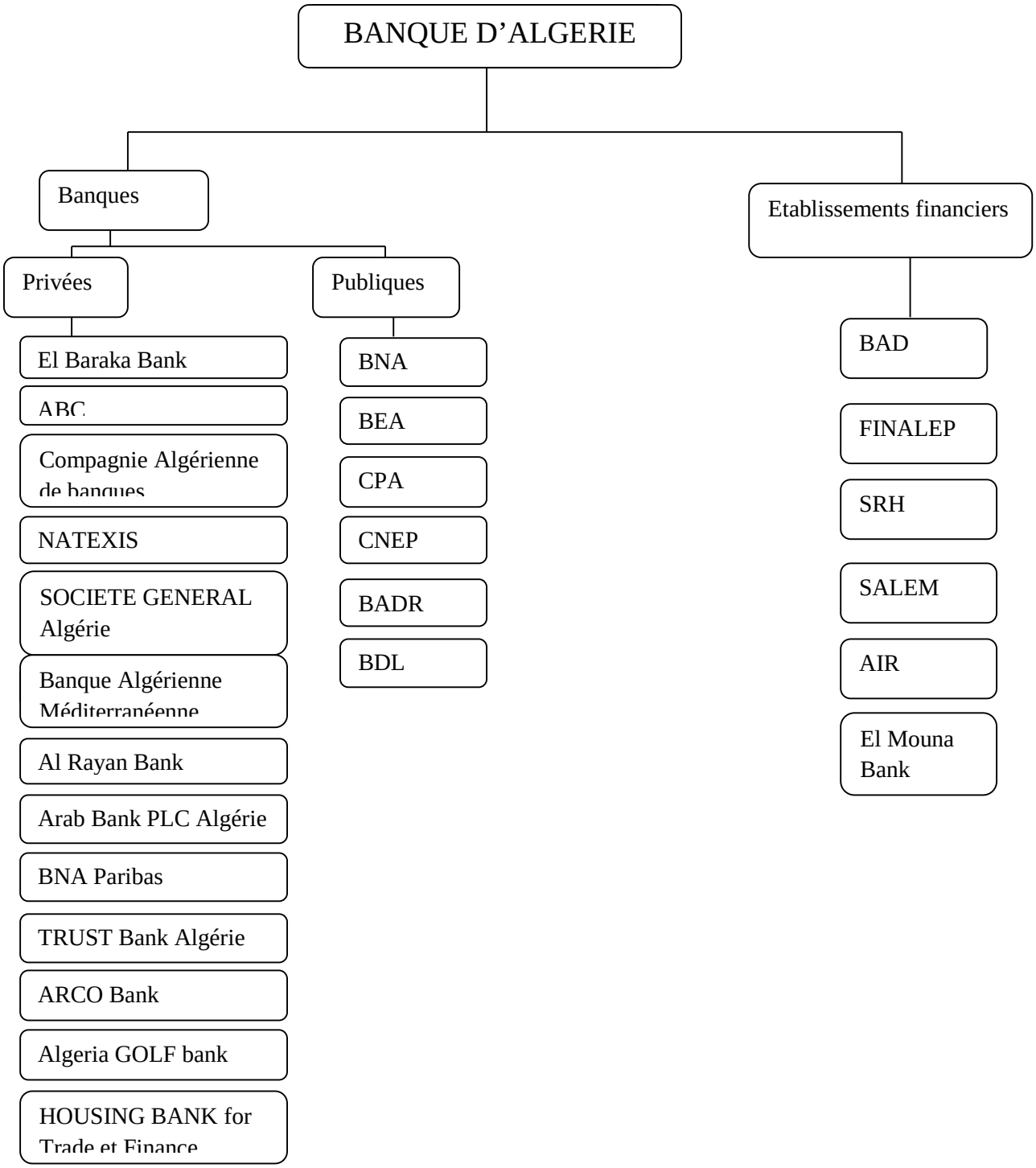

Source : http://www.perso.wanadoo.fr/malware.fr

## Annexe 06


Banque
Emetteur
4 Compensation
Banque
Acquéreur
5 Crédit du compte du commerçant
Emission
Délivrance Carte
2 Autorisation
5 Débit du compte du porteur
3 Acquisition
Télécollecte
Point d'acceptation
Espèces, Biens ou Services
Achat (ou retrait DAB)
Porteur
1 Acceptation
Commerçant
DAB/GAB

## Annexe 07

### - Système bancaire algérien -




Source : établit par nos soins

**Annexe 08**

# QUESTIONNAIRE

Nom de la banque : ……..
Capital social :……...
Date de création :……..
Effectif :……
Nombre d'agence et succursales :…….
La banque est : Privée ……. Publique : …… Autre : ……..
Nom est fonction de la personne qui remplit le questionnaire : (au choix)
…….....
Personne ou service à contacter pour des renseignements complémentaires :
……
……

## I- Questions relatives aux technologies de l'information et de la communication de la banque

**1)** Est-ce que votre banque a introduit de nouvelles technologies ?

OUI……. NON…….

Si OUI, lesquelles ?

a- Introduction de nouveaux équipements informatiques …..
b- Introduction de nouvelles applications informatiques (SGBD, système client-serveur) …….
c- réalisation d'un serveur vocal …..
d- création d'un service télécompensation …..
e- mise en place d'un système INTERNET …..
f- les postes de travail portables …..
g- autres, à préciser :……

(Cochez la case correspondant à votre choix)

**2)** Quel est l'impact de l'introduction des nouvelles technologies sur votre mode interne de travail ?

a- Rapidité et fiabilité de traitement des opérations
b- Amélioration de l'efficacité et de la précision
c- Réduction de la contrainte de la présence physique derrière un bureau
d- Réduction du risque d'erreurs
e- Suppression des taches en double
f- Autres, à préciser

(Veuillez les classer par ordre d'importance de 1à 6)

**3)** Quel est l'impact de l'introduction de nouvelles technologies, en tant qu'outil de travail, sur votre productivité ?

| | 1-Peu importante | 2-Importante | 3-Très importante |
|---|---|---|---|
| 1-Amélioration de la productivité | | | |

**4)** Quelles satisfactions avez-vous retirées de l'introduction de nouvelles technologies au sein de votre banque ?

| | 1-Aucune | 2-Peu | 3-Moyenne | 4-Assez | 5-Elevée |
|---|---|---|---|---|---|
| 1-Amélioration de la productivité | | | | | |
| 2-Fiabilité et rapidité de traitement des opérations. | | | | | |
| 3- Renforcement de la rentabilité | | | | | |
| 4-Amélioration de la qualité des prestations. | | | | | |
| 5-Fidélisation des clients. | | | | | |
| 6-Autres, à préciser : …… …….. ..…..... | | | | | |

(Cochez la case correspondant à votre choix)

**5)** Est-ce que vous vous êtes facilement adaptés aux mutations technologiques de votre banque ?

OUI……. NON…….

A- SI OUI, pourquoi ? .....
.....

B- Si NON, qu'avez-vous fait ?
- a- Séminaire ou stage de perfectionnement
- b- Cours de formation initié par votre banque
- c- Apprentissage par la pratique
- d- Autres à préciser : ……

**6)** Peut-on estimer :

| | 1-sans l'outil informatique | 2-avec l'outil informatique |
|---|---|---|
| 1) Le nombre moyens d'opérations* que vous effectuez par jour | | |
| 2) Le temps moyen consacré à chaque type d'opération ? | | |

(*) Opérations de retraits, versements, transferts, change, etc.

**7)** Selon vous, la technologie est vue comme :

a- Une charge pour la banque
b- Une ressource stratégique de la banque
c- Globalement, est-ce qu'il s'agit d'un gain :
Ou d'une perte :

(Cochez la case correspondant à votre choix)

**8)** Pourriez-vous nous indiquer votre opinion personnelle concernant le rôle que joue la technologie au sein de votre banque ?

……
……
……
……

**9)** Souhaitez-vous introduire d'autres nouvelles technologies au sein de votre banque ?

OUI……. NON…….

Si OUI, que proposez-vous ? ……..
…….

**10)** A quelle date votre banque a-t-elle introduit Internet (effectuer sa connexion) ?

……

**11)** Votre banque et l'ensemble de vos agences sont connectés sur Internet avec :

a- Une ligne téléphonique simple (modem)
b- Une ligne téléphonique numérique
c- Un câble de télédistribution
d- ADSL
e- Autres :

……
……

**12)** Avez-vous un quelconque partenariat avec un opérateur téléphonique ou Algérie Télécom ?

OUI…….. NON……..

Si OUI, lequel ? Pourquoi ?

……
……
……
……....

## II- Questions relative aux moyens de paiement (monétique et automatisation)

**1)** Quel est le moyen de paiement le plus automatisé dans votre banque ?

a- Le chèque …….
b- L'avis de prélèvement ……
c- La carte bancaire……
d- Autre (à préciser) :

……
……

(Cochez la case correspondant à votre choix)

**2)** Quel type de carte utilisez-vous ?

a- Cartes de retrait
b- Cartes de paiement
c- Cartes de crédit
d -Autre (veillez préciser) :

……
……
……

**3)** Depuis quand avez-vous mis en œuvre l'utilisation des cartes ?

……

**4)** Quel est le nombre de porteur de vos cartes ?

……
……
……

**5)** Si vous avez mis en place un processus d'automatisation de chèque, depuis quand est il en fonction dans votre banque ?

……
……

**6)** Êtes-vous membre du réseau SWIFT ?

OUI…… NON……

Si OUI, depuis quand ?

……....

-Quelle est son utilité ?

……..

**7)** Votre banque dispose t- elle d'un réseau de distributeurs et guichets automatiques (DAB/GAB) ?

OUI…… NON…….

Si OUI, combien ? (comprenant toutes les agences)

……
…….....

## III- Questions relative au système informatique

**1)** Avez-vous adopté une stratégie de développement de votre système informatique ?

OUI……. NON…….

Si OUI, sous quels critères ?

a- Réaliser une économie d'échelle ☐
b- Assurer une plus large diffusion des produits ☐
c- Modernisation ☐

Autres (à préciser) :

……
……

(Cochez la case correspondant à votre choix)

**2)** Comment pourriez-vous qualifier le processus d'informatisation de votre banque (y compris vos agences) ?

a- Graduel et rapide ☐
b- Graduel à vitesse plutôt moyenne ☐
c- Graduel mais lent ☐

(Cochez la case correspondant à votre choix)

**3)** A combien estimez vous le pourcentage d'informatisation de votre banque et vos agences ?

a- à moins de 10% ……
b- Entre 10 et 30% …...
c- Entre 30 et 50% ……
d- Entre 50 et 70% ……
e- Entre 70 et 90 % ……
f- A plus de 90% ……

**4)** Est-ce que votre banque a hébergé un site WEB ?

OUI……. NON…….

- Si OUI, à combien estimez vous le nombre moyen d'internautes qui accèdent à votre site par jour ? ……..
- Si NON, est ce que votre banque va pouvoir bientôt faire de l'hébergement ?

OUI……. NON…….

(Cochez la case correspondant à votre choix)

**5)** Pourquoi utilise- vous Internet ? (choix multiple)

a- Pour télécharger des fichiers (documents, rapport, études,…) ☐
b- Pour télécharger des logiciels (gratuit ou pas) ☐
c- Pour rechercher des informations ☐
d- Consultation de courrier électronique ☐
e- Echange de données avec les coopérants (ou liens avec vos agences) ☐
f- Echange de fichiers avec les clients ☐
g- Diminuer les couts ☐
h- La présentation de la banque ☐
i- Autre :

……
……
……

**6)** Quels sont les objectifs de la création de votre (vos) site(s) Internet ? (choix multiple)

a- Présentation de la banque ☐
b- Exposition des services à fournir ☐
c- Publicité et promotion de nouveaux produits ☐
d- Autres :

……
……
……

**7)** Le budget annuel destiné à l'informatisation (équipement et logiciel) est de :

a- …….....DA/ an

b- ……% du total du budget de la banque

**8)** Par rapport aux dernières années, le taux de croissance annuel des dépenses informatiques :

a- A augmenté ……. De quel pourcentage ? ……. %

b- A baissé ……. De quel pourcentage ? ……. %

(Cochez la case correspondant à votre choix)

**9)** Est-ce que vous contrôlez la performance de votre système informatique ?

OUI……. NON…….

Si OUI, comment ?

……

……

……

**10)** Ce contrôle se déroule :

a- Annuellement …….

b- Semestriellement …….

c- Trimestriellement …….

d- Mensuellement …….

Autre : ……

## IV- Questions relatives aux risques numériques et à la sécurité informatique

**1)** Avez-vous pensé à sécuriser votre réseau ?

OUI…… NON……

Si OUI, comment ou quel (s) est (sont) votre dispositif de sécurité ?

……

……

……

**2)** Disposez-vous d'un système d'alerte en cas d'effraction ou de menace à caractère numérique ?

OUI…… NON……

Si OUI, le (les) quel (s) ?

……

……

**3)** Quel est le nombre d'informaticiens auxquels votre banque fait appel ?

……..

**4)** Votre personnel informaticien se répartit :

a- …….. % de cadres

b- …… % d'agents de maitrise

c- ……% d'agents d'exécution

**5)** Quel est le pourcentage que représente le personnel informaticien de votre banque :
……..% du total de votre effectif

**6)** Quel est le budget consacré a la sécurité de votre système informatique ?

a- …… DA/an

b- ……% du total du budget de la banque

**7)** Le système de sécurité employé permet il d'assurer une surveillance efficace et permanente des risques encourus ?

OUI…….. NON……

Si OUI, comment ?

……
……
……

**8)** Existe-il un service de détection et de traitement de fraude ?

OUI…… NON……

Si OUI, le quel ? Comment fonctionne-t-il ?

……
……
……
……
……

**9)** Quel sont les critères qui vous permettent de détecter un comportement frauduleux ?

……
……
……
……

**10)** Pouvez vous estimer en nombre et en pourcentage les infractions liées aux TIC et auxquels la banque à fait face ?

……
……

**11)** Votre système aurait il été victime d'une intrusion « spamming » ou infection par virus « malware » ?

OUI…… NON……

**12)** Y' a-t-il un dispositif qui permet de lutter contre le blanchiment d'argent ?

OUI…… NON……

Si OUI, le quel ? Et comment?

……
……
……
……

**13)** Quel est le protocole applicable de votre banque ?

……
……

……
……

**14)** Quel est le temps moyen de traitement d'un quelconque risque numérique (acte frauduleux), ou de menace? (pour une identification et pour le traitement)

……
……

**15)** Avez-vous déjà reçu des plaintes de la part de vos clientèle ayant été victime de SPAM ?

OUI…….. NON……..

Si OUI, quel est le pourcentage estimer ?

…….....% par an

**16)** Existe-il un service interne qui permet aux particuliers de dénoncer des spam ?

OUI…….. NON…….

Si OUI, le quel ?

……
…….

Comment intervient-il ?

……
……
……

**17)** Combien de temps gardez-vous les données de connexions et de compte ?

……
……
……

**18)** Avez-vous fait face à des cas de piratage (le *hacking*, *malware*, vandalisme, le *Denial of service* (DdoS)) touchant les données ou le matériel ?

OUI……. NON……

Si OUI, a combien estimez voue ces attaques par année ?

…….% par an

**19)** Avez-vous fait face à des fraudes de cartes bancaires ou des cas d'usurpation de numéros de cartes bancaires ?

OUI…… NON……

Si OUI, quel est le pourcentage estimé ?

…….....

**20)** Avez-vous rencontré des cas de falsification de chèques ?

OUI……NON……

Si OUI, à combien l'estimez vous?

.....

**21)** Disposez-vous de mesures ou outils pour protéger et sécuriser vos données et matériel?

OUI……NON……

Si OUI, parmi ces outils vous disposez de :

a- Logiciels
b- Mesures juridiques

c- Autre (à préciser) :
……
……
…….....
.....

**MERCI POUR VOTRE COLLABORATION**

# - BIBLIOGRAPHIE -

- ***OUVRAGES***


1. **AZZOUZI Ali El**, « La cybercriminalité au Maroc », édition Ali El Azzouzi, 2010, Casablanca- Maroc.
2. **COUTINET NATHALIE**, "Définir les TIC pour mieux comprendre l'économie », ed. HAL (archives-ouvertes), 2007, Paris.
3. **DUFLOT. F**« les infections Informatiques Bénéfiques », Juriscom, 2004, Paris, France.
4. **FILIOL. F**« Les virus informatique : théorie, pratique et applications », Ed. Springer, 2004.
5. **GEMIGNANI**, "Computer Crime: The Law in '80, Indiana Law Review", Vol. 13, 1980.
6. **HASSAM FODIL**, « Le système bancaire algérien », Edition l'Economiste d'Algérie, Alger, 2012.
7. **GRANGER**, « Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus », 2001.
8. **KABAY,** "A Brief History of Computer Crime: An Introduction for Students", 2008.
9. **L. D. BALL**: *Computer Crime* in *The Information Technology Revolution* T. FORESTER, MIT Press, Cambridge, 1985, PP. 543-544.
10. **LAMOUREUX ANDREE**, "Recherche et méthodologie en sciences humaines", 2ème édition, Beauchemin, 2003.
11. **MARKUS** et al. "pour une synthèse de ces relations entre les technologies de l'information et la structure des organisations", (communication de recherche), (1988).
12. **M. CHAWKI**, Essai sur la notion de cybercriminalité, IEHEI, 2006.
13. **MOLANDER, RIDDILE, WILSON**, Strategic Information Warfare, 1996
14. **OLIVIER ITEANU**, « Tous cybercriminels », Jacques-Marie Laffont éditeur, 2004.
15. **PUTNAM/ELLIOTT,** International Responses to Cyber Crime, in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism, 2001.
16. **ROWE. F**, "Des banques et des réseaux : productivité et avantages concurrentiels", Ed Economica, 1994, Paris.
17. **SARRAZIN. J.** BTS BANQUE « Techniques bancaires du marché des particuliers », 3e édition, Canada (Québec), 2013.
18. **SIEBER**, « Computer Crime and Criminal Law », 1977.

19. **SOFAER; GOODMAN**, « Cyber Crime and Security », « The Transnational Dimension of Cyber Crime and Terrorisme», 2001.
20. **VELASCO SAN MARTIN**, "Jurisdictional Aspects of Cloud Computing", 2009.
21. **GERCKE**, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009.
22. **WILSON,** "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress", 2007.

- ***REVUES ARTICLES, ET DOCUMENTS DIVERS***

23. **ALTERMAN.H et BLOCH** : La Fraude Informatique (Paris, Gaz. Palais), 3 sep. 1988
24. **BEN YOUSSEF ADEL, HATEM M. HENNI,** « Les effets des technologies de l'information et de communication sur la croissance économique », 2004.
25. **BERNARD MICHEL**, directeur général adjoint du crédit agricole S.A, HORIZON BANCAIRE N° 316 - « Banque et nouvelles technologies », Février 2003.
26. **BIN LADENS MUSHARBASH**, "Intranet", Der Spiegel, Vol. 39, 2008.
27. **CHEN/THOMS**, Cyber Extremism in Web 2.0 – An Exploratory Study of International Jihadist Groups, Intelligence and Security Informatics, 2008, P. 98.
28. **CHETTAB NADIA**, « Economie, TIC et bonne gouvernance en Algérie », papiers imprimés, Université Badj Mokhtar, Annaba 2012.
29. **CRILLEY**, "Information warfare: New Battlefields – Terrorists, propaganda and the Internet", Aslib Proceedings, Vol. 53, No. 7 (2001).
30. **CLUSIF**, « les virus informatiques », décembre 2005.
31. **Code Pénal** d'Algérie, 2015.
32. **Code Pénal** de l'Etat de Californie (la section 502)
33. **Code Pénal** de l'Etat du Texas, (Sections 33. 02)
34. **Congrès des Nations Unies** (10ème), à Vienne, sous le titre « la prévention du crime et le traitement des délinquants »,10 – 17 avril 2000.
35. **DERDOURI ABDELAZIZ**, Directeur Général SSRI, article sur « Impact économique global de la cybercriminalité, 9juin 2014**DOUICI. N**, « l'alerte est donnée au niveau national, des cartes bancaires piratées à Béjaia », el Watan, le 30.05.2015.
36. **DZIDONU. C**, président de l'Institut International des Technologies de l'Information, dans l'ADEA (Association of Development of Education in Africa). Publication « Le développement de l'internet en Afrique », 1999,
37. **EALY**, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention".

38. **FOCUS**- les dangers liés au développement des monnaies virtuelles : l'exemple du « bitcoin », Revue de la « banque de France » n° 10-5 décembre 2013.
39. **FREED,** "Materials and cases on computer and law", 1971.
40. **JANKARI RACHID**, « Les technologies de l'information au Maroc, en Algérie et en Tunisie », vers une filière euromaghrébine des TIC ? », Consultant à l'Institut de Prospérité Economique du Monde Méditerranéen, Etudes & Analyse, vers une filière euromaghrébine des TIC ?, Octobre 2014, page 19, 20.
41. **LAMRI DOUIDI** ; CHABANE KHENTOUT et MAHIEDDINE DJOUDI, « Place de l'Algérie dans le monde des TIC, 2012.
42. **L. D. BALL**: Computer Crime in The Information Technology Revolution T. FORESTER (Cambridge, MIT Press), 1985.
43. **LEMAN-LANGLOIS STEPHANE**, Criminologie, vol. 39, N°1, 2006, P. 65.
44. **LEVY**; "Hacking Offences", Australian Institute of Criminology, 2005.
45. **JOEL MACHARIA**, « l'accès à Internet n'est plus un luxe », Revue, « Afrique Renouveau », Avril 2014.
46. **MITCHISON/WILIKENS/BREITENBACH/URRY/PORTESI** – Identity Theft – A discussion paper.
47. **ORIOLA,** "Advance fee fraud on the Internet: Nigeria's regulatory response, Computer Law & Security Report", Volume 21, Issue 3, P.237.
48. **REICH**, "Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security", IF-1, page.1.
49. **RENNARD MARC** et **BUONANNO OLIVIER**, France Télécom Orange. Article dans sur « Les télécoms, facteur de développement en Afrique », dans l'Expansion Management Review, N° 129, Editeur Roularta, page 9.
50. **ROWE**, « impact de l'information sur la performance de l'entreprise »,1994.
51. **SIEBER**, Council of Europe Organised Crime Report 2004
52. **SIEBER** & **BRUNST**, "Cyberterrorism – the use of the Internet for terrorist purposes", Council of Europe Publication, 2007..
53. **SLIVKA** & **DARROW**, "Methods and Problems in Computer Security", Journal of Computers and Law, 1975, p. 217.
54. **SOLUCOM** (les Synthèses), Management & IT consulting, Observatoire de la transformation des entreprises, n° 47, sur la Cybercriminalité.
55. **STEVENS**, "Identifying and Charging Computer Crimes in the Military, Military Law Review", Vol. 110, 1985.
56. **TABOY. T** , "Les modèles de m-banking", Bankable Frontier Associates/ Departement for International Developement, mais 2006.

57. **TCHENG. H**, Jean Michel Huet, Isabelle Viennois, Mouna Romdhane, 2008, « Les télécoms facteur de développement en Afrique », l'Expansion Management Review n°129, Ed Express Roularta, pp110-120.
58. **TEBIB HANA**, « la monétique et le e-citoyen en Algérie durant la période 2005-2013 : la contrainte culturelle: cas des clients de la BEA et de la BADR », in revue des Sciences Humaines, Université Mohamed Khider Biskra, N°34, Mars 2014. pp91-115.
59. **THORNBURGH**, "Inside the Chinese Hack Attack", "Time", du 25/08/2005
60. **TRAYNOR**,"Russia accused of unleashing cyberwar to disable Estonia", The Guardian, 17.05.2007.
61. **UNITED STATES HOMELAND SECURITY ADVISORY COUNCIL,** Report of the Future of Terrorism, 2007
62. **WALL. D**: Crime and the Internet (N.Y., Routledge), 2001
63. **Wall. D**, "Cybercrime, The Transformation of Crime in the Information Age", Polity Press, 2007.
64. **WEIMANN**, le rapport USIP, "How Terrorists use the Internet", 2004.
65. **WILSON**, "Computer Attacks and Cyber Terrorism, Cybercrime & Security", IIV-3. P.5.
66. **WODA,** "Money Laundering Techniques With Electronic Payment Systems», Information & Security, Vol. 18, 2006
67. **ZITTRAIN**, History of Online Gatekeeping, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2 ( D.C.P.), [1984], n° 7.

- ***TEXTES DE LOIS***

68. Instruction de banque d'Algérie n°05695 du 25/ 01/1995 et les dispositions des articles 472 et suivants du code de commerce, modifiés par la loi 05/02 du 06 février 2005 ; le règlement Banque d'Algérie n° 92/03 du 22/03/1992 plus l'instruction 71/92 du 24/11/1992.
69. Loi n° 06-23 du 20 décembre 2006 (JO n° 84, p.22), ajouté par la loi n° 04-15 du 10 novembre 2004 (JO n° 71, p.9).
70. Loi n° 04-15 du 10 novembre 2004(JO n° 71, p.10), par une section VII bis, intitulé "Des atteintes aux systèmes de traitement automatisé de données" comportant les articles de 394 bis à 394
71. Loi n° 06-23 du 20 décembre 2006 (JO n° 84, p.16), (JO n° 84, p.18) rédigé en vertu de l'ordonnance n° 66-156 du 8 juin 1966 ; (JO n° 84, p.19) ;
72. Loi n°14-01 du 04 février 2014 (JO n°07, p.5).
73. Loi n°15-04 du 1er Février 2015, p.6, p.7.

- ***RAPPORTS***


74. **ARPT**, Bilan annuel, l'observatoire du Mobile-Autorité de régulation, 2014, Algérie.
75. **IFCAM**, Rapport du groupe de travail, (Institut de Formation du Crédit Agricole Mutuel), « Moyen de paiement et services associés », 2013-2014.
76. **MINISTERE DES FINANCES ET DES COMPTES PUBLICS**, « les monnaie virtuelles », rapport du groupe de travail, juin 2014.
77. **MOHAMED AMINE KESSOURI**. « Les indicateurs de Télécommunication/ TIC : Etats des lieux en Algérie », 11ème réunion sur les indicateurs Télécom/TIC, Mexique, rapport d'Algérie Télécom, 2013, Algérie.
78. **Rapport** du "Council of Europe Organised Crime", par Sieber, 2004.
79. **Rapport** du Comité sur la préservation et l'utilisation des données économiques, 1965.
80. **Rapport,** sur « Comprendre la cybercriminalité : phénomène, difficultés, et réponses juridiques », élaboré par le professeur Marco Gercke, septembre 2012.
81. **Rapport de la Commission Bancaire**, annuel, 1999.
82. **Rapport de la Commission européenne**, Affaire intérieures, La cybercriminalité, 2009.
83. **Rapport,** "Global Phishing Survey 2H2013 : Trends and Domain name Use, clés statistiques, Avril 2014.
84. **Rapport de l'ONDRP**, 2011.
85. **Rapport USIP**, « HOW TERRORIST USE THE INTERNET », par Weimann, 2004.
86. **Rapport** sur la cybercriminalité « protéger les internautes », 2014
87. **Rapport de l'UIT**, « comprendre la cybercriminalité : guide pour les PED », Genève-Suisse, 2009 et 2012.
88. **Rapport de l'UIT**, « mesurer la société de l'information », Genève-Suisse, 2013 et 2014.
89. **Report "Phishing Activity Trends",** for the Month of April 2007.
90. **Report of The World Bank**, « Fondations for the development of information and communication technologies in Algeria", report No. 25841, Avril 2003.
91. **Rapport de** ROBERT, MARC, du groupe de travail Interministériel sur : « La lutte contre la cybercriminalité », , Février 2014
92. **Rapport**, « The Global Information Technology », Soumitra Dutta (Cornell University), Thierry Geiger, (World Economic Forum), Bruno Lanvin (INSEAD), 2015.


- ***MÉMOIRES***


93. **BOUCHELIT RYM,** « Les perspectives d'E-banking dans la stratégie E- Algérie 2013 »,

thèse de doctorat en sciences économiques, université de Tlemcen, 2014-2015.

***94.*** **CASILE J.-F**.: Le Code Pénal Á L'Epreuve De La Délinquance Informatique (Thèse, Aix-Marseille), 2002.

**95. ENDERLIN CLEMENT**, mémoire de recherché Diplôme Universitaire Sécurité intérieur/ extérieur dans l'union Européenne, "Les moyens juridique et institutionnels nationaux et européens de lutte contre la cybercriminalité dans le cyberespace », 2011.

***96.*** **MATIGNON EMMANUELLE**, mémoire de recherche sur « la cybercriminalité : un focus dans le monde des télécoms», Université Paris 1 Panthéon-Sorbonne, 2012.

- ***SITES WEB***

**97. BADR**, http://ebanking.badr.dz/fr/

**98. IFCAM**, www.ca-ifcam.fr

**99. INTERNET WORLD STATS**, www.internetworldststs.com/stats.html.

**100. IUT**, International Union of Telecommunication http://www.banque-info.com/lexique-bancaire/d/distributeur-automatique-de-billets--dab

**101. KASPERSKY LAB,** http://blog.kaspersky.fr/quest-ce-qui-motive-les-cybercriminels-largent-evidemment/372/

**102. LEGIGLOBE,** http://legiglobe.rf2d.org

**103. OFFICE QUEBECOIS DE LA LANGUE FRANÇAISE**, « bibliothèque virtuelle », Electronic check (e-check),http://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/internet/fiches/8370849.html

**104. OCDE,** http://data.oecd.org/fr/ict/investissement-dans-les-tic.htm#indicator-chart

**105.** http://www.adeanet.org/adeaPortal/adea/newsletter/Vol11No2/fr_9.html

**106. SATIM**, www.satim.dz

**107. SSRI**, http://www.ssri.dz/la-cyber-securite-etat-des-lieux-en-algerie/

**108. U.S. Department of Justice**, http://www.justice.gov/

**109. U.S**.https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

**110.** http://www.uncjin.org

**111.** www.erudit.org

**112.** http://abbinvest.com/index.php?page=blog&var=18

**113.** http://blogues.radio-canada.ca/triplex/2014/12/22/2015-montee-des-attaques-cybernetiques/

**114.** http://frenchweb.fr/5-monnaies-virtuelles-alternatives-au-bitcoin/153443

**115.** http://lci.tf1.fr/monde/moyen-orient/qui-est-le-pkk-bras-arme-des-kurdes-de-turquie-7764114.html.

**116.** http://openclassrooms.com/courses/la-cryptographie-asymetrique-rsa/rsa-qu-est-ce-donc

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

**118.** http://www.altospam.com/glossaire/scam.php >

**119.** http://www.arobase.org/arnaques/loteries.htm

**120.** http://www.banque-info.com/lexique-bancaire/c/carte-de-crédit

**121.** http://www.cairn.info/zen.php?ID_ARTICLE=EMR_129_0110 >

**122.** http://www.certissim.com/fraude.html

**123.** http://www.clusif. asso.fr

**124.** http://www.comscore.com/fre/actualites_et_evenements/Press-Releases/2012/2/The-Netherlands-and-France-Have-the-Highest-Penetration-of-Online-Banking.

**125.** http://www.comscore.com/fre/actualites_et_evenements/Press-Releases/2012/2/The-Netherlands-and-France-Have-the-Highest-Penetration-of-Online-Banking >

**126.** http://www.cyberlex.org/

**127.** http://www.eBay.com

**128.** http://www.hackerwatch.org

**129.** http://www.internetsanscrainte.fr/s-informer/quest-ce-quun-spam

**130.** http://www.itpro.fr/a/cheques-electroniques/

**131.** http://www.latribune.fr/technos-medias/informatique/20130416trib000759796/cyber-criminalite-les-nouvelles-techniques-d-attaques-toujours-plus-perfectionnees-et-redoutables.html.

**132.** http://www.lenetexpert.fr/la-chaine-tv5-monde-victime-dun-piratage-de-grande-ampleur-par-des-individus-se-reclamant-du-groupe-etat-islamique-le-net-expert-informatique/

**133.** http://www.leparisien.fr/economie/votre-argent/fraude-a-la-carte-bancaire-une-perte-de-513-millions-en-france-22-04-2015-4714959.php#xtref=https%3A%2F%2

**134.** http://www.phsihing-initiative.com

**135.** http://www.pointdecontact.net/partenaires/oclctic

**136.** http://www.senate.be/www/?MIval=/publications/viewPub.html&COLL=S&LEG=5&NR=1497&VOLGNR=1&LANG=fr

**137.** http://www.signal-spam.fr

**138.** http://www.zdnet.fr/actualites/le-groupe-petrolier-aramco-cible-d-une-cyberattaque-l-acte-d-activistes-39775459.htm

**139.** https://halshs.archives-ouvertes.fr/halshs-00199011

**140.** https://www.google.fr/#q=new+hacker%27s+dictionary+pdf

**141.** https://www.securiteinfo.com/attaques/hacking/dos.shtml

**142.** www.carrefourdalgerie.com/archive/pdf/2013/05/18-05-2013.pdf

# - LISTE DES TABLEAUX -

## CHAPITRE I



## CHAPITRE II



## CHAPITRE III

## *LISTE DES FIGURES*

### CHAPITRE I



### CHAPITRE II

**CHAPITRE III**



## ***LISTE DES SCHEMAS***

**CHAPITRE I**

# - Table des matières -

## Résumé

Les progrès fulgurants réalisés dans les technologies de l'information et de la communication (TIC), ces dernières années, ont imposé un nouvel espace d'échange où circulent des flux d'informations numériques, avec le libre accès, dans lequel s'effectuent tous types de transactions et prestations électroniques. La mise à disposition sur le web de nombreux outils et services s'adressant à la population mondiale, a rendu leurs utilisations vulnérables aux infections de logiciels malveillants et à conduit à la croissance d'actes cybercriminels.

La cybercriminalité est une activité lucrative qui traverse les frontières. Ainsi les efforts de l'Algérie dans la numérisation de ses infrastructures sans politique de sécurité pour l'accompagner, l'a exposé aux risques informatiques. Dans ce cadre, l'initiative de l'Algérie a été de promulguer des lois qui réglementent et encadrent ce genre de délinquance, Mais serait-elle suffisante ? Ne devrait-elle pas suivre ce progrès d'une politique plus appuyé de sécurité ? Qu'a fait l'Algérie dans ce secteur, mise à part le petit texte de loi qui ne couvre pas tous les aspects de la cybercriminalité?



Mots clés : cybercriminalité, risques informatiques, logiciels malveillants, TIC.



## Abstract

The rapid progress made in the information and communications technology (ICT) in recent years have imposed a new exchange space where circulate digital information flow, with free access in which to perform All types of transactions and electronic services. The availability on the web of many tools and services addressing the world's population, reported their use vulnerable to malware infections and leads to the growth of cyber criminals acts.

Cybercrime is a lucrative business that crosses borders and Algeria's efforts in modernizing and digitizing its security policy without infrastructure to accompany him, was exposed to IT risks. In this context, the initiative of Algeria was to enact laws that regulate and supervise this kind of crime, but would it be enough? Should it not take this progress a more pressing security policy? What did Algeria in this sector, apart from the small piece of legislation that does not cover all aspects of cybercrime?



Key word : Cybercrime, IT risks, malware infections, ICT.

# - GLOSSAIRE -

- **Attaque informatique** : terme générique désignant une action malveillante dont la cible ou le moyen est l'informatique et qui génère un dommage ou un préjudice. Le plus souvent, l'intrusion est facilitée par une vulnérabilité dans le logiciel ou le système de sécurité, qu'exploite l'agresseur aux fins d'installer un programme malware, qui soit récupère et transmet les données pour lesquelles il a été programmé (mots de passe, données personnelles, éléments de propriété littéraire et artistique, secret des affaires, analyse du réseau ou du système, écoute des communications) ou développe une autre attaque interne, à des fins par exemple, de blocage ou de sabotage. Le point d'attaque se situe ordinairement dans le terminal (ordinateur, téléphone portable et bientôt tout objet connecté), mais il peut aussi être dans le centre de données lui-même, ou dans le réseau.

- **Bitcoin** : monnaie virtuelle mise au point par un japonais en 2009, hautement spéculative et non contrôlée par une banque centrale ; certains délinquants l'utilisent pour le blanchiment d'argent.

- **Botnet** : réseau d'équipements compromis (ordinateurs, serveurs, ordiphones, etc.) par des logiciels malveillants à l'insu de leur propriétaire et dirigé à distance par un pirate informatique malveillant ("le maître"). Ce réseau est structuré de façon à permettre à son propriétaire de transmettre des ordres à tout ou partie des machines du botnet et de les actionner à sa guise, par exemple pour envoyer des courriers électroniques non désirés, pour lancer des attaques par déni de service, voire pour voler des informations. Certains réseaux peuvent porter atteinte plusieurs millions de machines.

- **Carding** : trafic de données de cartes de paiement négociées par le commerce en ligne sur des forums sécurisés, qui échangent des données bancaires entre organisations criminelles (carder = trafiquant de cartes bancaires).

- **Cheval de Troie** : dans le domaine informatique, il s'agit d'un programme malveillant, en apparence inoffensif, contenant une fonction illicite cachée et connue du seul attaquant, qui permet à ce dernier de prendre le contrôle de la machine compromise (=infectée) et de s'en servir à l'insu du propriétaire. Le plus souvent, ce programme est introduit sans qu'il le sache par l'utilisateur lui-même, via un jeu vidéo ou un petit utilitaire.

- **Cracker** : logiciel qui égrène les mots de passe jusqu'à ce qu'il trouve le mot valide ; l'expression désigne aussi un programme spécialisé dans le "cassage" des codes, mots de passes ou de protection de logiciels.

- **Cyberdéfense** : ensemble des mesures techniques et non techniques permettant à un Etat de défendre, dans le cyberespace, les systèmes d'information jugés essentiels.

- **Cyberespace** : espace de communication constitué par l'interconnexion mondiale d'équipement de traitement automatisé de données numériques.

- **Cybersécurité** : état recherché pour un système d'information lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la disponibilité,

l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

- **DoS (Distributed denial of service)** Déni de service : action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu, le plus souvent en le submergeant de Spams.

- **Enregistreur de frappe** (keylogger) : logiciel ou matériel employé par un utilisateur malveillant pour capturer ce qu'une personne saisi à partir de son clavier.

- **Escroquerie à la nigériane :** forme d'escroquerie en ligne basée sur l'envoi d'un courriel à la victime qui l'incite à effectuer un transfert d'argent dans l'espoir d'un gain substantiel ; il peut s'agir soit d'une donation, soit d'un héritage, soit même d'un gain à une loterie, bien sur fictifs, pour l'obtention desquels on demande à la victime d'adresser de l'argent en Afrique ou en Espagne, le plus souvent par mandat cash Western Union.

- **Firewall** (**Pare-feu)**: un pare-feu est un logiciel ou un équipement permettant de protéger un ordinateur ou un ensemble d'ordinateurs connectés à un réseau ou a! Internet. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant) initialisées par des programmes ou des personnes.

- **Hacker** : pirate informatique ; personne s'essayant de s'infiltrer dans un système informatique sécurisé en utilisant les faiblesses technologiques de ce système ; on distingue couramment les "hackers blancs", qui ne sont pas animés de capacités de nuire, et les "hackers noirs" qui sont malveillants.

- **Hameçonnage (Phishing)** : technique d'ingénierie sociale utilisée par les escrocs pour soutirer des données personnelles (codes d'accès, mots de passe, codes de cartes bancaires...) à leur victime en se faisant passer pour un tiers de confiance (administration, banque, CAF, E-Bay, Pay-Pal...). Cette technique doit son nom au fait que ces fausses pages WEB concernant soit disant des organismes de confiance sont envoyées à des milliers de victimes potentielles, parmi lesquelles une minorité accepte de saisir le n/ à 16 chiffres de leur carte de crédit ainsi que le cryptogramme à trois chiffres utilisé au dos de cette carte et leur identité complète ; ces données sont alors utilisées par l'escroc pour faire des achats en ligne ou pour encoder des cartes bancaires vierges, revendues sur les forums spécialisées pour être ensuite utilisées dans les commerces.

- **Ingénierie sociale** (social-engineering) : il s'agit de la technique mise en œuvre par des escrocs pour collecter et traiter de l'information ciblée, le plus souvent cerner l'environnement de leurs victimes potentielles, avant de passer à l'acte ; cette technique peut être parfois très élaborée, notamment dans le cadre des escroqueries par faux ordres de virement, qui sont précédées d'une phase de recueil de renseignements sur Internet concernant la société cible, les pratiques et les identités de ses dirigeants, leur environnement professionnel, puisqu'il s'agit ensuite de manipuler un interlocuteur bien positionné et susceptible de déclencher des ordres de virement de manière expresse.

- **IP ou internet protocole** : la communication sur Internet est fondée sur un protocole appelé IP pour internet protocole qui permet aux ordinateurs de communiquer entre eux. Ce protocole utilise des adresses numériques pour distinguer ces machines et tronçonne la

communication en paquets comportant chacun une adresse de source et une adresse de destination. Ce n/ IP unique permet d'identifier un ordinateur connecté sur le réseau Internet, mais non celui qui l'utilise.

- **Logiciel malveillant** (malware) : tout programme développé dans le but de nuire a! ou au moyen d'un système informatique ou d'un réseau. Les virus, les vers ou les « chevaux de Troie » sont des types de codes malveillants. Ce logiciel est ainsi implanté dans un ordinateur à l'insu de son propriétaire.

- **Peer to peer** : réseau permettant à plusieurs ordinateurs d'être directement connectés entre eux via le réseau Internet afin de pouvoir échanger directement des fichiers sans passer par un serveur.

- **Pharos** : plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements relatifs aux contenus ou activités illégales, émanant des internautes ou de professionnels ; il s'agit d'un dispositif interministériel géré par l'O.C.L.T.I.C.

- **Sécurité des systèmes d'information (SSI)** : ensemble des mesures techniques, organisationnelles, juridiques et humaines permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

- **Spam (Pourriel)** : tout courrier électronique non sollicité par le destinataire, envoyé souvent de manière massive et répétitive dans un but commercial ou frauduleux.

- **STAD** (système de traitement automatisé de données) : ensemble composé d'une ou plusieurs unités de traitement automatisé de mémoires, logiciels ou données, protégé ou non par un système de sécurité.

- **URL** (Uniform Resource Locator) : adresse internet ou localisation physique d'un fichier ou d'une ressource sur internet. Une URL est constituée de quatre éléments : le protocole de communication d'abord (http:// pour les pages web), ensuite le nom de domaine du site, le répertoire ou le sous-répertoire du site dans lequel est enregistré le document, et enfin le nom du fichier et son extension. L'URL constitue le moyen d'identification et le chemin d'accès à toute ressource internet.

- **Ver** : logiciel malveillant indépendant, utilisant les réseaux à la recherche des failles de sécurité lui permettant de se répliquer de machine en machine ; il perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs. Les vers sont des catégories de virus, qui se propagent de manière quasi-autonome et dont le vecteur primaire de propagation reste le réseau. Ils peuvent être également transmis par clé USB.

- **Virus informatique** : programme informatique malveillant dont le but est de survivre sur un système informatique (ordinateur, serveur, appareil mobile, etc.) et souvent d'en atteindre ou d'en parasiter les ressources (données, mémoire, réseau). Il provoque une perte d'intégrité des ressources ainsi qu'une dégradation, voire une interruption du service fourni.

- **Zombie** : équipement informatique (ordinateur, serveur, etc.) compromis inclus dans un réseau (botnet) contrôlé par un individu malveillant.