UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
FACULTE DES SCIENCES ECONOMIQUES, COMMERCIALES ET DES SCIENCES DE GESTION
DEPARTEMENT DES SCIENCES DE GESTION

Mémoire de fin d'étude

En vue de l'obtention du diplôme de master en Science de Gestion

Spécialité : Management Bancaire

Thème

La cybercriminalité dans le secteur bancaire Cas : Banques de la wilaya de Tizi-Ouzou

Présenté par :
ABELLA Aini
BAZIZ Samira

Rapporteur :
AKSIL Kayssa

Devant le jury composé de :

- **Présidente : BOUREKKACHE Feroudja. M.A.C.A .UMMTO.**
- **Examinatrice : BELADEL Amina. M.A.C.A .UMMTO.**
- **Rapporteur : AKSIL Kayssa. M.A.C.A. UMMTO.**

Promotion *2017/2018*

Remerciements

C'est avec modestie et gratitude que nous reconnaissons ce que nous devons :

Nous commençons par remercier et rendre grâce à Dieu le tout puissant de nous avoir donné le courage et la volonté de mener à bon terme ce travail.

Ainsi nous tenons à remercier notre promoteur M^me^: Aksil qui a su nous guider et nous orienter.

Nous tenons aussi à remercier tous les enseignants du département de Science de gestion option management Bancaire sans exception.

Nous tenons à remercier également nos enseignants de différentes phases d'enseignement.

Nous traduisons par la même occasion à remercier tous ceux qui nous ont aidés de prés ou de loin à la réalisation de ce travail surtout aux personnels de la sureté de la wilaya et du cyber « Le Bon Coin », il n'y a pas de place pour les citer que dans le cœur.

A tous, nous exprimons notre vive gratitude.

Dédicaces

Je dédie ce modeste travail

En premier lieu à ma très chère mère qui m'a toujours soutenu dans mon parcours d'étude.

À l'hommage de mon très cher père et frère Nordine que j'adore et que le bon dieu aie leur âmes.

Mes grands remerciements à mon époux qui m'a vraiment soutenu, et qui a toujours su me comprendre.

À mes adorables petits neveux Nordine, Elena,Youva, Bilou,Ameyes

À mon cher frère Salem et sa petite famille.

À mes très chères sœurs : fazia ; hassina,fatima ,Djamila et leur petite famille.

À mes beaux-parents : Abderahmane et Saliha

À mes beaux-frères : Omar et Mustapha

À ma chère Nawel et ses parents : Nacera et Tahar qui m'ont vraiment aidé.

À mes cousins et cousines.

À ma voisine messaad et sa petite famille.

À toutes mes amies surtout kamelia ; Thileli ; Samira; Nawel; Thiziri; Sarah; Nadjwa, Adel, Ahcene et tous mes collègues de travail de l'EPH L.N.I : Lydia, Aldjia, Fadhila et Dr Ould Saada.

À tous mes camarades de ma section surtout Imane (Management Bancaire)

À ma binôme Samira et sa famille.

À toutes les personnes qui m'estiment.

AINI

Dédicaces

Je dédie ce modeste travail

À mes parents qui m'ont toujours soutenu dans mon parcours d'étude.

À ma sœur Malika et sa petite famille : Salem, Lamia, Hakim, et le petit Aziz

A ma sœur Dalila et sa petite famille : kamel, Anis, Juba et Rayane.

À mon cher frère Mustapha.

A mes fréres : Rezak, Djimou,Malik.

Ama belle-sœur nadia et sa famille.

À mes cousins et cousines.

À toutes mes amies Thileli; Sabrina; Sandra; Farida, Wassila, Djahida

À tous mes amis : Rabah, Rezki, Yacine, Abdou, Hocine

À tous mes camarades de ma section (Management bancaire surtout Imane et Rabea)

À ma binôme Aini et sa famille.

À tous ceux qui me connaissent de prêt ou de loin.

Samira

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

Albert EINSTEIN.

Sommaire

Abréviation……..III

Glossaire……V

Introduction générale…….……12

Chapitre 1 : L'émergence des TIC et la naissance de la cybercriminalité……18

Section1 : Les NTIC une 3e révolution…….20

Section2 : La cybercriminalité une 3e grande menace……..40

Chapitre 2 : La banque face aux aléas de la cybercriminalité……62

Section 1 : Les failles de sécurité dans le secteur bancaire et financier……63

Section 2 : Les activités de veille pour lutter contre la cybercriminalité……..85

Chapitre 3 : La cybercriminalité en Algérie……...102

Section 1 : Algérie face au phénomène de la cybercriminalité……...103

Section 2 : Interprétation des résultats de l'enquête……122

Conclusion générale……..146

Bibliographie…….150

Tables des figures, tableaux, schémas et annexes……..155

Annexe……160

Tables des matières……...181

Listes des sigles et abréviations

Abréviations	Significations
ABC	Arab Banking Corporation
ACPR	autorité de contrôle prudentiel et de résolution
ADSL	Asymmetric Digital Subscriber Line
AGB	Arab Gulf Bank
ANSS	Autorité de contrôle prudentiel et de résolution
AT&T	American Téléphone & Télégraphe
BA	Banque d'Algérie
BADR	Banque de l'Agriculture et du Développement Rural
BB	Baraka Bank
BEA	Banque Extérieur d'Algérie
BNA	Banque Nationale d'Algérie
BNPP	Banque Nationale Paris Paribas
BDL	Banque de Développement Local
C B	Carte Bancaire
C I A	Central, Intelligence, Security
CD	Disque Compact
CRD	Capital Requiement Directive
C2C	Customer to Customer
CCP	Centres de Chèques Postaux
CE3	Centre Europeen3
CI	Contenus Illicites
CIB	Carte Interbancaire
CIRFU	Cyber Initiative and Ressource Fusion Unit
CNEP	Caisse Nationale d'Epargne et de Prévoyance
COS	Center,Organisation,Security
CPA	Crédit Populaire Algérie
CSI	Computer Security Institute
CSIRT	Computer Security Incident Response Teams
CSIS	Center for Strategic and International Studies
DAB	Distributeurs Automatique de Billets
DVD	Digital, Versatile, Disc
DVD	Disque, Numerique, Polyva
E C 3	Centre Europeen 3
E M V	E uropay, Mastercard ,Visa
EDI	Échange de Données Informatisé
EMV	Europay, Mastercard,Visa
F B I	Federal, Bureau of Investigation
FAI	FRS d'accès à internet
FB	Facebook
FTP	File, Transfert, Protocol
GAB	Guichet Automatique de Billets
GAFI	Groupe d'Action Financière,
I S O	Organisation International de Normalisation
IARPA	l'Intelligence Advanced Research Projects Activity
IBM	International Business Machine
IDI	Indice de Développement des TIC
IP	Internet Protocol
IUT	**U**nion **I**nternational de **T**élécommunication
LIL	Loi Informatique et Libertés
LOPPSI	loi d'orientation et de programmation, pour la performance de la sécurité intérieure
NCA	**A**gence **N**ationale de la **C**riminalité
NCFTA	**N**ational **C**yber **F**orensics **T**raining **A**lliance
NCFTA	National Cyber Forensics Training Alliance
NTIC	**N**ouvelle **T**echnologies de l'**I**nformation et de **T**élécommunications

OCDE	***O**rganisation pour la **C**oopération et le **D**éveloppement **E**conomique*
OLF	*l'**O**ffice **Q**uébécois de la **L**angue **F**rançaise* *Internet **C**rime **C**omplaint **C**enter*
ONDRP	***O**bservatoire **N**ational de la **D**élinquance et des **R**éponses **P**énales*
P2P	*pair-à-pair*
PC	***P**ersonnel, **C**omputer*
PDA	*Personnel Digital Disc Assistant*
PIB	***P**roduit **I**ntérieur **B**rut*
PIN	***P**ersonal **I**dentification **N**umber*
PMA	***P**ays **M**oins **A**vancé*
RSSI	*responsable de la sécurité des systèmes d'information*
SATIM	***S**ociété d'**A**utomatisation des **T**ransactions **I**nterbancaires et de **M**onétique*
S G C B	*Secrétariat General de la Commission Bancaire*
SG	*Société Générale*
S I	*Système d'Information*
SICB	***S**ystème d'**I**nformation **C**artes **B**ancaires*
TCP	***T**ransmission **C**ontrol **P**rotocol*
TPE	***T**erminaux de **P**aiement **E**lectroniques*
TPV	***T**erminal, **P**oint de **V**ente*
TIC	*Technologie De l'Information et de la Communication*
U E	*Union Européenne*
URL	***U**niform **R**esource **L**ocator*
USDJ	***U**nited **S**tates **D**epart of **J**ustice*
V P N	*Virtual, Private Network*
WLL	***Wireless, Local, Loup***

GLOSSAIRE

Adresse IP : (Internet Protocol) : numéro qui permet d'identifié un ordinateur sur le réseau internet ou adresse numérique d'un ordinateur connecté à internet (ex : 121.128.55.203)

Adresse URL (Uniforme Ressource Locator) : adresse unique permettant de localiser une ressource ou un document sur internet avec la méthode pour y accéder. Le nom de serveur et le chemin à l'intérieur du serveur (Ex : http//www.entreprise .com./index.html)

Attaque informatique : Terme générique désignant une action malveillante dont la cible ou le moyen est l'informatique.

Attaque : Action malveillante qui tente d'exploiter une faiblesse dans le système et de violer un ou plusieurs besoins de sécurité

Bit : information représentée par un symbole à deux valeurs généralement notée 0 et 1, associée à deux états d'un dispositif.

Bombardement de courriels ("Mail Bombing") : Forme de déni de service contre les systèmes de messageries par l'envoi en grand nombre de courriels à un destinataire ciblé, dans une intention malveillante.

Bombe logique : partie de programme qui reste dormante dans le système hôte jusqu'à ce qu'un instant ou un événement survienne, ou que certaines conditions soient réunies, pour déclencher des effets dévastateurs en son sein.

Canular ("Hoax") : Information vraie ou fausse, souvent transmise par messagerie électronique ou dans un forum, et incitant les destinataires à effectuer des opérations ou à prendre des initiatives, souvent dommageables.

Capteur clavier, enregistreur de frappes ("Keylogger", "keystroke logger") : Logiciel ou matériel employé par un utilisateur malveillant pour capturer ce qu'une personne frappe au clavier.

Chantage ("Ransomware") : Forme d'extorsion imposée par un code malveillant sur un utilisateur du système. Si ce dernier refuse de payer ou d'effectuer une tâche imposée, le service auquel il veut accéder lui est refusé par le code malveillant.

Cheval de Troie : programme effectuant une fonction illicite tout en donnant l'apparence d'effectuer une fonction légitime ; la fonction illicite peut être de divulguer ou d'altérer des informations, ou peut être une bombe logique.

Chiffrement : Transformation cryptographique de données produisant un cryptogramme.

Code malveillant ("Malware", "Malicious software ") : Programme développé dans le but de nuire au travers d'un système informatique ou d'un réseau; chevaux de Troie, virus et vers sont des codes malveillants.

Contrefaçon : reproduction, usage, apposition ou un imitation d'une marque identique ou similaire à celle désigné dans l'enregistrement, sans l'autorisation du propriétaire ou du bénéficiaire du droit exclusif d'exploitation.

Crédit renouvelable : 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

Cyber attaque : Acte malveillant envers une cible informatique, généralement via un réseau de télécommunications.

Cyber défense : Ensemble des mesures permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

Cyber menace : Action menaçante locale ou à distance visant l'information ou le système d'information. Pêcher ou de limiter fortement la capacité d'un système à fournir le service attendu.

Cyber sécurité : État recherché pour un système d'information lui permettant de résister à des événements 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. La Cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une Cyber défense.

Cybercriminalité : "Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible."

DoS / DDoS : déni de service attaque d'un serveur destinée à l'empêcher de remplir sa fonction. Méthode classique : faire crouler le serveur sous une masse de requêtes généralement mal formées à dessein pour entraîner une réponse anormale et paralysante. L'attaque utilise très souvent une multitude de PC zombies travaillant de concert, infectés par des backdoors/chevaux de Troie et mobilisables à distance par un pirate. Il est aussi possible de bloquer à distance des routeurs en tirant parti de failles de leur software.

Espiogiciel ("spyware") : Logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations sur l'environnement sur lequel il est installé, sur les usages habituels des utilisateurs du système, à l'insu du propriétaire et de l'utilisateur.

Filoutage ou hameçonnage ("phishing") : Technique trompeuse visant à obtenir des renseignements personnels en abusant les détenteurs. Vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime.

Fournisseur d'accès internet (FAI) : intermédiaire entre l'internaute et le réseau internet.

Ingénierie sociale ("Social Engineering") :

Intrusion : faute opérationnelle, externe, intentionnellement nuisible, résultant de l'exploitation d'une vulnérabilité dans le système.

IP ("Internet Protocol") : Protocole de communication fondé sur des adresses numériques distinguant les machines connectées, segmentant la communication en paquets, et comportant une adresse IP source et IP adresse de destination lors d'une session.

Keylogger : enregistreur de frappe de touches de claviers qui sont ensuite adressées aux pirates agissant à distance.

Machine piratée ou ‘’zombie" : Machine compromise incluse dans un réseau ("botnet") contrôlé par un contrôleur de ce réseau de "zombies".

Manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes.

Menace : Violation potentielle d'une propriété de sécurité

Money mule : intermédiaire prêtant ses comptes aux cyber délinquants moyennant un pourcentage (Money muling).

Pare-feu ("Firewall") : Un pare-feu (ou garde-barrière) est un outil permettant de protéger un ordinateur connecté à un réseau ou à l'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.

Pirate informatique ("Hacker") : Individu s'introduisant dans un système informatique souvent par défi intellectuel, pas toujours par intention malveillante, ou par profit.

Porte dérobée ("Backdoor") : Accès logiciel ou matériel permettant à un individu de se connecter à une machine distante de façon furtive.

Pourriel : le spam, pourriel ou polluriel est une communication électronique non solliciter, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grandes quantités effectuées à des fins publicitaires.

Réseau de robots ("botnet") : Réseau de machines compromises conçu pour permettre la transmission des ordres à tout ou partie de ces machines et diriger une attaque déguisée en masse sur une seule ou sur plusieurs cibles déterminées par un système de commande et contrôle (C2) administré.

Reseau social : permet la mise en relation des personnes partageants les centres d'intérêts personnels ou professionnels (Faceboock, Twiter, Friendster, Linkdink…..)

Risque : Couple (menace, vulnérabilité

Sniffing (écoute passive) : accéder aux données transmises sur canal de communication (e.g., câble de réseau) stockée sur un support vulnérable (e.g., disques externes). Menace: accès à des informations sensibles, e.g., mot de passe d'un utilisateur tapé sur un terminal connecté à un ordinateur central, et qui transite en clair entre ce terminal et la machine.

Spamming : l'usage abusif d'un système messagerie destiné à exposer délibérément (et de manière répétée) les utilisateurs à des contenus non pertinents et non sollicités.

Spoofing (usurpation d'identité) : se faire passer pour quelqu'un d'autre afin de faire une action malveillante (e.g., envoi virus, spam, …)**Exemple :** • IP spoofing = utiliser l'adresse IP d'une machine, ou d'un équipement, afin d'en usurper l'identité.• Fishing : site miroir "contrefait" semblables à des portails de renom. Attirer internaute réellement client du site plagié.

Spyware : contraction de spy et software. Logiciel espion qui collecte des données personnelles avant de les envoyer à un tiers, e.g., Keylogger : transmettre les données saisies au clavier.

STAD (Système de Traitement Automatisé de Données) :ensemble composé d'un ou plusieurs unité de traitement automatisé de mémoires, de logiciels, de données, cette ensemble étant protégé ou non par un dispositif de sécurité.

Système informatique : il s'agit de l'ensemble de matériels et de logiciels ainsi que tout les moyens de télécommunications qui permettent d'automatisées les fonctions et les informations.

TCP/IP (Transmission Control Protocol Internet) : suite de protocole des noms des deux protocoles majeurs (TCP/IP). Il représente d'une certaine façon l'ensemble des regles de communications sur internet et se base sur la notion d'adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine de réseau afin de pouvoir acheminer des paquets de données.

Ver : programme autonome qui se reproduit et se propage à l'insu des utilisateurs

Virus : segment de programme qui, lorsqu'il s'exécute, se reproduit en s'adjoignant à un autre programme (du système ou d'application), et qui devient ainsi un cheval de Troie ; Propriétés : infection, multiplication, fct nocive

VPN Virtuel Net Work : (Réseau Privé Virtuel) : réseau invisible des autres utilisateurs connectés.

Vulnérabilité : faiblesse / faille : faute accidentelle ou intentionnelle introduite dans spécification, conception ou configuration du système.

Web : expression employée pour la premiere fois en 2005 par M.Tim. OREILLY por désigner une mutation du Web statique (1.0) vers un Web participatif dit social dans le lequel l'internaute devient fournisseur d'information.

Zombie : ensemble de machine compromise, contrôler à distance par un pirate informatique.

Depuis l'existence humaine chaque siècle marque une révolution importante ; comme la fin du moyen âge a vue celle de l'imprimerie, le 19e siècle voit la consécration des technologies numériques. Cette révolution contemporaine est notamment liée à la structure même d'internet et de l'espace virtuel qu'il génère, « le cyberespace ». Ce dernier est communément défini comme un ensemble de données numérisées constituant un univers d'information et de communication lié à l'interconnexion mondiale des ordinateurs, plus précisément est défini comme « *un ensemble de réseaux commerciaux, réseaux publics, réseaux privés, réseaux d'enseignements, réseaux de services qui opèrent à l'échelle planétaires* »[1] .

L'ère numérique ignore désormais toutes les frontières. Elle permet l'accès à la culture et à la connaissance ; favorise les échanges entre les personnes. Elle rend possible la constitution d'une économie en ligne et rapproche le citoyen de son administration. Les technologies numériques sont porteuses d'innovation et de croissance en même temps qu'elles peuvent aider ou accélérer le développement des pays émergents[2].

Les progrès fulgurants des Technologies de l'Information et de la Communication (TIC) ont conduit à l'introduction de concept moderne de '' société de l'information'', ce dernier est un modèle de société qui lui permis d'avoir un libre accès à l'information, la retirer des mains de pouvoir central et 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-sante, etc. Autant d'exemple pour montrer que les TIC sont une partie intégrante de notre quotidien[3].

Mais un certain pessimisme vient tempérer cette approche idéaliste. Tous les progrès génèrent aussi de nouvelles fragilités et vulnérabilités propices aux menaces ou aux risques, car ils aiguisent l'imagination des criminels.la cybercriminalité est désormais une réalité.

En 1972, le doyen Jean CARBONNIER affirmait déjà que *« l'évolution des mœurs et des technologies donne naissance à de nouvelles formes de délinquance »*[4].

En effet la plupart des grandes découvertes technologique ont « *presque toujours engendré, à cote des progrès économiques qu'elles procurent à l'humanité, des retombes*

[1] LEBERT M.F « *de l'imprimerie à l'internet* » thèse de doctorat, Paris, 1999.

[2] BOOS Romain « *lutte contre cybercriminalité au regard de l'action de l'Etat* » thèse de doctorat, univ de LORRAINE, Paris, 2016

[3] BELATTAF Sylia « la cybercriminalité: l'Algérie est-elle suffisamment outillée ?le cas des banques algériennes », univ Abderrahmane Mira Bejaia, 2014-2015.

[4] CARBONNER(J), « sociologie juridique », éd. A. Colin, 1992, ed.PUF, collthemis, Paris, 1978, refondue coll. Quadrige, (1994) et (2004).

négatives parmi lesquelles figure en bonne place l'avènement de nouvelles formes de criminalités. Internet n'échappe pas à cette loi sociologique du développement »[1].

Selon le général d'armée Marc Watin AUGOUARD

> « *Lorsque le développement économique se limitait au secteur primaire agricole l'insécurité se résumait aux atteintes contre les personnes. Le secteur secondaire a vu l'apparition de la production de biens manufacturés donc de vols, destructions, dégradations. Le développement du secteur tertiaire des services a inspiré les infractions dites ''intelligentes''»* [2].

Avec l'apparition d'un nouveau secteur quaternaire de l'économie ou' l'information est devenue une source de la richesse, la cybercriminalité est devenue désormais une réalité. Elle se joue des frontières entre les Etats, rapproche la victime de son agresseur mais éloigne le délinquant de son juge.

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[3], 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[4].

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[5].

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.

---

[1] GASSIN(R), « le droit pénal de l'informatique », DS, éd Chron, 1986, p.35.
[2] WATIN AUGOUAR(M), préface du livre « cybercriminalité défi mondial »VII.
[3] Article sur les enjeux de la cybercriminalité, paru en juillet 2009 par EL AZZOUZI Ali, page1.
[4] KASPERSKY Eugene, « *Cybercriminalité, une guerre perdue ?* », documentation française, article n°6 sécurité globale, défis de la cybercriminalité, hiver 2008-2009 ; France ; PP.18.1
[5] http:// www.ssri.dz la-cyber-sécurité-état-des-lieux-en-Algérie/; 2014, consulté le 24/04/2018

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[1]. Statistiquement la cybercriminalité a engendrée un préjudice estimé à «1000 *milliard de dollars en 2008, soit environ 1,64% du PIB mondial. Ces coûts devraient passer à plus 2100 milliards de dollars d'ici 2019 »*[2]. Cela a même dépassé pour la première fois les recettes du marché illégal de stupéfiants.

L'insécurité liée au web engendre de lourds 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 et de fraude pour les banques qui sont totalement noyées dans la transformation digitale et dans la démocratisation d'internet. Ces estimations montrent clairement qu'il est vital de protéger les infrastructures de l'information et de garantir le bien-être économique et la sécurité, en élaborant des stratégies de prévention qui doit être une partie intégrante des stratégies nationales de « *Cyber sécurité* ».

- **Le choix du thème**

Nous avons choisi ce thème dans le but de faire comprendre et éclaircir certaines notions liées à la cybercriminalité dans le secteur bancaire ainsi l'état des lieux de ce phénomène en Algérie. Ce qui nous a incités de choisir un tel thème est que c'est :

1. Un thème qui n'a pas été déjà traité au sein de notre faculté.
2. Un thème d'actualité influençant la finance de tout pays même où le système financier n'est pas développé (comme l'Algérie) ;
3. Absence de confiance numérique ;
4. Sensibiliser les autorités publiques, les banques et tout étudiant et enseignant sur le risque engendré par le phénomène et les encourager à s'impliquer dans une cyber-sécurité sur l'échelle nationale pour prévenir et lutter contre son émergence.

- **Problématique**

A la lumière de ce qui précède, nous avons illustrés notre problématique, en se posant la question suivante :

[1] Commission européenne-affaire intérieures-la cybercriminalité-avril 2012, page.1. Voir le lien www.ec.europa.fr consulté le 14/042018

[2] Etudes réalisées par l'éditeur d'antivirus McAfee, présenté au « forum économique mondial de Davos (suisse). Des éléments ont été recueillies auprès de plus de 800 responsables au Japon, en Chine, en Inde, au Brésille, en Grande Bretagne, à Dubaï, en Allemagne et aux Etats Unis. lien www.McAfee.fr consulté le 14/042018

Face à l'infiltration massive du phénomène de la cybercriminalité dans l'ensemble du système économique et financier, les banques allouent-elles les dispositifs de sécurité nécessaires pour renforcer leur activité de veille et faire face à cette menace ?

Pour bien cerner notre problématique, nous somme amenées à détailler cette question centrale par quelques questionnements dont l'importance est évidente à savoir :

- En quoi les technologies de l'information et de la communication permettent-elles des dérives délictueuses et criminelles ?
- Qu'est-ce que la cybercriminalité ?
- Pour quoi la cybercriminalité est considérée comme un risque systémique pour la banque ?
- Quelles sont les failles de sécurité qui favorisent la cybercriminalité dans le système bancaire ?
- Qu'en est –il du cas de l'Algérie et des banques algériennes ?

- **Les hypothèses**

1. Admettant que, l'émergence d'une 3^{e} révolution (TIC) a mené à l'avènement d'une 3^{e} grande menace (*cybercriminalité*) ;
2. L'ingéniosité grandissante des cyber-délinquants pousse la banque à renforcer son activité de veille et d'innover d'avantage dans le domaine de cyber-sécurité ;
3. Le retard dont est victime l'Algérie en matière d'introduction et d'utilisation des TIC serait la raison de la faible exposition de notre pays au phénomène de cybercriminalité.

Pour valider ou invalider ces hypothèses, nous baserons notre travail sur des études déjà réalisées sur la question, et nous allons les compléter par une étude sur le terrain.

- **Méthodologie**

La réponse à ces questions pourrait permettre de mieux comprendre le phénomène qui s'illustre sous deux volets :

Le premier est d'ordre théorique, élaborée sur la base d'une revue bibliographique utilisant des ouvrages, articles, documents, mémoires et thèses ; pour savoir ce qui a été écrit sur la cybercriminalité et ses aléas sur le secteur bancaire, dans le but d'assurer la qualité du questionnement ;

Le second est d'ordre pratique qui consiste à faire une enquête sur le terrain basée sur des questionnaires et des entretiens en s'adressant aux banques publiques et privés implantées à la wilaya de Tizi-Ouzou en premier lieu et aux autorités concernées qui ont le pouvoir de lutter contre la cybercriminalité en deuxième lieu.

L'objectif de cette enquête est d'analyser et comparer le degré d'exposition de ces banques et l'ensemble de la communauté tizi ouizienne à ce phénomène. Pour ce faire, notre travail consiste à déposer les questionnaires au niveau de ces agences bancaires pour être rempli et faire des entretiens avec les responsables. Cette technique est très utile car elle permet à notre étude de se baser sur des données fiables et va nous aider dans la récolte des informations nécessaires pour notre travail.

Pour mener à bien notre recherche, nous allons structurer notre travail en trois chapitres :

Le premier chapitre sera consacré essentiellement à l'émergence des TIC et la naissance de la cybercriminalité selon deux points : après avoir donné quelques notions sur les TIC; leur état des lieux et enfin leur avantages et risques, nous allons procéder à la démystification du phénomène de cybercriminalité, en retraçant d'abord un historique de son évolution ; ensuite en déterminant les motivations diverses qui poussent les cybers délinquants à agir et enfin son impact sur l'économie mondiale.

Le second chapitre traite l'action de la banque pour lutter contre la cybercriminalité et s'organise autour de deux points : en premier lieu on a scindé les différentes infractions cybercriminelles classées selon l'IUT dans le système bancaire, puis nous citons les différents dispositifs de sécurités appliqués par les banques afin de renforcer son activité de veille.

Dans le troisième chapitre, il est question d'analyser la place de ce phénomène en Algérie, ainsi on a procédé à l'étude et l'analyse des différents résultats obtenus dans notre recherche.

Introduction

Dès les dernières décennies du second millénaire, l'humanité est entrée dans l'âge de l'information et de la connaissance numérique. Cette ère se caractérise par la mondialisation de l'économie et l'avènement des technologies de l'information et de la communication (*TIC*), qui sont considérés comme les moteurs de la nouvelle économie. C'est la naissance d'un nouvel ordre mondial de l'information et de l'économie. Il y a quelques années, on les appelait encore les '' *nouvelles technologies de l'information et de la communication''* (*NTIC*).[1]

Les technologies de l'information et de la communication ont bouleversé notre vie quotidienne. Les téléphones fixes ou mobiles, les ordinateurs et leurs périphériques (*Imprimerie, Scanner, etc.),* les logiciels, les appareils photo, les téléviseurs, font tous partie des TIC qui permettent de produire, transformer ou échanger de l'information en quantité importante en temps réel ou dans des délais très courts. Le rapprochement de l'informatique et des télécommunications bénéficièrent de la miniaturisation des composantes ; le meilleur exemple, à cet égard, est l'internet qui est devenu accessible sur le téléphone portable. Ce réseau reflète bien cette idée de « *Village Global* », de circulation de flots continus d'information, de communication instante (*Urgente et Pressante*) et instantanée (*Immédiate*) amenant ainsi la notion d'interdépendance.

L'importance des TIC n'est pas les technologies en soi, mais leur capacité à donner accès à la connaissance, à l'information et aux communications, qui sont autant d'élément qui comptent chaque jour davantage dans les interactions économiques et sociales d'aujourd'hui.

Le secteur financier, dont les métiers reposent essentiellement sur la gestion de l'information, se situe à l'épicentre de ces mutations.[2] Au cours des 10 dernières années, les banques ont dû faire face à une révolution technologique rendant indispensable une adaptation rapide des structures, systèmes et mentalités. Leurs évolutions sont conditionnées par la présence d'une clientèle, sans cesse plus exigeante.

Davantage équipée et familiarisée avec ces nouvelles technologies dans sa vie professionnelle et personnelle, elle attend de ses partenaires banquiers des réponses, adaptées rapidement communiquées, sur les appareils qu'elle possède *(BADOC, LAVAGSSIERE, COPIN, 1998).*

[1] BOULENOUAR Nassima Ouarda, « *Les nouveaux supports de communication TIC : facteurs de différentiation dans l'activité bancaire* », mémoire de magister, UNIV d'ORAN, 2014.

[2] Le prix Nobel Stock et Scholes ont démontré que le prix d'une option sur actions ne représentait que la valeur des informations connues.

> « *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).*

Il y a 20 ans, les clients n'étaient pas en prise directe avec le système informatique des banques, la relation bancaire se faisant alors essentiellement en agence, par l'intermédiaire d'un conseiller. La démocratisation d'internet, puis des Smartphones, a bouleversé la donne, les consommateurs s'enthousiasmant pour les services en ligne. A la société générale, pas moins que 86% des contacts entrants entre les clients et la banque, passent désormais par les canaux digitaux. Les banques ont donc été obligé d'ouvrir une partie de leur système informatique à leur client et prospects, ce qui a « *augmenté de façon considérable les risques de fraude* »,avait reconnu Bruno DELAS, « *Chief Operating Officer* » des réseaux France à la société générale.[1] Cette transformation digitale a engendré la multiplication d'attaques informatique contre les banques 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.[2]

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 et à près de 500 milliards USD en 2014.[5]

Afin de bien structurer ce chapitre, on a vu que c'est nécessaire de l'entamer par une première section dans laquelle on essayera de donner quelques notions et une vue générale sur les TIC dans le monde pour mieux comprendre l'influence de 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 décortiquer le phénomène de «*Cybercriminalité* » développé et rendu complexe avec l'évolution des TIC.

---

[1] www.latribune.fr « *Les banques face au défi de la cybercriminalité* ». Article rédigé par Christine LEJOUX 20/04/2016 consulté le 20/03/2018

[2] Sylia BELATTAF, « *La cybercriminalité : l'Algérie est-elle suffisamment outillée ?le cas des banques algériennes* » mémoire de master, UNIV Abderrahmane MIRA de BEJAIA 2014-2015.

[3] Observatoire National de la Délinquance et des réponses Pénales.

[4] Rapport de l'ONDRP, 2011. www.ONDRP.fr consulté le 20/03/2018

[5] Rapport de l'UIT, « *Comprendre la cybercriminalité : guide pour les PED* », UIT, 2009, page 14.

Section 1 : L'émergence des NTIC

En favorisant l'extension du commerce électronique, internet est désormais un des outils majeurs de cette mutation. La naissance de NTIC est due notamment à la convergence de trois activités : [1]

- Du domaine des télécommunications qui comprend le matériel et les équipements ;
- Du domaine de l'informatique qui comprend le matériel, service et logiciels ;
- Du domaine de l'audiovisuel qui comprend principalement la production et les services audiovisuels ainsi que l'électronique au grand public.

Les supports inhérents à ces NTIC sont incomptables parmi eux on peut citer : internet ; intranet ; extranet ; data warhose; knoweledge management; E-commerce; E-Learning…

Les TIC influencent tous les domaines notamment le domaine bancaire qui les utilise beaucoup plus dans les télécommunications, dans les moyens de paiements et même dans la fonction principale de service par la banque à distance. Dans les télécommunications on trouve la banque par fil(*le téléphone et le fax*) ; la banque par écran *(internet, extranet, et EDI*), comme instrument de paiement on trouve la télé compensation et la monétique, les DAB, GAB, TPE.

I /Définition et terminologies

I.1. Evolution de la terminologie

Après l'avènement de l'écriture puis l'apparition de l'imprimerie, les débuts d'une société de l'information ont été marqués par le télégraphe électrique, puis le téléphone et la radiotéléphonie, quant à la télévision, le Minitel et l'Internet puis la télécommunication mobile ont associé l'image au texte et à la parole, "sans fil". Sur le téléphone portable, qui sert aussi d'appareil photo, on a accès à l'Internet et à la télévision[2].

L'utilisation parallèle de l'informatique et des télécommunications, dans les années 90, a bénéficié de la miniaturisation des composantes ce qui a permis la production d'appareils «*Multifonctions* » à des prix raisonnables, dès la première décennie du 21ème siècle. L'influence des NTIC, et des réseaux en particulier, sur le secteur bancaire a commencé dans les années 70.

[1] Abdelkader RACHEDI(2003). « *Tic structure et comportement de l'homme dans l'entreprise* », thèse de doctorat ; UNIV de Abou Baker BELKAID, TLEMECEN, P8.

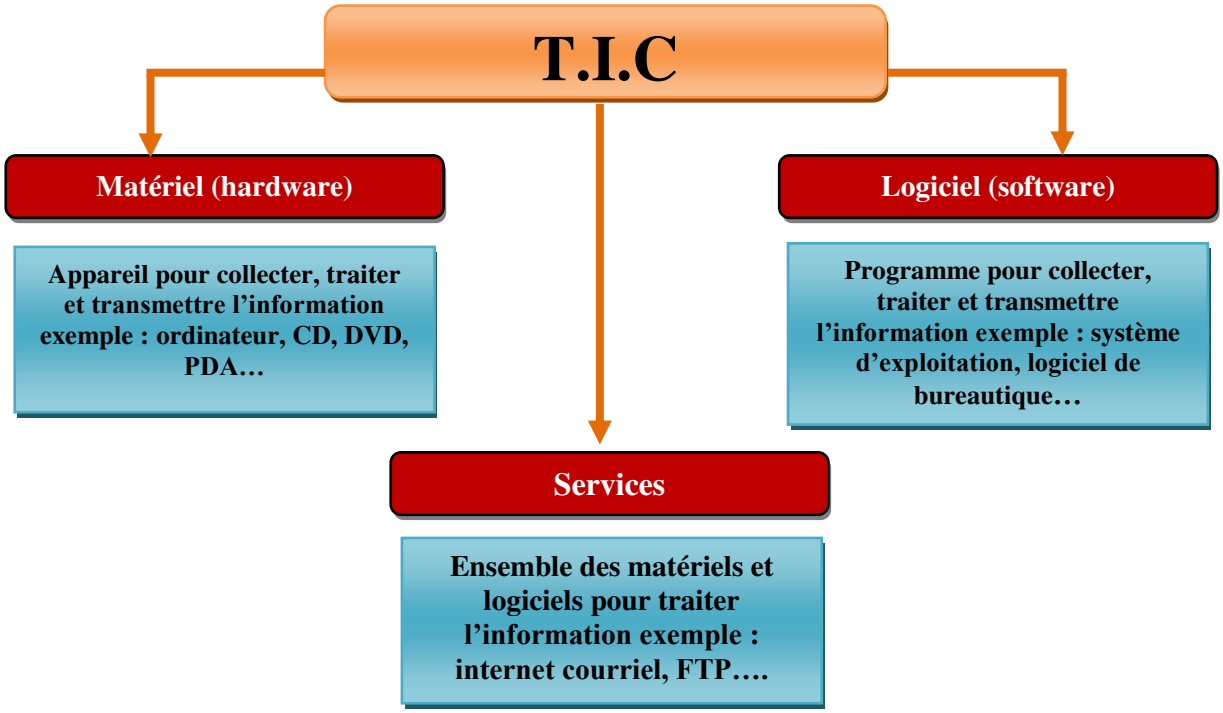
[2] BOUCHENOUA Karima, BELAIDENE Lydia, « *Impact des TIC sur la performance bancaire cas des banques de la ville de Bejai* », Univ Abedarahmene MIRA, 2015/2016, P9.

Les NTIC ont déjà provoqué deux évolutions au sein des banques. Dans le premier temps, elles ont été le support logistique au traitement interne des informations et aux relations au sein de la profession (*développement des réseaux interbancaires*). Dans le deuxième temps, elles sont devenues le moyen le plus rapide pour accéder aux marchés de capitaux, et ont permis la création de marchés électroniques globaux, ainsi que la modernisation des bourses de valeurs.

Dans les années 1970, la banque a subi une première révolution informatique, celle des grands systèmes capables de traiter des millions d'opérations autrefois exécutées par des gros bataillons de collaborateurs. Dix ans plus tard, l'informatique répartie a touché chaque agence et a permis d'effectuer, à partir de terminaux décentralisés, des opérations affectant la comptabilité clients tenue par les ordinateurs centraux. Aujourd'hui, la généralisation de l'informatique et l'ensemble des NTIC (messagerie électronique, téléphones portables...), bouleversent l'activité du secteur.[1]

Les TIC comprennent tout d'abord le matériel (informatique télécommunication), logiciels tel qu'illustré dans la figure suivante :

Figure 1 : Eléments de définition des TIC



Source : Abdelkader RACHEDI (2003). « *TIC, structure et comportement des hommes dans l'entreprise* » ; UNIV de Abou Baker BELKAID, Tlemecen.P09.

[1] BOUCHENOUA Karima, BELAIDENE Lydia ; *O*p. cit, p10

I.2. Définitions des TIC

Dans les différentes littératures de management, le concept de TIC (technologie de l'information et de la communication) fait l'objet de différentes définitions (*voir annexe n°1*) selon le point de vue de la source utilisée ou selon l'époque de la définition, on constate que la définition sémantique des TIC reste floue. Le terme technologie peut être défini comme étant « *un ensemble de connaissance relatives à certains type d'événements et d'activités associés à la production et à la transformation des matériaux* ».[1]

La définition internationale qui capte comme domaine des TIC des activités économiques qui aident au traitement, stockage et la transmission de l'information de plus en plus facile et de moins coûteux. L'expression TIC désigne des technologies récentes issues du mariage de l'informatique, du téléphone et de l'audiovisuel. Elle concerne le recueil, l'élaboration, le traitement, la conservation et le transport de textes, de sons, en plus des traditionnelles données numériques, elles se caractérisent par une grande diversité d'objets numérisés, une grande capacité de diffusion et de transport en réseau, une forte interactivité.[2]

Selon le grand dictionnaire terminologique[3] les TIC sont un :

> « *Ensemble des technologies issues de la convergence de l'informatique et des techniques évoluées du multimédia et des télécommunications qui ont permis l'émergence de moyens de communication plus efficaces, en améliorant le traitement, la mise en mémoire, la diffusion et l'échange de l'information* ».
>
> « *Les technologies de l'information et de la communication se définissent comme une technologie qui, initialement, a beaucoup de marge d'amélioration et, en fin de compte, est, utilisée dans une grande proportion des activités productrices, car ses usages sont multiples et présentent de fortes et nombreuses complémentarités avec d'autres technologies existantes ou à venir* ».[4]
>
> *LIPSEY et AL. (1998a).*

CHAPRON donne la définition suivante des TIC :

> *« TIC, Technologie de l'Information et de la Communication : expression aux contours assez flous, apparue avec le développement des réseaux de communication, désignant tout ce qui tourne autour d'internet et du multimédia. Elle recouvre également la notion de convivialité accrue de ces produits et services destinés à un large public de non-spécialistes. Au confluant de l'informatique, des réseaux de télécommunication et de l'audiovisuel, les TIC s'adressent au plus grand nombre. »* [5]

[1] GUELLEC.D et RALLE.P(2003), « *Les n^elle théories de croissance* », 5e édition, la découverte, Paris. P47.
[2] GOUVAERE Virginie(2002), « *L'évolution de travail avec les NTIC* », institut national de recherche et de sécurité, Lorraine, Paris, P2.
[3] Office Québécois. De la langue française. Le grand dictionnaire terminologique. Québec. retrieved marche 10/ 2009. From.www.systemed'information.fr/glossaire.htm/, consulter le 05/04/2018
[4] LIPSEY R.G, C BEKAR, et K CARLO (1998A)," what requiries explantation in help men", general perpuse technologies and economic grouth.
[5] CHAPIRON. B (2006). « Evaluation du système d'information pour une optimisation des forces de vente » Glossaire. Http://www.systemesdinformation.fr/glossaire.html, Recueilli le 10 Mars 2009, consulté le07/04/2018.

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

a) **Omniprésence :** c'est-à-dire que ces technologies sont présentes dans la plupart des secteurs comme l'éducation, la santé, la finance… ;
b) **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 ;
c) **Source d'innovation :** en plus de leur évolution propre, ces technologies contribuent à l'élaboration de nouveaux produits ou processus.[1]

I.3. Les TIC, une troisième révolution ?

« *Les TIC sont perçus comme étant une troisième révolution industrielle. Les technologies de l'information et de la communication constituent une technologie à usage général(TUG) et contribue donc à la productivité nationale.* »[2] *Patrick BISCIARI.*

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 mondiales. Elles constituent une technologie à usage général qui touche à tous les domaines et contribue à la productivité nationale et à une croissance forte et dure, permettant aux grandes nations le passage du support physique appuyé sur les ressources comme la richesse (*économie traditionnelle*) vers le support immatériel appuyé sur l'information et la communication (*nouvelle économie*).[3]

On remarque que 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.[4]

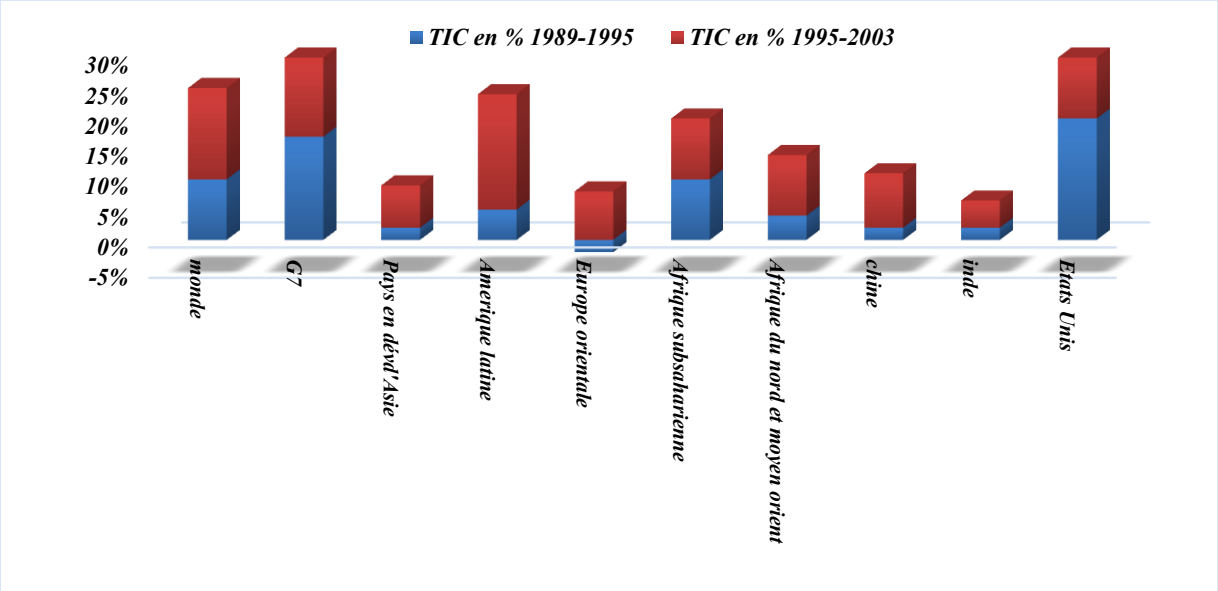
Suivant le raisonnement de Patrick BISCARI, l'UIT montre aussi le rôle que jouent les TIC dans la croissance économique : La plupart des études qui analysent l'incidence des TIC sur l'économie (en dehors du secteur des TIC proprement dit) s'intéressent essentiellement aux effets de la "productivité".

---

[1] Sylia BELATTAF ; *O*p.cit.; 2014/2015, p8.
[2] Patrick BISCIARI, Nouvelle Economie, Working papers-document series, PDF, www.nouvelleeconomie.com consulté le 10/04/2018
[3] Olivier BOMSEL, « *nouvelle économie, économie Numérique, Netéconomie*», édition DALLOZ, CERNA Paris, 2001, p5.
[4] Nathalie COUTINET, « *Définir les TIC pour mieux comprendre l'économie* », éd HAL (archives-ouvertes), decembre2007, Paris. P163.

Dans les pays développés, des ressources considérables et des efforts de créativité importants ont été consacrés à l'analyse des gains de productivité dans l'économie tout entière ainsi qu'aux niveaux des secteurs et des entreprises. Plusieurs études comparatives ont été réalisées en vue d'analyser la disparité des gains de productivité entre différents pays et différentes régions du monde. S'il est vrai que l'ampleur de l'incidence peut différer, on s'accorde en général à reconnaître que les TIC influent manifestement sur la croissance économique en augmentant la productivité.[1] Comme le montre le (*Graphe.1.)* suivant :

Graphe.1. : Contribution des TIC à la croissance économique



Source : UIT, adaptation de JORGENSON et VU, 2005.

Note : G7 : Canada, France, Italie, Allemagne, Japon, Royaume-Uni, USA

Dans une étude internationale très détaillée, comparant la période 1989-1995 avec la période 1995-2003, des mesures séparées des investissements en matière de TIC, des investissements non consacrés aux TIC et plusieurs indicateurs de la main d'œuvre ont été utilisé pour déterminer la corrélation entre l'évolution des niveaux d'investissement en matière de TIC et la croissance du PIB dans les différentes régions. D'après cette étude, le G7 est le groupe qui a bénéficié le plus des TIC : en effet, près d'un tiers (27%) de la croissance du PIB survenue entre 1995-2003 était dû à des investissements dans le domaine des TIC.

Toutefois, dans les principaux pays en développement et pays dont l'économie est en transition, le capital représenté par les TIC a joué un rôle plus limité (bien que de plus en plus important).

[1] Rapport de l'UIT, rapport sur le développement des télécommunications/TIC DANS LE MONDE 2006, UIT 2006.

En Afrique subsaharienne, l'incidence économique de la croissance du capital représentée par les TIC a été similaire pendant l'ensemble de la durée considérée – environ 10% – alors que l'incidence a été plus marquée au cours des 2 périodes pour la plupart des autres groupes. En ce qui concerne l'Amérique latine, on a observé un bond phénoménal entre la première et la seconde période *(Graphe.1.).*

II/ Etats des lieux des TIC

Les dernières données de l'UIT[1] concernant le développement des TIC indiquent que la connectivité et l'utilisation des TIC sont en constante progression. La disponibilité des communications connaît une croissance ininterrompue depuis dix ans, emmenée par le développement de la téléphonie cellulaire mobile et, plus récemment, de la large bande mobile. L'expansion des infrastructures large bande fixes et mobiles stimule l'accès à l'Internet et son utilisation.

Les réseaux cellulaires mobiles sont de plus en plus répandus et représentent désormais la solution la plus utilisée pour fournir des services de télécommunication de base. On recense aujourd'hui plus d'abonnements à la téléphonie cellulaire mobile que d'habitants dans le monde, même si de nombreuses personnes n'utilisent toujours pas de téléphone mobile, en particulier dans les pays en développement. Le nombre d'abonnements à la téléphonie fixe continue de chuter, passant ainsi sous la barre du milliard à l'échelle mondiale, et est particulièrement bas dans les pays les moins avancés (PMA).

- **Indice de développement des TIC (*IDI*)**

L'Indice de développement des TIC (*IDI*) de l'UIT est un outil unique permettant de comparer le niveau de développement des TIC dans les pays du monde entier. L'IDI associe onze indicateurs *(Annexe n°2)* relatifs à l'accès aux TIC, à leur utilisation et aux compétences connexes, rendant ainsi compte l'aspect essentiel du développement des TIC au moyen d'une mesure unique qui permet de dresser des comparaisons entre les pays et dans le temps. L'IDI de 2017 couvre 176 pays. Une comparaison avec l'IDI de 2016 montre que l'accès aux TIC et l'utilisation de ces technologies continuent de progresser dans presque tous les pays.

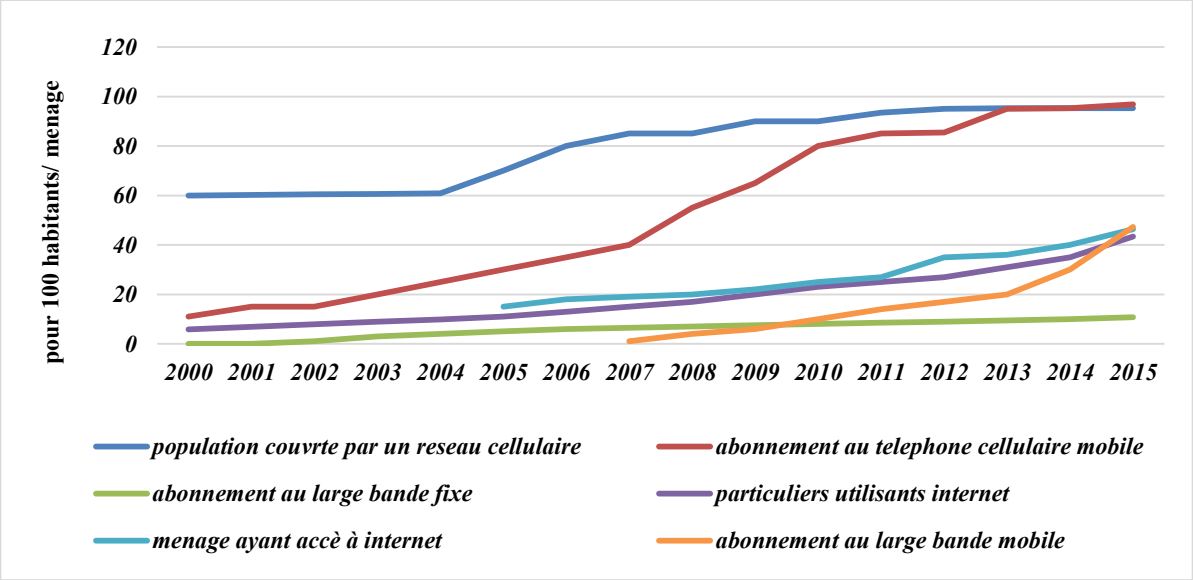
Toutefois, on constate également que de grandes disparités subsistent en matière de développement des TIC entre les pays bien connectés et ceux qui le sont moins, disparités contre lesquelles il convient de lutter si l'on veut que les sociétés de l'information inclusives contribuent à faire du développement durable une réalité et à atteindre les autres objectifs internationaux.

[1] Se référant aux rapports de l'UIT (*2015-2016*) « *Mesurer la société de l'information* ».UIT.

II.1.Au niveau mondial

- 3.2 milliard d'individus sont désormais en ligne (43% de la population) ;
- Le nombre d'utilisateurs de l'internet dans les pays en développement presque doublé en cinq ans ;
- Le nombre d'abonnement au cellulaire mobile est passé de 2.2 milliards à 7.1 milliards en 10 ans ;
- Le pourcentage de la population ayant accès aux réseaux 3G est passé de 45% à 69% en quatre ans ;
- L'écart entre les hommes et les femmes pour l'utilisation de l'internet est 11% ;
- Les abonnements à la large bande mobile sont passés de 0.8 milliards en 2010 à 3.5 milliards en 2015, selon les estimations ;
- Entre 2013 et 2014, le prix de la large bande a baissé de plus de 25% dans les PMA ;
- Le prix de large bande fixe a considérablement augmenté en 2014 ;
- L'internet des objets et des méga données offrent la possibilité de relever les grands défis du développement.[1]

Graphe.2. : Evolutions mondiales des principales TIC, 2000/ 2015* *(*données approximatives).*



Source : UIT.

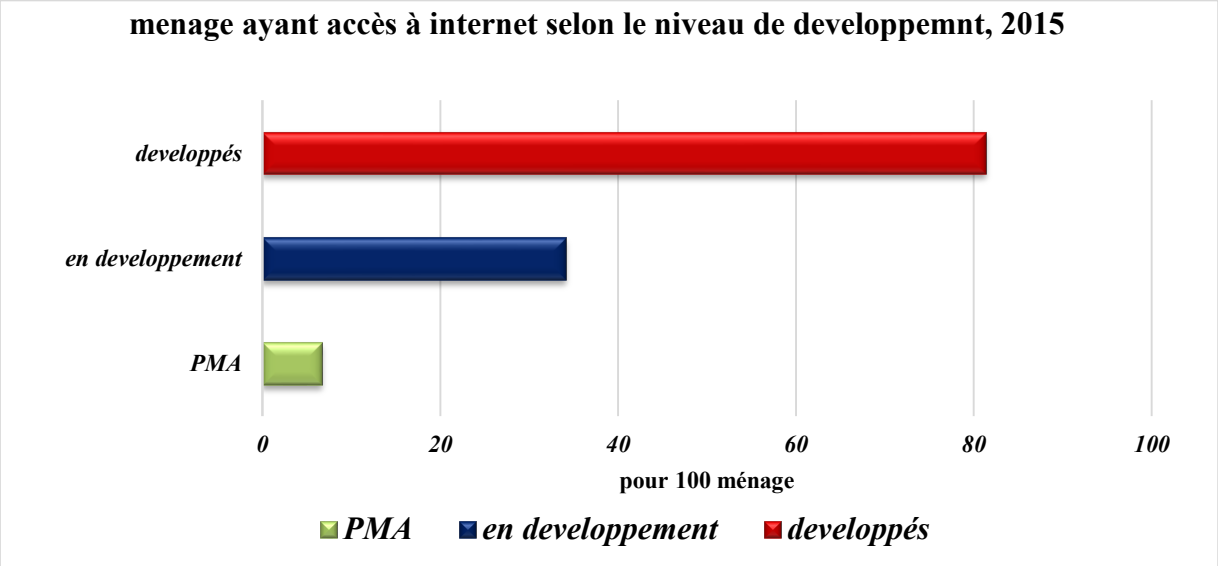
Les réseaux cellulaires couvrent désormais de plus de 95% de la population mondiale, et le nombre d'abonnements au cellulaire mobile est passé de 2,2 milliards en 2005 à 7,1 milliards en 2015, selon les estimations *(Graphique.2.).*

[1] Se référant aux rapports de l'UIT (*2017*) « *Mesurer la société de l'information* ».UIT.

La croissance du taux de pénétration du marché cellulaire mobile mondial a ralenti à mesure que le nombre d'abonnements s'approche de celui des habitants de la planète. Mais il reste encore un bout de chemin pour atteindre l'accessibilité et l'utilisation universelles de la téléphonie mobile dans les pays en développement. Les abonnements au téléphone fixe ont connu un déclin lent mais régulier, passant de 1,25 milliard en 2005 à 1,06 milliard (d'après les estimations) en 2015, notamment en raison du remplacement du fixe par le mobile.

Le nombre d'abonnements à la large bande mobile dans le monde a augmenté de 0,8 milliard en 2010 à 3,5 milliards (d'après les estimations) en 2015, tandis qu'il a été augmenté beaucoup plus lentement dans la large bande fixe, pour atteindre 0,8 milliard (d'après les estimations). Le nombre d'utilisateurs d'Internet a aussi augmenté rapidement. Il est maintenant estimé à plus de 40% de la population mondiale *(Graphique.2.).*

Graphe.3. : Accès à internet* *(*données approximatives)*

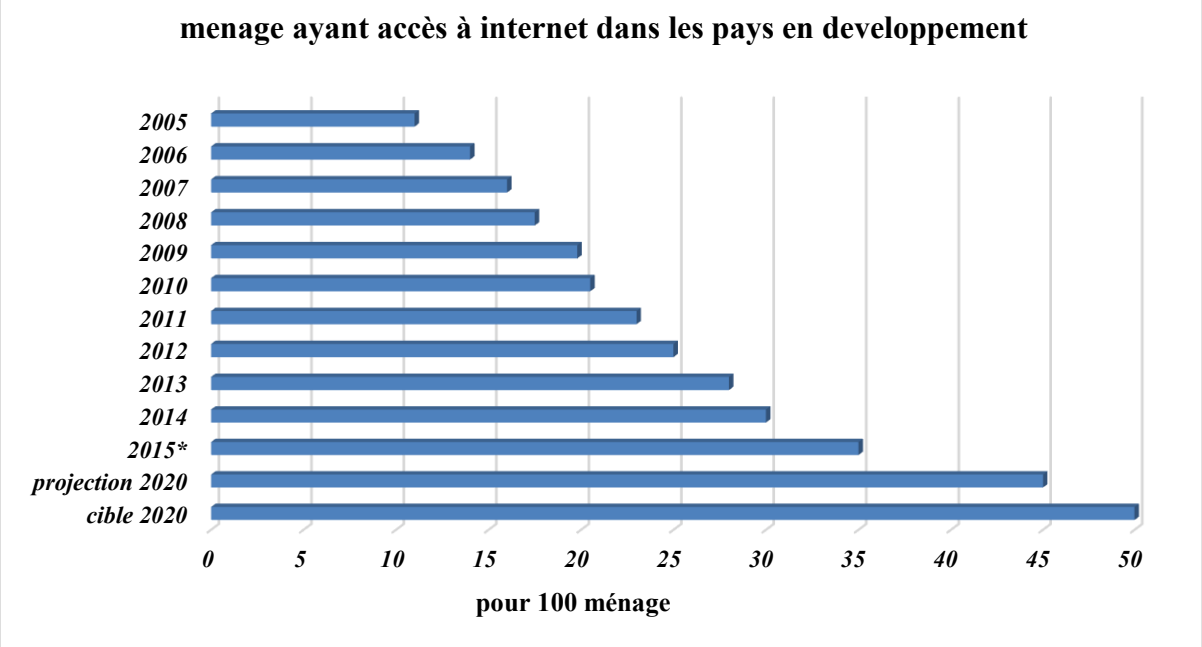


Source : rapport mesurer la société de l'information 2015de l'UIT.

Le rapport de l'UIT 2016 fait apparaître *(Graphique.3.)* que 6,7% seulement des habitants des 48 pays désignés par l'ONU comme étant les pays les moins avancés (*PMA*) ont accès à l'Internet à domicile, par rapport à 34,1% dans le monde en développement et 81,3% dans les pays développés. De plus, l'écart global entre les PMA et les autres pays en développement croît, selon l'indice de développement des TIC (IDI) de l'UIT.[1]

[1] Se référant aux rapports de l'UIT (*2015-2016*) « *Mesurer la société de l'information* ».UIT

Graphe.4.Les cibles du programme Connect 2020[1]*(*données approximatives).*



Source : rapport mesurer la société de l'information 2015de l'UIT.

Des mesures supplémentaires seront nécessaires pour faire en sorte que les cibles relatives à la croissance et à l'inclusion soient effectivement atteintes dans les pays en développement, particulièrement dans les PMA. Le Programme Connect 2020 a pour ambition de faire en sorte qu'au moins 50% des ménages des pays en développement, et 15% de ceux des PMA, aient accès à l'Internet à l'horizon 2020. Toutefois, selon les estimations de l'UIT, seuls 45% des ménages des pays en développement et 11% de ceux des PMA auront accès à l'Internet à cette échéance. Comme le montre (*Graphe.4.)*

II.2. Dans les Pays Arabes

Dans la région des Etats arabes[2], le développement des TIC est très inégal. Cette région est également très hétérogène du point de vue de l'IDI. Cette région compte un certain nombre de pays pétroliers à revenu élevé, dont trois se situent dans le premier quartile de l'IDI, mais aussi des pays à faible revenu, dont quatre font partie des pays les moins connectés. Ce sont les pays à revenu intermédiaire qui ont enregistré la plus forte progression dans la région, avec une augmentation de la valeur moyenne de leur IDI par deux fois supérieure à celle des pays se trouvant en tête et en queue du classement régional. Ce constat montre que l'écart est peut-être en train de se creuser en ce qui concerne le numérique entre les pays les moins connectés et les pays les plus prospères de la région.

[1] Se référant aux rapports de l'UIT (*2015-2016*) « *Mesurer la société de l'information* ».UIT
[2] Se référant aux rapports de l'UIT (*2017*) *O*p.cit. UIT.

II.3.En Afrique

L'Afrique met tout en œuvre pour faire progresser son indice de développement des TIC. En 2016, il s'élevait en moyenne pour la région à 2,48 points, soit à peine plus que la moitié de la moyenne mondiale qui est de 4,94 points. La majorité des 39 pays d'Afrique pour lesquels l'IDI a été calculé en 2016 sont des PMA. Ces chiffres s'expliquent par le niveau moins élevé de développement économique dans la région, qui nuit au développement des TIC.

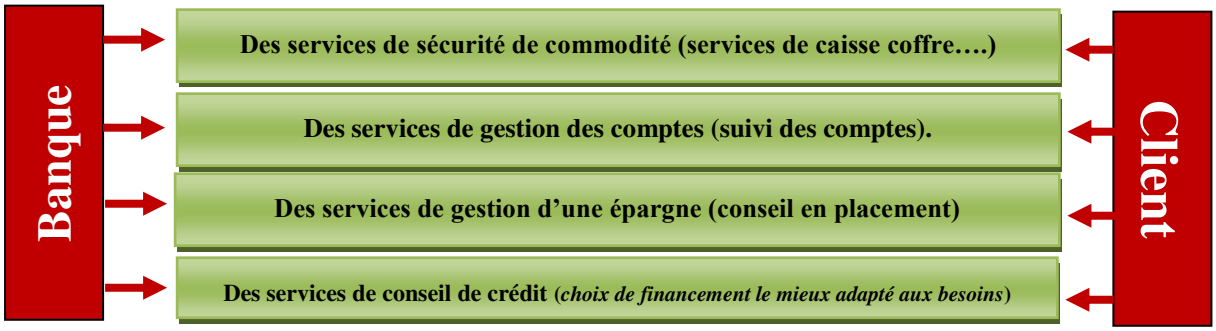
Le nombre d'abonnements au mobile cellulaire est l'indicateur ayant connu la plus forte croissance, contrairement à d'autres régions, où c'est le nombre d'abonnements au mobile large bande qui a le plus progressé. L'Afrique demeure toujours la région où l'IDI est le plus faible, en 2017, la valeur moyenne de l'IDI na pas vraiment changé, elle est de 2,64 points, soit à peine plus de la moitié de la moyenne globale qui est de 5,11 points. Seulement un pays de la région, Maurice, se situe dans la première moitié du classement global, tandis que 28 des 38 pays africains pour lesquels l'IDI a été calculé en 2017 figurent dans le dernier quartile. En revanche, deux des trois pays dont la valeur de l'IDI a le plus progressé au cours de l'année, à savoir la Namibie et le Gabon, appartiennent à cette région. (*La région Afrique de l'UIT ne comprend pas les Etats arabes d'Afrique du Nord*).

II.4.TIC et banque

Le rôle principal d'une banque est la création monétaire ainsi que la perception d'intérêts en prêtant l'argent déposé par leurs clients. L'activité des banques englobe la réception des fonds du public, leur mise à la disposition de la clientèle, ainsi que la gestion de moyens de paiement. Les fonds recueillis sont affectés à la conduite d'opérations de crédit, elles-mêmes génératrices de nouveaux dépôts par le supplément de monnaie qu'elles sont amenées à créer : les banques sont au centre du processus de « *création monétaire* ».[1]

Le schéma.1.montre l'ensemble des prestations de l'offre bancaire.

Schéma n°.1. : Le schéma de l'offre bancaire



Source : TOURNOIS N. « Le marketing bancaire face aux nouvelles technologies », édition .Masson.1989.P71.

[1] www.microsoftencarta.com Consulté le 29/03/2018.

L'internet représente l'une des plus importantes innovations technologiques dans le domaine des services bancaires, menant à un changement radical du comportement du consommateur. Son intégration dans les institutions financières donnes lieux à des nouvelles pratique de « *E-business* » et plus précisément de « *E-banking* » ou encore « *Banque Online* » permettant une efficacité d'actions commerciales, des réductions de cout considérables et un grand rapprochement des gouts et des attentes des clients.

Grâce à toutes les TIC électroniques, l'industrie bancaire a pris son élan dans l'évolution de son offre et de ses prestations, 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. En effet l'adoption de « *E-banking* » ouvre constamment aux banques de nouveaux horizons qui puissent être susceptibles de les aider à innover leurs services et leurs produits pour répondre aux exigences et aux conditions d'un développement durable et d'une solide relation banque-clients.

Au sein du secteur financier, les banques utilisent actuellement plusieurs canaux de distributions électroniques pour livrer leurs services. On peut les regrouper dans trois catégories suivantes**,** interpersonnelle, automatisées et à distance.[1]

- Libre-service automatisé : ou' le client remplit la pluparts des activités, à travers l'utilisation du support matériel simple, on pense généralement aux guichets automatiques de banque (GAB) ;
- Les services bancaires à distances : il existe peu d'investissements de la part des clients avec l'environnement physique. Sous cette appellation on inclut l'exemple du téléphone et de l'internet, ou' une multitude de services est offert aux consommateurs ;
- Les services interpersonnels : le client, tout comme l'employé doivent être présents sur le lieu de service. La servis cène affecte la nature et la qualité des interactions sociales.

Le schéma N°2 montre que la prestation de service bancaire contient deux variables principales :

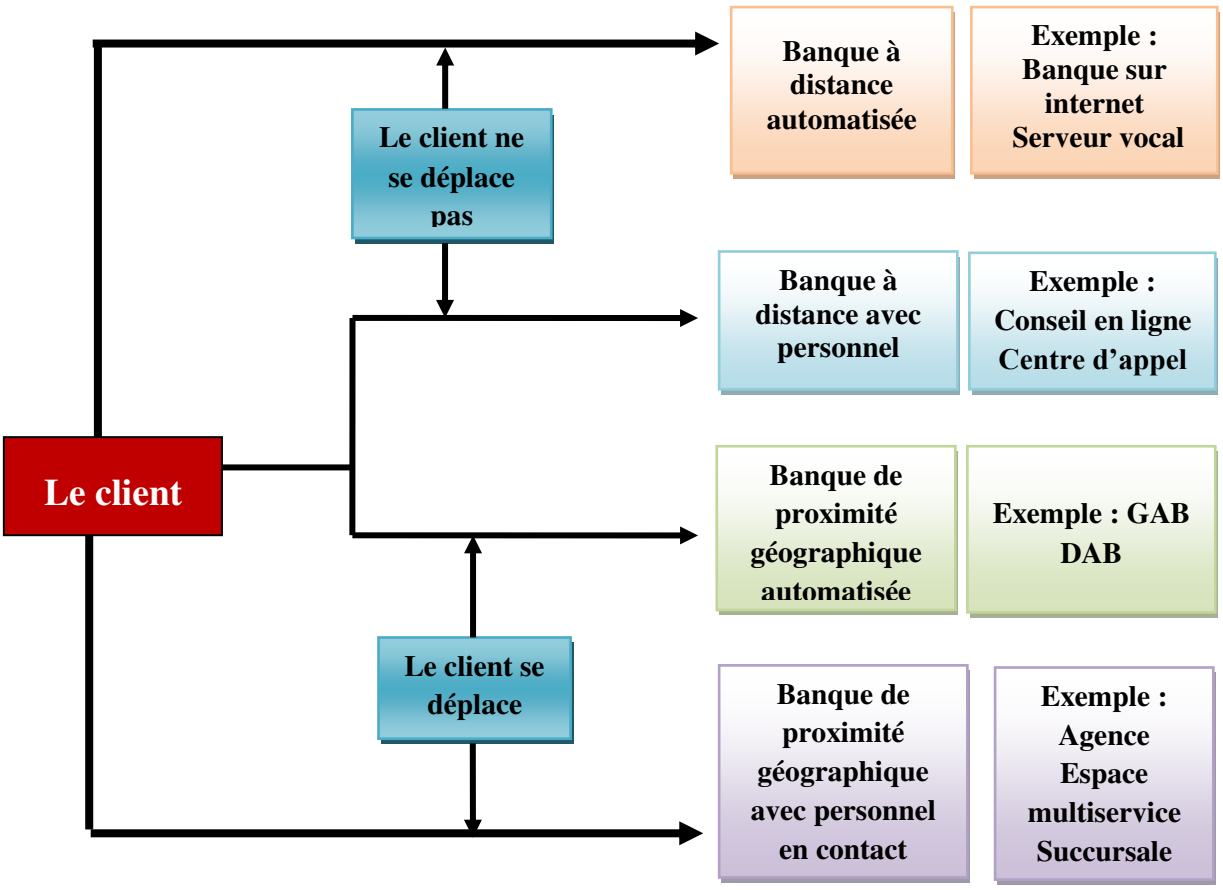
Le mode de contact à distance ou de proximité) ;

La nature de contact avec personnel ou sans personnel.

L'obtention des services bancaires peut être présentée comme suit.

[1] CHAOUKI Ourda ; Mustapha ZGHAL (2008), « *Les facteurs explicatifs de l'utilisation des technologies bancaires libre services* ».7eme journée Nantaise de Recherche sur le E-marketing, université de Nantes(IAE), Paris, 12 septembre, P.4**.**

Schéma.2. : Classification des modes de prestations de services bancaires selon le déplacement des clients



Source : CHAOUKI Ourda ; Mustapha ZGHAL (2008), « *Les facteurs explicatifs de l'utilisation des technologies bancaires libre services* ».7eme journée Nantaise de Recherche sur le E-marketing, université de Nantes(IAE), 12 septembre, P.4.

Après avoir présenté de façon générale l'attribution des TIC dans la banque, il nous parait essentiel de s'interroger sur les différentes TIC utilisées dans les banques et sur les moyens de paiement modernes. A cet effet, nous tenterons de présenter dans le point qui suit les principales TIC utilisées par le secteur bancaire.

A. Les nouveaux outils de télécommunication

La télécommunication est un élément important pour la banque dans ses relations avec les clients et les autres institutions. Les nouvelles technologies ont apporté de nouveaux moyens plus performants. Parmi ces moyens, on peut citer la banque par fil et la banque par écran.

A.1. La banque par fil : elle regroupe le téléphone et le fax.

- **Le téléphone** : la consultation par serveur vocal qui fonctionne 24 h sur 24 et 7 jours sur 7 est souvent très limitée .Comme exemple, nous citons la consultation du solde et les dernières opérations.

- **Le fax** : le service consiste à informer les abonnés de leurs mouvements bancaires de la semaine. l'abonné reçoit par fax son relevé des comptes détaillé de toutes les transactions effectuées.

A.2. La banque par écran : elle regroupe l'internet, l'intranet, l'extranet et les EDI**.**

- **L'internet :** c**'**est un réseau informatique mondial qui est accessible pour tout le monde. Il permet de relier des banques entre elles par l'intermédiaire de différents canaux et supports (câble, lignes téléphoniques). Cela pour transmettre différentes types d'informations (son, image et texte).
- **L'Intranet bancaire :** L'Intranet bancaire est le système d'information commun qui relie et que partagent l'ensemble des employés d'une même banque, aussi bien au niveau du siège que sur la totalité de son réseau d'agences. C'est l'ensemble des applications et des informations bureautiques et de télécommunication au service du fonctionnement interne de la banque.[1]
- **L'extranet :** C'est une extension du système d'information d'une banque. C'est un réseau informatique privé. Pour qu'une banque puisse échanger et partager de manière sécurisée des informations avec ses partenaires (clients, d'autres banques,…etc.). Il est basé aussi sur les mêmes protocoles que l'internet.
- **L'EDI (Échange de Données Informatisé) :** l'EDI est un outil au service de l'échange électronique consistant à transporter automatiquement de l'application informatique d'une entreprise à l'application informatique d'une autre entreprise, par des moyens de télécommunication. Mais l'EDI est d'abord un effort d'organisation consistant à analyser les procédures d'échanges et leurs flux de données pour les rationaliser, les codifier et en déduire une automatisation (machine to machine) des relations répétitives entre des acteurs qui communiquaient jusqu'ici par papier, fax ou message électronique (*Human to Human*).[2]

Le secteur bancaire utilise l'EDI de manière intensive, pour favoriser les échanges de masse avec les clients. Depuis de nombreuses années, il considère de plus en plus souvent cette technologie comme un vecteur important de service client**.**[3]

[1] Pascal THONIEL « *Usage de l'authentification dans le domaine bancaire* » Éditions Techniques de l'Ingénieur, Paris, 2010
[2] Pascal, THONIEL Ibid, P17.
[3] Michel LAFITTE « *Les systèmes d'information dans les établissements financiers* » directeur adjoint de la direction des assurances de personne à la FFSA, banque éditeur, 2009.

B. Les instruments de paiement

En période actuelle, toutes les banques connaissent la même ressource d'instruments de paiement, qui ne sont pas les pièces ou les chèques, mais par la reproduction d'une nouvelle forme qui est la monétique. Le système de paiement est un transfert d'actifs monétaire. Aussi c'est l'outil qui permet de transférer les fonds. Il assure la compensation et le règlement des ordres de paiement.[1]

B.1. La télé compensation

La télé compensation désigne l'ensemble des traitements électroniques, informatiques et télématiques qui est nécessaire à la gestion des transactions et de transferts de fonds monétaires. Le système de télé compensation repose sur certains principes qui sont les suivants :[2]

- La notion de la place unique, c'est-à-dire un seul centre de compensation par banque ;
- La sécurisation des moyennes de paiement (*Chèque, Cartes*) ;
- Règles d'échanges disciplinés aux normes inter bancaires.

B.2. La monétique *(voir annexe n°3).*

La monétique appelée aussi monnaie électronique peut être définie comme l'ensemble de techniques informatiques magnétique, électronique et télématique. Elle permet l'échange de fonds sans support de papier.[3]

Actuellement, la monétique est le moyen le plus efficace pour assurer un maximum de transaction. Elle assure au propriétaire d'une carte bancaire, la possibilité de retirer des espèces auprès de n'importe quel distributeur automatique. Le développement de la carte bancaire peut conduire pour une partie au moins, à la justification du système bancaire et éviter l'indifférence de la clientèle quant à l'utilisation des services de la banque.

La monétique est donc, l'ensemble des moyens électroniques mis en œuvre pour automatiser les transactions bancaires (*cartes de paiement, de retrait,…),* ou encore l'ensemble des technologies, procédés et équipements permettant une électrisation du transfert de fonds, de mise à disposition de liquide et informations de la clientèle sur ses *comptes.*

B.2.1.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.[4]

---

[1] Dominique RAMBURE, « *Les systèmes de paiement* », édition ECONOMICA, Paris, 2005, P12.
[2] Document interne de la CNEP banque : formation des administrateurs de la solution de dématérialisation.
[3] D.PLIHON « *La monnaie et ses mécanisme* », édition la découverte, Paris 2000 ; 2001.page 17.
[4] http://www.banque-info.com/lexique-bancaire/d/distributeur-automatique-de-billets--dab.consultéle 29/04/2018

Les premières cartes ont été mises en circulation dès 1967 et à partir de 1970, la carte de paiement devient aussi carte de retrait [1] dans les distributeurs de billet appelés BANKOMAT.[2]

Le développement de son utilisation rejoint alors celle des chèques au début des années 2000.

En effet, la carte bancaire est un moyen à la fois sûr et pratique de fournir au commerçant les informations sur son compte bancaire et de prouver son identité par rapport à ce compte. Le commerçant dispose d'un TPV (terminal point de vente) qui permet de vérifier que le client/consommateur a tapé le bon code secret ou code PIN (Personal Identification Number) et qu'il est donc bien le possesseur de sa carte.[3]

On distingue différents types de cartes, parmi elles on cite :

-1-La carte de retrait:[4] 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.

-2-La carte de paiement :[5] 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).

-3-La carte de crédit :[6] 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.

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

[1] Dont la seule utilisation est le retrait d'argent du distributeur ou éventuellement, à un guichet.
[2] Groupe de travail d'IFCAM (*Institut de Formation du Crédit Agricole Mutuel*), « *Moyen de paiement et services associés* », 2013-2014, www.ca-ifcam.fr. Consulté le 6/05/2018.
[3] D. PLIHON ; Op cit, p19.
[4] Jean-Luc SARRAZIN, BTS banque « techniques bancaires des marchés des particuliers »,3e édition, Canada(Québec), 2013,
[5] *Idem.* P52.
[6] http://www.banque-info.com/lexique-bancaire/c/carte-de-credit. Consulté le06/05/2018.

accroître les crédits et donc de se retrouver à un moment donné en situation de surendettement.

4-Le porte-monnaie électronique MONEO [1]

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 ou parking.

5-La e-carte (réseau carte bleu) [2]

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).

6-Les cartes de hautes gammes et cartes de prestige [3]

- **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). [4]

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.

Les cartes bancaires sont les plus connues des instruments de paiement de retrait bancaire. Elles sont acceptées chez les commerçants affiliés au réseau monétique bancaire et sur tous les distributeurs automatiques de billets (DAB) installés sur le territoire national.

[1] Jean Luc SARRAZIN, *O*p-cite, P54.
[2] *Idem* P54.
[3] *Idem*, P55.
[4] Voir le lien suivant : http://abbinvest.com/index.php?page=blog&var=18.Consulté le 03/05/2018.

A la fin de l'année 2008, les cartes bancaires qui sont émises en Algérie est de 273000 cartes. Mais la plupart sont des cartes de retrait. Durant la même année, on compte un millier de distributeurs de billets sur le territoire national.[1]

Il existe plusieurs types de cartes qui exercent les fonctions suivant :

- Un instrument de paiements pour effectuer des achats et services sur les terminaux de paiement électroniques (TPE) installés au niveau des commerçants affiliés aux réseaux bancaires ;
- Un instrument de retrait de billets dans des DAB connectés aux réseaux monétiques interbancaires ;
- Un instrument de crédit qui donne à son titulaire, la possibilité d'effectuer des achats à paiement différé précédent ;
- Le télépaiement par internet.

B.2.2.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 [2](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 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* ».[3]

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).

B.2.3.Le m-banking (ou m-payement)

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 est l'application internet sans fil,

[1] Http : www.SATIM-dz.com consulté le 02/05/2018
[2] 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)conslté le20/05/2018
[3] http://www.itpro.fr/a/cheques-electroniques/consulté le 20/05/2018.

parfois appelé m-banking. BARNE et CORBITT, (2003)[1] définissent le m-banking comme étant une combinaison de l'internet et de téléphone mobile, un nouveau service qui permet aux clients d'utiliser la connexion internet de leur téléphone mobile pour vérifier les soldes de leurs comptes bancaires, les actifs de transferts entre comptes, le contrôle de ligne de crédits ainsi le règlement des factures. La banque offre les services bancaires à partir d'un téléphone cellulaire numérique ainsi qu'à partir de certains appareils sans fil.

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 :[2]

- M-Pesa ;
- Wizzit ;
- Celpay ;
- Zébra.

C. Les technologies du système de paiement

Ce sont des appareils permettant le retrait automatique d'espèces qui sont installés au niveau des agences. Il s'agit des GAB, DAB et TPE qui sont décrit dans ce qui suit **:**

C.1.Guichets automatiques de billets (GAB)

Les GAB sont des appareils automatiques. Ils sont aménagés à l'intérieur des agences et ils permettent au client d'effectuer eux même leurs opérations bancaire (*retrait d'argent, consultation de compte, commande de chéquier*), à l'aide de sa carte bancaire et de son code confidentiel.[3]

C.2.Les distributeurs automatiques de billets (DAB)

Les DAB sont des appareils automatiques permettant à la clientèle d'effectuer des retraits d'espèces.[4]

Ils sont installés par les établissements de crédit, les centres de chèques postaux (CCP) ou par les grands émetteurs de cartes (grandes boutiques…etc.) qui permettent aux clients de retirer des sommes d'argent de leurs comptes à l'aide d'une carte bancaire et d'un code confidentiel.[5]

[1] BARNES, S. J and CORBITT, B. (2003), « *mobile banking: concept and potential* », Internationnal Journal of mobile communication, Vol.1, N°.3, pp273-288.
[2] Voir : http://www.cairn.info/zen.php?ID_ARTICLE=EMR_129_0110 consulté le 28/05/2018.
[3] Y .COLVERT, Dictionnaire des Banques et Assurances, Paris 1988.p287.
[4] Y .COLVERT, *Ibid*.p287.
[5] Document relative la BDL banque op.cit.

C.3. Terminal de Paiement Electronique(TPE)

Un terminal de paiement électronique (aussi appelé TPE) est un appareil électronique capable de lire les données d'une carte bancaire, d'enregistrer une transaction, et de communiquer avec un serveur d'authentification à distance.[1] Il assure ainsi un traitement à la fois sécurisé, rapide et performant des transactions de paiement. Pour utiliser un TPE, un commerçant doit passer un contrat avec sa banque par lequel est fixés un montant maximal de transaction au-dessus duquel une autorisation est obligatoire, ainsi que le montant que la banque prélèvera comme commission sur chaque paiement effectué.

Ce type d'appareil présente plusieurs avantages notamment : la grande sécurité ; son utilisation est facile ; non encombrant ; permet un gain de temps ; moyen de paiement moderne et efficace, et accepte toutes les cartes bancaires.[2]

III/ Avantages et risques des NTIC

D'un point de vue plus général les avantages des TIC peuvent être définis à 3 niveaux :

- **Au niveau du système d'information :** Hausse de la productivité du travail pour la saisie de l'information, donc baisse des coûts. Délocalisation de la production (centre d'appels), amélioration de l'efficacité de la prise de décision permise par une banque de donnée plus importante sur ses partenaires.
- **Au niveau de la structure de l'entreprise et de la gestion du personnel :** Organisation moins hiérarchisée, partage d'informations. Meilleure gestion des ressources humaines (recrutement, gestion des carrières plus facile), meilleur suivi du personnel.
- **Au niveau commercial :** Nouveau circuit de production grâce à l'extension du marché potentiel (commerce électronique). Une baisse des coûts d'approvisionnement. Développement des innovations en matière de services et réponses aux besoins des consommateurs. Amélioration de l'image de marque de l'entreprise (entreprise innovante).[3]

Au fur et à mesure que les TIC se développent, des risques sont en nette hausse.

- **Les accidents** : comportent les pertes de données, les pannes ;
- **Les erreurs** : comme les erreurs de conception, les erreurs de réalisation et les erreurs à l'utilisation ;
- **La malveillance** : on recense les vols et vandalismes, les fraudes (utilisation non autorisée des ressources du système d'information pour un travail personnel, pour le détournement

[1] http://blog.wikimemoires.com/2011/04/definition-du-paiement-electronique-e-paiement/consulté le 09/05/2018.
[2] Document relative la BDL, Ibid.
[3] http://experts-univers.com/inconvenients-avantages-des-ntic.html.consulté le 09/05/2018.

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

Le développement des nouvelles technologies fait que nous sommes à l'aube d'une nouvelle ère, celle de l'information. On peut désormais transmettre et stocker une information sur des supports physiques variés (*câbles électriques, fibres optiques, ondes satellites, support magnétiques et optiques…*). La transmission et la copie se font quasiment sans perte d'informations, et le traitement automatique des informations est très aisé.

Malgré la bonne santé de l'économie liée aux télécommunications et technologies de l'information et de la communication (TIC), le développement de l'usage d'Internet occasionne également de nombreuses menaces en raison du développement important des arnaques réalisées à l'aide des outils numériques (téléphone cellulaire et Internet) aussi bien à l'intérieur des pays qu'au plan international. 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 désinformation[1], etc. Autant de délits qui peuvent être réunis et expliqués en un seul terme « *Cybercriminalité* ».

[1] Qui est l'utilisation d'informations erronées

Section 2: La naissance de la cybercriminalité

Le développement contemporain des Technologies de l'Information et de la Communication (TIC) constitue un enjeu majeur pour le développement économique. Cependant, il a été à l'origine de l'apparition du phénomène de la cybercriminalité dont les caractéristiques particulières ont entraîné l'inadaptation des systèmes répressifs de la plupart des États, dont les réponses traditionnelles conçues pour un environnement matérialisé et national, se sont révélées inappropriées pour saisir ce nouveau phénomène criminel, immatériel et mondial de l'ère numérique.

I/ Définition et terminologie

I.1. Evolution de la terminologie

La cybercriminalité se développe entre 1980 et 1988. La première date se réfère à la création d'Internet qui fait suite à la séparation d'Arpanet entre un réseau militaire et un réseau civil. La seconde date renvoie au premier outil de piratage connu et complètement automatisé.il correspond au premier incident informatique de type « *Malware* » occasionné par un ver Internet qui a infecté en quelques jours plus de 6000 serveurs Unix sur un parc d'environ de 60 000 reliés au réseau Internet de l'époque, soit un taux d'infection de 10%. Plus communément appelé « *ver Morris* » ou « *ver de Morris* » du nom de son concepteur, ce ver informatique est le premier d'une longue série, à l'origine d'une nouvelle course en avant, celle du piratage informatique.

Devenu un véritable fléau dès la fin du XXe siècle, le piratage informatique n'est plus un mythe, ou une chimère à laquelle certains ne voulaient ou ne semblaient pas croire, comme certains organisme ou grandes entreprises. Les pirates informatiques n'en finissent plus de faire parler d'eux.

En témoigne le ver informatique « *I Love You* » qui s'est répandu en quelques jours sur plus de trois millions de machines à travers le monde, soit 10% des ordinateurs connectés à internet[1].

- **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, il a réussi à modifier le programme de facturation étendant les heures creuses à toute la journée.

[1] Romain BOOS, « la lutte contre la cybercriminalité au regard de l'action des Etats », thèse de doctorat, Univ LORRAINE, France, 10/07/2017

- 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.
- 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.
- 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.
- 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.
- 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.
- En **2012** (Aout)**,** le groupe pétrolier Aramco a été la cible d'une cyberattaque et plus de 30 000 ordinateurs du groupe pétrolier, basé en Arabie Saoudite, ont 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 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 «

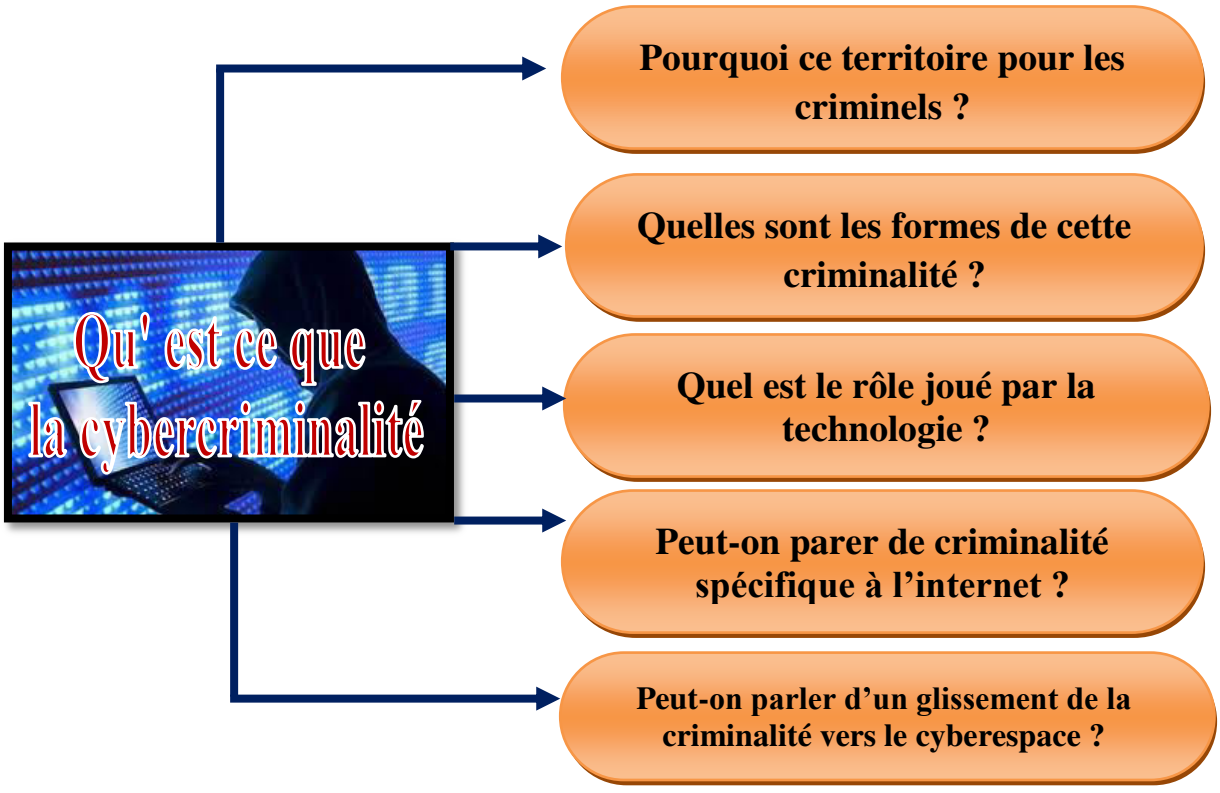
botnet » (machine zombie), une série de noms d'utilisateurs et de mots de passe ont été automatiquement testés jusqu'à l'aboutissement du méfait. Aussi, en Avril 2015, la chaine TV5 monde a été victime de piratage par des militants islamistes se revendiquant de l'organisation Etat Islamique (EI).

- En **2016**, Des cybercriminels ont volé près de 20 millions de livres au Royaume-Uni dans des comptes bancaires en utilisant le malware Dridex. L'affaire a été confirmée par l'Agence Nationale de la Criminalité (NCA).

I.2. Définitions appropriées à la cybercriminalité

Plusieurs définitions peuvent être assimilées à la cybercriminalité car elle doit définir clairement les actes qui sont inclus dans ce terme. Le terme même de cybercriminalité ne se prête pas à une définition simple, et est considéré comme une série d´actes ou de comportements plutôt que comme un unique acte.

Schéma N°3: Définir la cybercriminalité



Source: fichier power point ; www.definitiondelacybercriminalité.com; consulté le20/05/2018,formation trinôme; avril2009.

A partir de ce schéma on remarque qu'il s'agit d'une notion largement définie. Il n'y a pas de définition universelle de la cybercriminalité qui a été admise, si bien que chaque Etat l'a défini selon ses propres critères.

A. Définitions proposées

- **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*».[1]
- **L'approche du Professeur LUCAS** qui considère :

> *Que « la seule démarche acceptable consiste à réserver l'acception de fraude informatique aux hypothèses dans lesquelles la technique informatique est au cœur de l'agissement incriminable » tout en sachant fort bien qu'il est parfois difficile d'isoler le « noyau dur » de la« périphérie».*[2]

- **Selon les experts de l'Organisation pour la Coopération et le Développement Economique (OCDE),** à savoir « *tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne un traitement automatique de données et/ou de transmissions de données* ».[3]
- **Selon l'O.N.U**.

> *La « Cybercriminalité » doit recouvrir « tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent », et dans une acception plus large « tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique»* [4].

- **Définitions adoptées en Europe**

Selon le ministère de l'Intérieur français, la cybercriminalité recouvre « *l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunications en général et plus particulièrement sur les réseaux partageant le protocole TCP- IP,*[5] *appelés communément l'Internet*» [6]**.**

Pour **l'Office fédéral de la police suisse**, la cybercriminalité s'entend « *des nouvelles formes de criminalité spécifiquement liées aux technologies modernes de l'information, et de délits connus qui sont commis à l'aide de l'informatique plutôt qu'avec les moyens conventionnels* »[7].

[1] D. WALL: *Crime and the Internet*, ed Routledge, (N.Y), 2001, p. 3.
[2] A. LUCAS : Le Droit de l'Informatique, éd PUF, Paris, 1987, n° 413.
[3] H. ALTERMAN et A. BLOCH : La Fraude Informatique, éd Gaz. Palais, Paris, 3 sep. 1988, p. 530.
[4] 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 12/1/2018).
[5] Désigne les protocoles communs de communication utilisés par l'Internet, permettant l'interconnexion généralisée entre réseaux hétérogènes.
[6] Le Ministère de l'Intérieur Français <http://www.interieur.gouv.fr/> (consulté le 24/01/2018).
[7] Rapport d'analyse stratégique, [Octobre 2001].

- **Définitions adoptées au canada**

  Selon le Collège canadien de police définit la cybercriminalité comme « *la criminalité ayant l'ordinateur*[1] *pour objet ou pour instrument de perpétration principale* ».[2]

- **Définitions adoptées aux Etats-Unis**

  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 perpétration, son investigation, ou ses procédures pénales* ».[3]

Selon 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 ; 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* ».[4]

Selon le Code pénal du Texas (section 33.02) va plus loin. Il considère comme cybercriminalité, « *le fait d'accéder à un ordinateur, à un réseau, ou à un système informatique sans avoir l'autorisation de son maitre* ».[5]

B. Démystification de la cybercriminalité

Dans l'usage courant, la cybercriminalité sert à désigner toutes les formes d'attaques réalisées au moyen de réseaux informatiques ou de systèmes d'information, où les ayant pour cible. En d'autres termes la cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet comme le montre le schéma du dessous *(schéma n°.4.).*

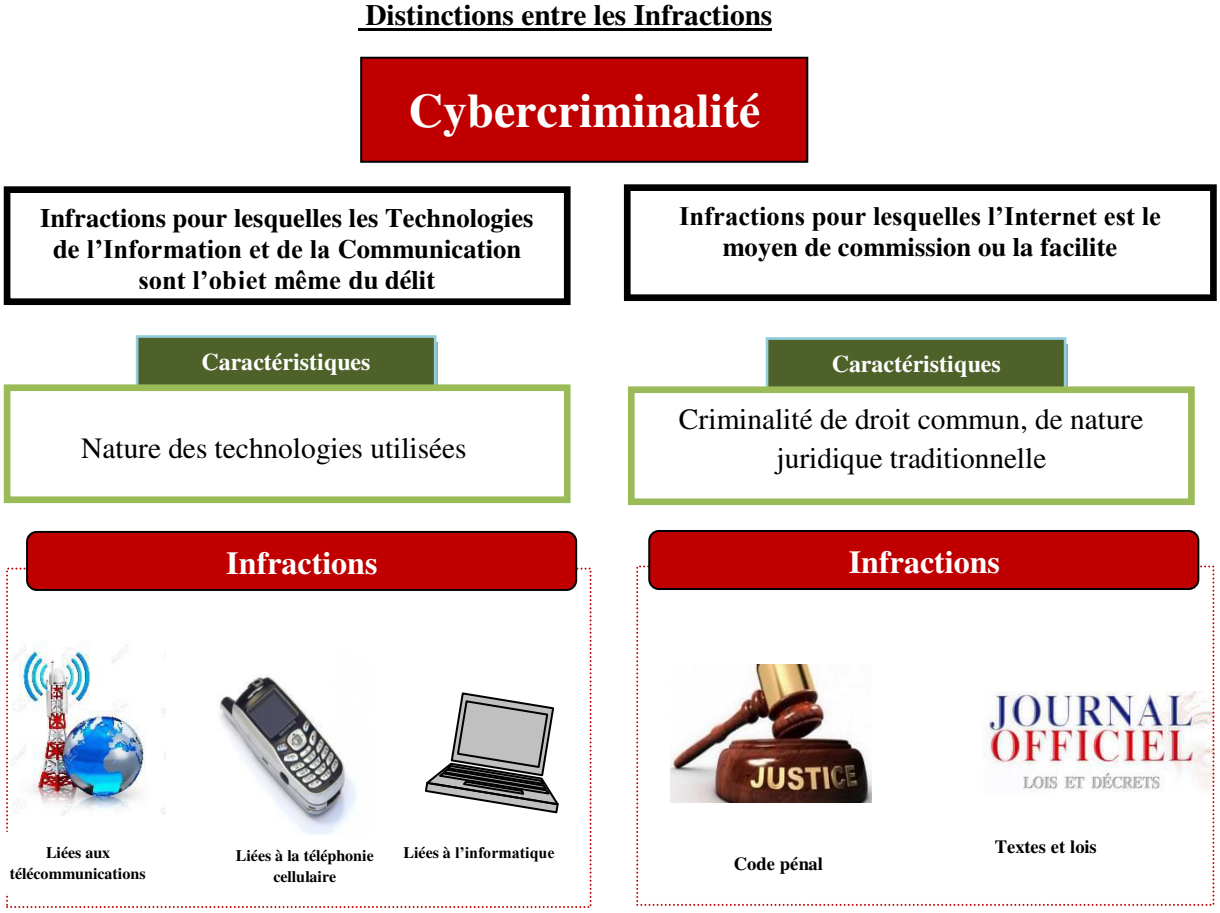
- La cybercriminalité ne définit pas à elle seule une infraction, mais un ensemble d'atteintes aux biens ou aux personnes commises via l'utilisation des nouvelles technologies.
- Par nouvelles technologies, on entend tout mode de communication, à savoir l'Internet mais également la téléphonie mobile, peu importe le protocole utilisé.
- Cette notion de cybercriminalité peut concerner les infractions relatives au contenu qu'il s'agisse de textes (insultes, propos négationniste ou xénophobes) ou d'images.
- Elle peut concerner également les atteintes à la propriété intellectuelle, qui constitue un véritable fléau pour l'économie.

---

[1] M. CHAWKI, « *Essai sur la notion de cybercriminalité* », IEHEI, juillet 2006, P. 8
[2] Centre canadien de la statistique juridique, disponible à l'adresse : http://collection.nlc-bnc.ca/ consulté le 11/01/2018.
[3] U.S. Department of Justice <http://www.justice.gov/>. Consulté le 2/02/2018
[4] Code pénal de l'Etat de Californie (section 502). http://www.justice.gov/>. Consulté le 2/02/2018
[5] Code pénal de Texas (section 33.02).). http://www.justice.gov/>. Consulté le 2/02/2018

- Parfois, l'utilisation directe des NTICS qui peut constituer à elle seule une infraction.

Schéma n° .4. : Décortication de la cybercriminalité



Source : La Cybercriminalité **;** Les acteurs, les infractions, Cas concret et retour d'expérience Par Vincent LEMOINE Chef du Groupe Cybercriminalité de la B.R Nanterre Expert non inscrit ; Nanterre, France, 2016 .

B.1.Indicateurs statistiques concernant la cybercriminalité

La quantification de l'effet de la cybercriminalité est un acte très difficile à réaliser et ce, par rapport aux nombres inestimables d'infractions et de pertes qu'elle entraine. Selon le rapport de l'UIT[1] sur la cybercriminalité, les pertes enregistrées par les entreprises et les institutions aux Etats-Unis du fait de la cybercriminalité pourraient atteindre 67 milliards USD; il est cependant difficile de savoir si l'extrapolation des résultats des sondages donne des chiffres fiables car le nombre de cyber-délits est inexact, vue que les signalements, par les victimes, ne sont pas systématiques. Pour cela la réalisation des enquêtes sur l'impact de la cybercriminalité est un paramètre plus pertinent que le nombre précis de cyber-délits dans une seule année, qui peut être obtenue par la comparaison des résultats sur plusieurs années.

[1] Rapport de l'UIT 2009 «*Comprendre la cybercriminalité : Guide pour les pays en développement*», p20.21.

On peut citer, à titre d'exemple, l'étude *Computer Crime and Security Survey 2007*, réalisée par l'institut américain CSI [1], qui analyse, entre autres tendances, le nombre d'infractions informatiques. Cette étude repose sur les réponses fournies par 494 professionnels de la sécurité informatique travaillant dans des entreprises, des organismes publics et des établissements financiers américains aux Etats-Unis.

L'étude fournit des informations sur le nombre d'infractions signalées entre 2000 et 2007 par les organismes interrogés. Elle montre que, depuis 2001, la proportion des organismes ayant subi ou noté des attaques par virus ou des accès non autorisés à des données, a diminué, sans toutefois en donner la raison. Cette diminution du nombre d'infractions reconnues est corroborée par des études menées par d'autres instituts. Des statistiques réalisées en Allemagne montrent par exemple qu'après avoir atteint un pic en 2004, le nombre d'infractions informatiques a presque retrouvé son niveau de 2002.

Les statistiques sur la cybercriminalité sont sujettes à interprétation du moment qu'elles ne peuvent pas fournir d'informations fiables : à la fois pour l'incertitude du niveau ou l'ampleur des infractions signalées, ainsi que pour la réduction inéprouvée du nombre de cyber-délits. En conséquence, les données actuellement disponibles sont insuffisantes pour prévoir les tendances et les évolutions futures.

B.2.Dimensions internationales de la cybercriminalité

Les contenus illicites(CI) transmis par courriel transitent par plusieurs pays avant d'atteindre le destinataire, d'où vient la notion de dimension internationale de la cybercriminalité[2]. Ces (CI) parfois sont stockés à l'étranger et font l'objet de contradiction (autorisés par certains et jugés illicites par d'autres).

Il est donc essentiel que les Etats concernés par un cyber-délit collaborent étroitement aux enquêtes diligentées. De même l'informatique repose fondamentalement dans le monde sur la même technologie, alors cette harmonisation des normes techniques qui a permis la mondialisation des technologies et des services, elle devrait aller bien au-delà et conduire à l'harmonisation des législations nationales. Cependant, comme l'ont montré les négociations portant sur le Premier Protocole à la Convention du Conseil de l'Europe sur la cybercriminalité, le droit national évolue beaucoup plus lentement que les techniques. Internet nie toutes frontières, mais des moyens existent pour restreindre l'accès à certaines informations.

[1] Computer Security Institute (CSI), United States.
[2] Rapport de l'UIT 2009, *O*p.Cit, p15;16.

Le blocage de l'accès à certains sites et le refus des connexions venant de certains pays en filtrant les adresses IP (on parle de "ciblage IP"), demeurent des instruments utiles pour préserver des différences territoriales dans un réseau mondial.

B.3.Les motivations des cybers délinquants *(voir annexe N° 15)*

L'anonymat virtuel dont se distingue le cyber-crime motive différents types de personnes car les chances d'être détectés sont minimes. Il est parfois difficile de cerner toutes les motivations des cybercriminels mais, on peut distinguer les quatre (04) les plus majeures :[1]

- **L'idéologie** : 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 ;
- **Les gains financiers directs** : pour la majorité des cybercriminels, l'argent est la principale motivation[2], il s'agit, par exemple, du vol de données bancaires, de données personnelles mais aussi de données critiques de l'entreprise. Ces données seront revendues par la suite ou utilisées pour réaliser des fraudes ;
- **La déstabilisation entre Etats ou le Cyber-terrorisme :** 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 ;
- **L'obtention de capacités d'attaques :** 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. La figure ci-dessous résume les quelques organismes et Etats qui ont été victimes de cyber attaques :

I.3. La distinction de la cybercriminalité et les criminalités apparentées

Selon le point précédent le phénomène de la cybercriminalité s'avère très vaste, complexe et touche plusieurs domaines[3]. Dans la même idée, certains auteurs confondent dans le sens du délinquant, en désignant sous la terminologie de « *pirate* » tous les délinquants en informatique.[4] Ainsi, il convient de faire une distinction de la cybercriminalité et les criminalités apparentées**.**

[1] Se référant< http://1-cybermenace-cybersecurité-V3-pdf.fr/ Cybercriminalité, Cyber-menace et entreprise numérique Quels problèmes, quelles solutions ? WISG 2015 : 3 Février> consulté le 24/08/2018
[2] D'après les données du KASPERSKY Lab, < http://blog.kaspersky.fr/quest-ce-qui-motive-les-cyber-criminels-l'argent-évidemment/372/ >, consulté le 03/03/2018
[3] Se référant au document M. CHAWKI, « Essai sur la notion de cybercriminalité », IEHEI, juillet 2006, P. 25
[4] P. BLANCHARD: Pirates de l'Informatique, Enquête sur les Hackers Français (Addison Wesley), France, 1995.

A. La distinction relative aux termes juridiques

La cybercriminalité est entendue dans un sens large comme toute infraction qui, implique l'utilisation des technologies informatiques. De même, les notions de « *criminalité informatique* », « *délinquance informatique* », « *criminalité de haute technologie* » sont souvent employées indifféremment. Cette distinction est comme suit :

A.1.La cybercriminalité et la criminalité informatique

La cybercriminalité et la notion de criminalité informatique ont une relation très étroite, cependant il existe une distinction qu'on juge utile de mettre en évidence. 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. [1] (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 ».[2]

Selon Mme.L.D. BALL, la criminalité informatique est « *une action illicite où l'ordinateur joue un rôle principal pour la commettre* ».[3]

A.2.La cybercriminalité et la criminalité en col blanc

En 1939, l'auteur américain SUTHERLAND, dans son étude, mit en évidence pour la première fois 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 :

[1] Voir P. DELEPELEERE, *O*p.cit.; E. CESAY, "Digital Evidence and Computer Crime", Academic Press, Londres, 2000, P.9.
[2] K. TIEDEMANN, « *Fraude et Autres Délits d'Affaires Commis à l'Aide d'Ordinateurs* », Revue. D.C.P, Bruxelles 1984, n° 7, P.612.
[3] L. D. BALL, "Computer Crime in The Information Technology Revolution". T. FORESTER, MIT Press, Cambridge, 1985, PP. 543-544.

- 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.

A.3.La cybercriminalité et la criminalité de haute technologie

Selon M. CHAWKI, la criminalité de haute technologie peut couvrir deux catégories :[1]

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

Selon les définitions données 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.

B. 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 :

B.1.Le Hacker

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* »[2].

Selon M. CHAWKI, le terme hacking, comme défini dans le New Hacker's Dictionnary[3], signifie :

[1] M. CHAWKI, *Op*-cit, P, 30.
[2] Voir le document : M. CHAWKI, *Op*-cit, P. 32.
[3] https://www.google.fr/#q=new+hacker%27s+dictionary+pdf consulté le 20/05/2018

- 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 ;
- Une 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* ».

D'après la définition émise par l'OLF (l'office québécois de la Langue Française) sur le pirate Informatique, 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[1], le piratage informatique, au sens juridique, est donc la reproduction sans droit d'un logiciel. Et ce sens différent de son sens courant qui échappe parfois à quelques professionnels du droit pour désigner le pirate.

B.2.Le « *Crasher* »

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[2].

B.3.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[3].

B.4.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.).

[1] J.-F. CASILE : « *Le Code Pénal Á L'épreuve De La Délinquance Informatique* », Thèse doctorat, Aix-Marseille,France, 2002, P24.
[2] M. CHAWKI, *Op*.cit, P. 34.
[3] Voir le lien suivant: http://fr.wikipedia.org/wiki/Cracker_(d%C3%A9plombeur_de_logiciels), consulté le 01/06/2018

B.5. 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.[1] Néanmoins, ils peuvent présenter parfois une menace réelle pour la sécurité des systèmes.

B.6. 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.[2]

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.[3]

I.4. La cybercriminalité, une 3e grande menace ?

« La cybercriminalité est la troisième grande menace pour les grandes puissances, après les armes chimiques, bactériologiques, et nucléaires».[4] *Colin ROSE*

D'après le raisonnement de Colin ROSE, spécialiste de la cybercriminalité pour la société écossaise Buchanan International, classe la cybercriminalité au troisième rang des menaces pour les grandes puissances, après les armes chimiques et bactériologiques et le nucléaire.

Exemple de l'évolution des menaces cyber favorisant cette criminalité en ligne, le bitcoin, monnaie virtuelle utilisable anonymement, est prisée par les cyber-délinquants mais aussi dans le blanchiment d'argent et le financement du terrorisme.

À l'heure où Internet s'immisce partout, y compris dans nos objets connectés du quotidien, et que le Dark Web monte en puissance, la cybercriminalité s'impose comme « la menace du XXIe siècle ». Affirme Mireille BALLESTRAZZI[5] (pour la Tribune dans une

[1] Ali AZZOUZI, « *Cybercriminalité au Maroc »,* Casablanca (Maroc), 2010, page 86.
[2] http://www.actimize.com/index.aspx?page=news196. consulté le 24/06/2018.
[3] M. CHAWKI, *Op*.cit, P. 35.
[4] COLIN Rose, spécialiste de la cybercriminalité pour la société écossaise Buchanan International (http://cyberpolice.over-blog.com/article-358465.html) consulté le 24/06/2018.
[5] Mireille BALLESTRAZZI occupe la fonction de directrice centrale de la police judiciaire et préside le comité exécutif d'Interpol depuis novembre 2012. (*Crédits : DR*).pour plus d'informations consulter le site www.latribune.fr /« *La cybercriminalité est la nouvelle menace du XXIe siècle* ».htm Propos recueillis par Sylvain ROLLAND, 26/07/2015.

interview lors du nouveau Complexe mondial Interpol pour l'innovation de Singapour, une forteresse high-tech consacrée à la lutte contre les cyber-menaces en 2015).

La cybercriminalité est clairement la nouvelle menace du XXIe siècle. Elle force les polices à repenser leurs moyens d'action, à se mettre au niveau techniquement et à développer des outils transnationaux, car l'échelle devient mondiale.

Le cyber-crime est d'autant plus difficile à appréhender qu'il prend des formes diverses et n'a, par définition, pas de frontières. Il peut s'agir d'apologie du terrorisme, de réseaux de pédopornographie ou de proxénétisme, ou encore d'attaques contre des systèmes de données, comme celle qu'a connue récemment TV5 Monde. Internet donne aussi aux malfaiteurs un nouveau terrain de jeu pour mettre en place des escroqueries comme la fraude à l'e-paiement, le blanchiment d'argent ou le trafic de stupéfiants.

Le cyberespace permet l'expression de menaces inédites par l'utilisation des nouvelles technologies, mais il étend aussi le périmètre des crimes « classiques ». Avec la démocratisation de l'accès à Internet et l'innovation constante autour des nouvelles technologies, la cybercriminalité devient un enjeu de société, à la fois pour les gouvernements, les entreprises et les citoyens. Et ce n'est que le début ; toutes les études tablent sur une augmentation significative du nombre de crimes liés à Internet dans les années et décennies à venir. Il s'agit d'un vrai défi pour les États et les polices du monde entier.

II/ Typologies, et techniques de la cybercriminalité

II.1. Typologie des cas de cybercriminalité

La synthèse de la typologie des phénomènes cybercriminels présentes les situations dans lesquelles les technologies sont objets, moyens et simples supports de phénomènes relevant de la cybercriminalité. Cette typologie englobe tous les domaines de vie où ce phénomène était l'élément causal de délinquance comme le montre le schéma n°.5.

Schéma N°5 **Typologies des cas de la cybercriminalité**

La technologie

I/ objets
- Atteintes aux systèmes d'information
  - -à la confidentialité
  - -à la disponibilité
  - -à l'intégrité
- Atteintes aux systèmes automatisés
- Atteintes aux systèmes de cryptologie

II/ moyen
- Atteintes aux intérêts des Etats et cyber-terrorisme
- Atteintes aux personnes
  - -aux libertés intellectuelles et à la vie privée
  - -aux traitements de données à caractère personnelle
  - -association de malfaiteurs informatiques
- Atteintes aux biens
  - -escroqueries sur réseaux
  - -spamming et fishing
  - -vol et usurpation d'identité
  - -escroqueries sur une information
  - -recel informatique
  - -abus de confiance
  - -blanchiment d'argent
- Atteintes à la propriété intellectuelle
- Infractions relatives aux moyens de paiements électroniques

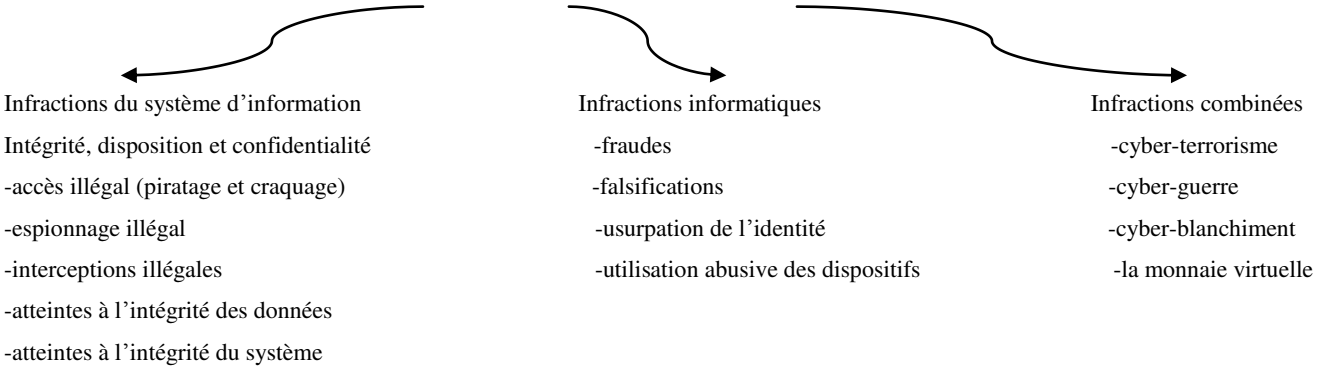
III/support
- Atteintes aux mineurs
- Infractions de presse
- Racisme en ligne
- Dérives sectaires
- Autres infraction : harcèlement….

Source : schéma établie par nos soins à partir du rapport de l'UIT 2009 .

II.2.Infractions de cybercriminalité touchants le système économique et financier

Comme notre thème de recherche est de traiter les aléas du phénomène de la cybercriminalité dans le secteur bancaire, nous allons essayer de faire ressortir et d'éclaircir les différentes infractions qui peuvent infecter le système bancaire et le système économique et financier en général, qu'on peut illustrer comme suit :

Schéma N°.6. : Infractions de cybercriminalité touchants le système financier



Source : schéma établie par nos soins à partir du rapport de l'UIT 2009.

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

A. 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 :

- **Accès illégal (*piratage, craquage*) :** Avec le développement d'Internet, Le « Hacking» (piratage), considéré comme l'une des infractions informatiques les plus anciennes[2], est devenu un phénomène de masse ; il désigne l'accès illégal à un ordinateur. Parmi les organisations qui ont été victimes de 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 ;
  - Création de site Internet d'espionnage (qu'on appelle aussi « Spoofing ») ;
  - Installation de logiciel ou matériel d'enregistrement de frappe.

[1] Rapport de l'UIT 2009, *O*p.cit, p21-69.
[2] Article de LEVY, "Hacking Offences, Australian Institute of Criminology", 2005.

- **Espionnage de données :** Lorsque le système est connecté à Internet, un pirate essayera de s'introduire et de saisir ces données. Pour accéder aux systèmes informatiques, les pirates utilisent diverses techniques :[1]
- L'utilisation de logiciels conçus pour rechercher les ports non protégés ;[2]
- L'utilisation de logiciels conçus pour contourner les mesures de protection ;
- L'ingénierie sociale.

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* ».

- **Interception illégale :** Elle représente l'interception des communications électroniques ou les transferts de données dans le but de récolter des informations. L'interception peut se faire par l'accès physique aux lignes de réseau (écoute téléphonique et surveillance des transmissions radios), ou par les services Internet (messageries électroniques, les discussions en ligne, voix IP, etc.).[3]
- **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 […][4] ».

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 altération -Par limitation d'accès -Par suppression

- **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 […][5] ». La destruction de fichiers, de 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 ».[6] Ce dernier se traduit par une saturation du site.[7] Les attaques informatiques s'appliquent également aux systèmes informatiques.

[1] SIEBER, Council of Europe Organised Crime Report 2004, P.88.
[2] EALY, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", P.9., voir : http://fr.wikipedia.org/wiki/Port_%28logiciel%29 consulté le 20/06/2018.
[3] Rapport « comprendre la cybercriminalité », *Op*.cit, 2009, P.28.
[4] 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..
[5] *Idem.*
[6] https://www.securiteinfo.com/attaques/hacking/dos.shtml. Consulté le 20/06/2018
[7] ENDERLIN Clément, Un focus sur la cybercriminalité, 2011, P.42.

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 ;[1]
- Les attaques par refus de services

B. 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.

- **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 :
  - La fraude bancaire ;
  - La fraude aux enchères en ligne **:** Les enchères en ligne sont des services de commerce électronique. Les plates-formes d'enchères ne peuvent pas distinguer entre les utilisateurs honnêtes et malfaiteurs, c'est ainsi que les fraudeurs profitent.
  - La fraude aux avances sur commission[2] **:** Ce type de fraudes consiste à envoyer des mails qui sollicitent l'aide d'un destinataire pour transférer de grosses sommes d'argent.
- **Falsification informatique :** Ce type d'infractions désigne la manipulation de documents numériques, elle comprend : [3]
- 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.

[1] SIEBER,« *Council of Europe Organised Crime Report 2004* », P.107. Egalement voir le rapport de l'UIT : « La cybercriminalité : guide pour les PED », 2009, P.34
[2] www.oriola.com consulté le 25/05/2018, Volume 21, Issue 3, P.237
[3] ITU Global Cybersecurity Agenda/ High-Level Expert Group, Global Strategic Report, 2008, page39.

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.

- **Usurpation d'identité:** Considéré comme une nouvelle criminalité instituée, par la loi d'orientation et de programmation, pour la performance de la sécurité intérieure (LOPPSI)[1]. Concrètement, l'usurpation d'identité consiste à utiliser sur Internet, sans votre accord, des informations permettant l'identification tel que :

  Nom et prénom -Numéro de sécurité sociale ou numéro de passeport
  Adresse électronique -Mots de passe de comptes non financier
  Numéro de téléphone -Mot de passe de comptes financiers

- **Utilisation abusive de dispositifs :** La diffamation ou la fraude en ligne, nécessitent qu'un ordinateur et un accès à un réseau et celles qui sont plus sophistiquées nécessitent l'utilisation de logiciels spécialisés. Les outils de deuxième génération rond ces opérations plus accessibles et facile, ils permettent d'automatiser de nombreux cyber-délit (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.

C. Infractions combinées

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

- Cyber-terrorisme : 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 ;
- Guerre numérique ou « *Cyber-Guerre* **» :** Il désigne l'utilisation des TIC pour mener une guerre dans le cyberespace. Il partage certaines caractéristiques avec le Cyber-terrorisme.
- Cyber blanchiment
- La monnaie virtuelle

II.3. Les techniques de la cybercriminalité

La cybercriminalité touche diverses atteintes aux biens : Téléchargement illégal, Hameçonnage ou phishing, Intrusions ou piratages des données, Différents types d'intrusions dans le système informatique par le biais de programmes malveillants : [2]

- Le ver : pour se propager entre ordinateurs avec des séries de codes informatiques ;

[1] 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 », France, 2011, P.49
[2] Bulletin 32 Cyber.pdf www.crft.dz.consulté le 02/06/2018

- Le virus : pour infecter d'autres programmes ;
- Le cheval de Troie : pour avoir un contrôle à distance de l'ordinateur infecté ;
- Les bombes logiques : pour détruire de façon différée ;
- L'attaque en déni de service : pour empêcher d'utiliser un service par saturation d'exécution de programmes ;
- Le spam : communication électronique, expédiée en masse à des fins publicitaires ou autres ;
- L'adware : pour afficher des bannières publicitaires ;
- Le spyware : pour installer un logiciel espion et imposer régulièrement des informations statistiques sur les habitudes de l'utilisateur ;
- L'ingénierie sociale **:** Elle est, aussi, appelée « *élicitassions* », 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 d'un utilisateur ses codes d'identification, mots de passe et références bancaires ;

III/ Impact de la cybercriminalité

Les pertes financières dues à la criminalité informatique et à la criminalité sur Internet sont importantes. Plusieurs études publiées récemment témoignent ainsi de l'impact économique majeur de la cybercriminalité. L'estimation des pertes financières pose le même problème que la production de statistiques sur la criminalité : il est difficile de savoir dans quelle mesure les chiffres publiés sont exacts, car il est probable que bien des personnes ne signalent pas les infractions dont elles sont victimes. Une étude réalisée par la CSIS (Center for Strategic and International Studies) qui met en lumière l'impact économique de la cybercriminalité dans nos sociétés. Son coût est estimé à près de 500 milliards de dollars.

L'estimation du coût de la cybercriminalité et du cyber espionnage engendrerait une perte annuelle de 100 milliards de dollars à l'économie américaine et une suppression de 508 000 emplois.[1]

On peut citer parmi les impacts indirects néfastes, les dommages causés à la réputation de l'entreprise, la perte de confiance des actionnaires, la perte d'avantages concurrentiels au travers de l'espionnage industriel, les pertes financières sur le long terme ou les conséquences de l'extorsion et de la divulgation de données.

[1] https://www.mag-securs.com/communiques/id/33116/la-cybercriminalite-coute-tres-cher-a-l-economie-mondiale.aspx consulté le 26/06/2018.

Le CSIS[1] a classé les impacts liés aux activités malveillantes comme suit :

- La perte de la propriété intellectuelle ;
- La perte de données sensibles de l'entreprise, incluant une éventuelle manipulation du marché boursier ;
- Les coûts d'opportunité, y compris les interruptions de service et la confiance réduite pour les activités en ligne ;
- Le coût supplémentaire de sécurisation des réseaux, l'assurance et les dommages d'une cyber-attaque ;
- L'atteinte à la réputation de l'entreprise piratée ;
- La diversité des actions cybercriminelles.

Conclusion

La cybercriminalité occupe une place grandissante dans un monde désormais exposé au développement des technologies de l'information et de la communication. L'avènement d'une société numérique incite chaque citoyen à s'interroger sur ces évolutions qui concernent tant l'intérêt général et les libertés individuelles que le droit, l'économie et les relations internationales.

[1] D'après le rapport du CSIS (*Center for Strategic and International Studies*) sponsorisée par McAfee http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf consulté le 24/05/2018.

Conclusion

Les Technologies de l'information et de la communication jouent un rôle de plus en plus important dans les vies professionnelles et personnelles de chacun. Malgré la bonne santé de l'économie liée aux technologies de l'information et de la communication, mais elles n'ont pas toujours une empreinte peinte en rose ou en vert respectivement sur la société et l'environnement. Le développement de l'usage d'Internet occasionne de nombreuses menaces sur le rayonnement économique des pays et leur image à l'extérieur, ainsi certains usagers très doués dans le domaine (hackers) utilisent ces TIC pour violer les secrets des gouvernements, des sociétés, des banques et des personnes. Mais l'impact négatif qui touche l'humanité entière est l'impact sur l'environnement.

La cybercriminalité fait partie des conduites les plus odieuses que l'on ait pu imaginer. Hélas, l'apparition de nouvelles technologies comme celle de l'internet a permis l'amplification de ce phénomène insupportable, au point que cette infraction est devenue l'une des sources majeures de profits pour les organisations criminelles. (*AZZOUZI A., 2010*).

Parallèlement à l'informatique et au digital, la cybercriminalité évolue sans cesse, avec des attaques toujours plus sophistiquées, ciblant des acteurs inhabituels comme les PME, banque… utilisant des outils récents comme le bitcoin… Les réponses à cette criminalité en ligne s'organisent, avec le travail du service hautement spécialisé de la police judiciaire, les nouvelles règles qui renforcent la sécurité des banques construites avec l'ANSSI, l'émergence du cyber-assurance….

En définitive, les problèmes de criminalité et d'insécurité s'adaptent à l'évolution de la société, avec les technologies de l'information et de la communication tandis que l'homme est sensé de penser en premier lieu à sa sécurité avant toute aventure technologique **«** *L'Homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique*[1]**»** *Albert EINSTEIN.*

[1] El AZZOUZI, A. (2010) : la cybercriminalité au Maroc, p.132.

Introduction

L'émergence récente du terme cybercriminalité pourrait laisser entendre que nous assistant à un phénomène nouveau à la fois à ses moyens et ses objectifs, mais en réalité se sont les techniques d'attaques qui évoluent et se complexifient [1]; dont les objectifs visés sont essentiellement de trois types : l'intérêt financier direct (*fraude par vol ou par manipulation de données bancaires*) ; la nuisance a l'établissement par l'atteinte à sa réputation (*sabotage, blocage, atteinte à l'image via la défiguration du site internet*) ou l'espionnage, qui peut être pratiqué par un concurrent ou une puissance économiques étrangère.

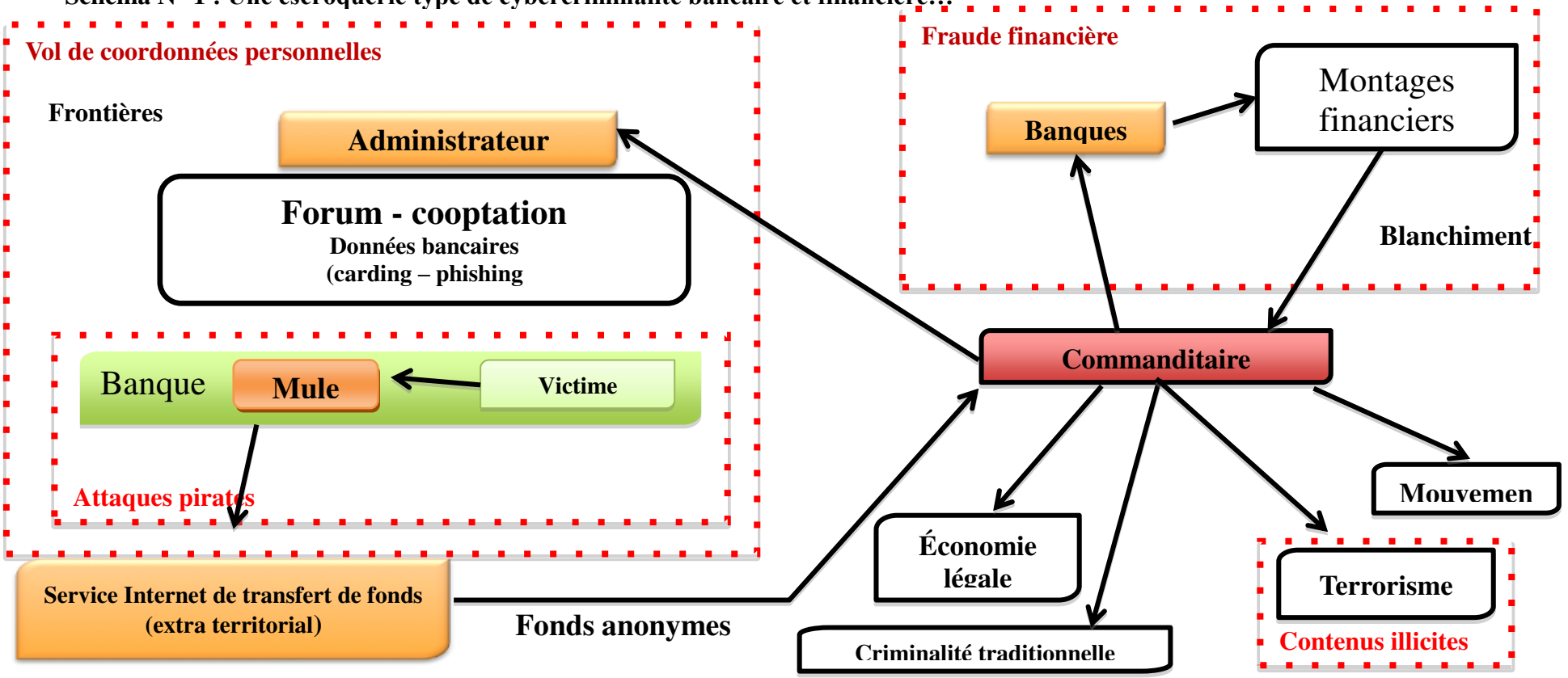
Depuis l'essor du e-commerce et de la banque en ligne au début des années 2000, les fraudeurs ont tenté d'usurper des données d'identification et des mots de passe de la clientèle (*carte de paiement ou comptes bancaires*), afin de réaliser à leur profit des paiements frauduleux. Des vols massifs de données de cartes ont ainsi pu être observés notamment aux Etats-Unis. L'usurpation de mots de passe de banque en ligne par phishing s'est également intensifiée. Le montant de la fraude est toutefois resté jusqu'à présent plutôt contenu notamment en Europe où le niveau de sécurité des techniques d'authentification a été constamment relevé.

Les attaques portantes atteintes à la confidentialité des données représentent aujourd'hui une menace forte, tant pour les établissements bancaires, de ce fait l'enjeu est majeur car le secteur financier joue un rôle clé dans le fonctionnement de l'économie, au point que l'atteinte à un établissement pourrait avoir des conséquences néfastes sur les opérations économiques courantes d'un pays entier. Or les menaces sont variées et leur sophistication s'accroit. En application d'une réglementation spécifique sur la sécurité des systèmes d'informations et en réponse à un environnement plus menaçant, les banques et les assurances adaptent et renforcent leur politique de prévention des risques liés à la cybercriminalité.

En effet, nous serons alors amenés à étudier en 1ère section les failles de sécurité auxquelles sont exposées les banques en retraçant l'image de la cybercriminalité bancaire et financière sur le terrain et le risque encouru face à cette menace, ensuite nous allons rechercher les moyens de lutte adaptés par les banque en 2ème section.

[1]Édouard FERNANDEZ BOLLO -, Secrétaire général, Autorité de contrôle prudentiel et de résolution (*ACPR*). Contact : Edouard.Fernandez-Bollosacpr.banque-france.fr. www.-institutions-financières-et-cybercriminalité.pdf consulté le 17/07/2018.

Schéma N° 1 : Une escroquerie type de cybercriminalité bancaire et financière…



Source: fichier power point ; www.definitiondelacybercriminalité.com; consulté le07/07/2018 formation trinôme; avril2009.

Section 1 : Les failles de sécurité dans le secteur bancaire et financier

La cybercriminalité bancaire est en croissance favorisée par les paiements à distance, et notamment sur le canal Internet. Elle exploite des modes opératoires originaux et complexes qui ne connaissent aucune limite territoriale. Sa nature par définition virtuelle favorise aussi de nouvelles formes plus complexes pour les procédures de blanchiment. La cybercriminalité financière doit aussi être considérée sous l'angle des détournements des flux financiers.

I/ La cybercriminalité bancaire et financière

La nouvelle théorie de l'intermédiation financière a permis d'expliquer les raisons d'être d'une banque par référence aux trois critères suivants : économiseur de coûts de transactions, délégateur de surveillance, producteur et assureur de liquidité. La banque constitue un domaine particulièrement privilégié, compte tenu de son rôle central dans le fonctionnement des économies (*octroi des crédits, mobilisation de l'épargne, financement des investissements*…).

Par ailleurs, afin d'affiner et renforcer son rôle bénéfique dans l'économie, le système bancaire s'émet d'accord de procéder à une libéralisation financière et d'appliquer la règle des trois D[1]; et suite aux innovations technologiques et la venue d'une troisième révolution(*TIC*); la dématérialisation des services et l'intégration d'internet dans le domaine bancaire est devenue une obligation pour tout établissement afin de répondre à la fois aux exigences de la clientèle, suivre et atteindre les objectifs de cette libéralisation financière.

Suivant ce raisonnement quelques soit l'impact des TIC sur le secteur bancaire (positif ou négatif) a une influence directe sur le secteur financier en général. Le climat actuel de l'économie montre qu'une Technologie à Usage Général (*TUG*); (*Ce point est bien détaillé dans le chapitre1, section1, p11.12*) ; et une libéralisation financière exercée dans un environnement institutionnel peu développé accentue la prolifération de nouvelles formes de délinquances et de phénomènes incontrôlables qui causent des risques et crises paralysants le système entier.

Un acte cybercriminel peut être aussi l'incarnation nouvelle d'une opération criminelle classique avec la seule différence, l'utilisation d'un ordinateur comme facilitateur. Parmi les actes de délinquance électronique les plus recensés dans le cyberespace, nous retenons

[1] La règle des trois D : Déréglementation ; Décloisonnement ; Désintermédiation.

l'escroquerie, les techniques de la fraude bancaire, le blanchiment de l'argent, le cyber-terrorisme sur l'internet.

Pour mieux comprendre l'infiltration de la cybercriminalité dans le secteur bancaire et financier nous allons traiter chacun à part.

I.1. La cybercriminalité bancaire

Depuis quelques années, l'activité des cybercriminels est de plus en plus effrénée. Et pour cause, Internet avance à pas de géant chaque jour et le nombre d'internautes ne cesse de grandir et les quantités de données personnelles avec. A cela, s'ajoute l'essor du e-commerce. Un cocktail explosif qui fait des heureux chez les pirates !

Trois méthodes sortent du lot et mérites d'être détaillées car elles sont massivement exploitées par les pirates informatiques : l'escroquerie, le phishing et les malwares. Ce sont en effet les **t**echniques les plus répandues et les plus efficaces actuellement. Pour finir, nous aborderont le carding « *physique* ».

A/ Faux ordres de virement (FOVI) : escroquerie

L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

Pour mettre en place ces fraudes aux ordres de virement (*FOVI*), les escrocs recueillent des informations (*réseaux sociaux, Google, presse spécialisée, registre du commerce, société.com*…) sur les entreprises ciblées. Des données précieuses qui leur permettront non seulement d'usurper, de manière crédible, l'identité d'un dirigeant de l'entreprise ou d'un de ses fournisseurs, mais aussi d'identifier la personne (*assistante de direction, comptable…)* avec qui entrer en contact (*téléphone, courriel, réseaux sociaux...)* pour lancer l'arnaque. Les attaques sont préparées, et se font lors de conditions favorables (*déplacement du dirigeant à l'étranger).*

Exemple :

Un individu se faisant passer pour le dirigeant (avec usurpation du n° d'appelant et modification de la voix, aujourd'hui techniquement possible), demandant à une assistante de faire un virement ''urgent et confidentiel''. Mise en œuvre de techniques d'intimidation, de flatterie (*''vous étiez très en beauté lors de la cérémonie à Paris avec votre robe rouge''*

(l'assistante portait effectivement une robe rouge photo publiée sur FB), de menace aussi si la personne ne s'exécute pas[1].

B/ Les techniques virtuelles

a) Hameçonnage : Il désigne les différentes techniques utilisées pour soustraire des informations sensibles. Le principe consiste non pas à utiliser une faille informatique mais une ''faille humaine'' en dupant les internautes par le biais d'un courriel (*phishing),* d'un appel (*vishing*) ou d'un sms (*smishing*) apparemment sûr (*voir annexe n°4*).

Il emprunte le plus souvent l'identité d'une entreprise de confiance et demande à l'internaute de mettre à jour des informations le concernant via un formulaire factice. Les pirates réussissent à obtenir identifiants, mots de passe ou encore données personnelles ou bancaires (numéros de client ou numéro de compte en banque). Conséquence : les hackers peuvent transférer directement de l'argent sur un autre compte.

Le phishing[2] : C'est vieux mais toujours très en vogue car le taux de retour de personnes trop crédules reste élevé… Le principe est d'envoyer un mail en se faisant passer pour une organisation connue et de confiance et de demander des renseignements confidentiels. Bien souvent, les pirates auront recours à des faux sites, plus ou moins réussis, qu'ils mettent en place à l'aide de kits de phishing achetés ou téléchargés sur la Toile.

Certains se spécialisent dans la création de ces derniers, afin de les rendre disponible sur le BlackMarket. Certains de ces sites sont de simples espaces extorqués à des sites légitimes après les avoir piratés via une faille Web ou serveur. L'URL est alors facilement détectable pour un oeil averti, et le taux de retour ne sera de ce fait pas très élevé. Un cybercriminel mieux organisé et plus doué tendra plutôt à monter un véritable piège, avec un vrai nom de domaine ressemblant en tout point avec celui d'une institution réelle mais aussi en poussant plus loin encore, par exemple en mettant en place un faux certificat SSL, faisant croire à un maximum d'internautes qu'ils se trouvent sur un site sécurisé, le tout grâce au fameux petit cadenas présent dans le navigateur de la victime…

Vous l'aurez compris, il faut impérativement vérifier tous les éléments d'un site afin de savoir si l'on a réellement sur le vrai ou une simple copie. Dans la mesure du possible,

[1] https://www.clusif.asso.fr consulté le 21/07/2018.

[2] https://www.pcsansvirus.com/pages/emsisoft-anti-malware/attention-aux-phishing-dis-hameconnage-et-vos-donnees-personnelles.html. Consulté le 21/07/2018

n'accédez jamais à un site bancaire en ligne via un lien présent dans un mail mais tapez toujours l'URL directement depuis votre navigateur.

b) Malwares [1] : De multiples types de malwares sont dangereux pour les données confidentielles (*voir annexe n°5*).

Les chevaux de Troie ou trojans. Ils sont capables de prendre subrepticement le contrôle des machines sans rendre compte. Ensuite, le pirate ayant la main dessus pourra espionner la vie numérique, et dérober des données critiques, telles que les identifiants bancaires ou les données de carte de crédit lors d'un paiement en ligne.

Les trojans bancaires sont très puissants et permettent des solutions sur mesure pour récupérer le plus de données possible : capture d'écran régulières sur les sites bancaires afin de voler les codes tapés sur les claviers virtuels, form grabber capturant les identifiants saisis au sein des formulaires Web ou encore vol de mots de passe enregistrés sur la machine.
Ensuite, les keyloggers font aussi des dégâts, bien que ces derniers soient de mieux en mieux détectés par les solutions de sécurités modernes. Ils permettent d'enregistrer en local chaque frappe au clavier en local puis de les envoyer sous diverses formes au pirate de manière régulière. Les keyloggers permettent de simplifier la tâche du vol en lui-même mais nécessite un gros travail de tri ensuite… C'est pourquoi les pirates préfèrent utiliser des « *form grabbers*», qui ne capture que les données les plus intéressantes : les identifiants.

Pour cela, le procédé se greffe sur le navigateur Web et sniffe le trafic des requêtes POST envoyées à la suite de la validation d'un formulaire en ligne. Des mots clés types sont alors utilisés pour filtrer et ne garder que ceux qui ont un intérêt.

Pour finir, les « *password stealer* » font aussi beaucoup de victimes. Ces malwares ciblent tous les logiciels installés sur votre machine pouvant stockés en local des identifiants utilisateurs. Et ils sont nombreux ! Les navigateurs Web, clients de messagerie et les clients FTP font partis des cibles prioritaires.

Les identifiants utilisateurs y sont stockés de manière chiffrée, dont l'algorithme diffère selon les logiciels. Les passwords stealers sont capable, lors de leur exécution, de localiser ces identifiants puis de les isoler et de les déchiffrer à la volée. Ensuite, il n'aura plus qu'à les envoyer discrètement au pirate via divers moyens plus ou moins efficaces : fichier texte sur un FTP, texte dans un e-mail ou encore via des requêtes HTTP vers une interface Web qui stockera les données en base de données.

[1] https://www.pcsansvirus.com.*Op*-cit.

En résumé, les techniques sont nombreuses et tout internaute est une cible potentielle. Il est non seulement nécessaire de posséder à une suite de sécurité installée et mis à jour sur son système mais aussi de savoir naviguer et télécharger de manière réfléchie et de ne pas tomber dans les nombreux pièges tendus par les pirates du Web.

Exemple :

Le Cheval de Troie : ‘’je rentre, je prends, je disparais…’’

Un hacker crée un site de logiciels très connus, gratuits (ex : retouche de photos, antivirus gratuit), dans lesquels il va introduire des logiciels malveillants…pendant l'installation du logiciel, le cyber-pirate va accéder à toutes les données en moins de 5 minutes (code secret, données bancaires) et pourra ainsi aller puiser dans le compte, en toute liberté.[1]

C/ Les techniques physiques

a) Le skimming (*carding physique*) [2]

Les techniques citées précédemment sont purement virtuelles et ne nécessites aucune intervention physique. Ce n'est pas le cas du skimming.

Dans ce cas, le pirate va se munir de matériel spécifique afin de piéger un distributeur automatique de billets (DAB) en y insérant son skimmer (*voir annexe n°6*). Le but est de copier les données de la bande magnétique de toute carte de crédit insérée dans ce dernier, et ce, en sans que l'utilisateur s'en aperçoive. Afin d'intercepter le précieux code confidentiel à 4 chiffres, un clavier piégé peut aussi être mis en place.

Une fois les données enregistrées, le pirate va pouvoir à l'aide d'autre matériel, transférer les données dans des cartes vierges, prévues à cet effet. Et voilà, le tour est joué ! Il va ensuite pouvoir l'utiliser un peu partout sans être inquiété.

Exemple :

Yescard et payements frauduleux

La yescard est une carte à puce programmable qui permettait de faire des transactions d'achats sur quelques types d'automates de paiement électronique. La réflexion « théorique » a donné lieu à une fraude organisée avec un préjudice de plusieurs MF mais très localisée à quelques départements.[3]

b) Fraude à la carte bancaire

[1] Panorama clusif 2001.
[2] https://www.pcsansvirus.com.*Op*-cit.
[3] Panorama *O*p.cit.

Une fraude de carte bancaire correspond à une usurpation d'identité bancaire[1]. 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 par 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 internet sur des sites peu ou pas sécurisés. Les fraudes à la carte bancaire, dans le monde, a conduit à des détournements et pertes colossales pour certains pays.

Le phénomène de fraude à la carte bancaire est en évolution constante. Certes l'avènement de l'internet grand public a favorisé l'utilisation frauduleuse des coordonnées bancaires sur les sites marchands. Mais la fraude à la carte bancaire sur le web n'est rien en comparaison avec la fraude offline. En effet, le paiement par carte bancaire sur l'internet reste globalement un phénomène mineur par rapport au total des opérations réalisées par cartes physiquement. L'internet est rarement le lieu d'origine de la compromission des informations bancaires de l'acheteur. Selon une étude réalisée par FIA-NET[2], les données dérobées le sont le plus souvent dans le monde physique et l'internet est avant tout un lieu d'utilisation de ces informations bancaires.[3]

- **Scénario de la fraude lors de l'utilisation de la carte bancaire** *(Voir annexe n°7)*
  - Le client insère sa carte bancaire dans la fente et tape son NIP ;
  - L'écran demande le montant du retrait ;
  - Le client tape le montant du retrait et confirme ;
  - Le guichet crée une transaction et l'envoie au serveur transactionnel ;
  - Le serveur vérifie l'authenticité de la transaction et la relaie aux services financiers ;
  - La transaction est confirmée ;
  - Le guichet demande au client de retirer sa carte bancaire ;
  - Le guichet remet l'argent au client et imprime un relevé de transaction.

La fraude aux cartes peut s'opérer au niveau technologique : fausse goulotte pour lire la piste magnétique, caméra pour enregistrer la composition du code.

I.2 .La cybercriminalité financière

Sur l'internet, en raison notamment de la multiplication des banques en ligne, des casinos virtuels, des sites de paris en ligne et des possibilités de placements boursiers en ligne,

[1] Voir le lien suivant : http://www.certissim.com/fraude.html. Consulté le 21/07/2018.
[2] FIA-NET : http://static.fianet.com/__docs/livre_blanc_juin-2008.pdf consulté 21/07/2018.
[3] FIA-NET « La fraude à la carte bancaire : le livre blanc 2008 », http://static.fianet.com/__docs/livre_blanc_juin-2008.pdf consulté 21/07/2018.

les possibilités de blanchiment d'argent sont illimitées. Ainsi, transférer des capitaux sur le web est devenu une activité fleurissante. Les intermédiaires recrutés sont qualifiés de «mules» et peuvent gagner une somme d'argent considérable, en toute illégalité.[1]

Avec ces modes opératoires, les activités cybercriminelles demeurent incontrôlables et les poursuites en justice se révèlent parfois impossibles.

Les diverses mafias se sont logiquement tournées vers la Toile pour l'activité de blanchiment de l'argent. D'abord, la monnaie virtuelle joue un rôle central dans le fonctionnement des black markets. Elle est insaisissable, difficile à tracer et permet aux cybercriminels, en leur garantissant l'anonymat, d'effectuer leurs transactions sans risque. Mais les bénéfices des ventes sur les marchés noirs de la cybercriminalité ne restent pas longtemps virtuels. Le vendeur devra, pour récupérer le résultat de ses ventes, faire appel à différents acteurs. L'économie souterraine de la cybercriminalité possède, comme pour le trafic de drogue, ses propres mules.

La cybercriminalité rejoint dès lors la criminalité classique qui utilise aussi majoritairement ces deux procédés afin de blanchir l'argent issu d'activités frauduleuses.

A/Les principales étapes de procédé [2]

- Ciblage de la victime ;
- Courriel argumenté usurpé avec invitation à ouvrir un fichier pourvu d'un code malveillant ;
- Courriers postaux classiques ou fax ;
- Ingénierie sociale par flatterie ou pression - usurpation du numéro de téléphone et de l'adresse de messagerie ;
- Utilisation des réseaux sociaux pour récolter des informations (*sur l'entreprise, les dirigeants, les salariés*) ;
- Contact avec la banque : courriel et/ou n° de téléphone usurpé pour procéder au virement à l'étranger ;
- Répartition rapide des montants et blanchiment ;
- Exfiltration des données : contrôle des flux – cryptage ;
- Effacement des traces.

B/ La monnaie virtuelle

[1] Les actes du forum, 5e Forum international de la cyber-sécurité, cyberespace, enjeu de souveraineté et de sécurité, FIC, France ,2013.
[2] www.luttecontrelacybercriminalité.com consulté le 05/07/2018.

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. Dans son premier livre blanc[1]sur les marchés noirs de la cybercriminalité, CEIS relevait la place essentielle des monnaies virtuelles comme pilier de l'économie des black markets.

Le rôle des monnaies virtuelles et l'analyse des liens entre cybercriminalité et criminalité physique traditionnelle y avaient déjà fait l'objet d'une attention particulière.

La monnaie virtuelle utilisée dans les marchés noirs de la cybercriminalité – à ne pas confondre avec la monnaie virtuelle servant dans les jeux multi-joueurs en ligne ou de simulation comme Second Life – est une solution qui permet, grâce au porte-monnaie virtuel qui s'y rattache, de réaliser des achats en ligne sans communiquer ses coordonnées bancaires Initialement prévue pour simplifier les transactions - légales - sur Internet (pour les internautes ne disposant pas de carte bancaire ou ne voulant pas l'utiliser), son utilisation présente des avantages non-négligeables pour le cybercriminel : simplicité, anonymat et opacité, fiabilité et sécurité.

A l'époque, les cybercriminels s'étaient accordés sur l'utilisation d'une monnaie virtuelle en particulier : Liberty Reserve. Depuis, les choses ont évolué : Liberty Reserve est tombé et les évènements se sont enchainés (saisies de Bitcoins, chute du marché Silk Road…). Et si plusieurs monnaies semblent avoir pris la relève, les pouvoirs publics font désormais de l'observation des flux des monnaies virtuelles l'un des piliers de la lutte contre la cybercriminalité. 28 mai 2013, le Procureur de New York annonçait la mise en accusation de Liberty Reserve et de sept de ses membres fondateurs et administrateurs pour conspiration de blanchiment d'argent, transfert de fonds d'origine criminelle et conspiration et exercice de la profession d'intermédiaire financier sans licence[2].

Les forces de l'ordre de 17 pays ont été impliquées dans l'enquête et l'arrestation des fondateurs et administrateurs de Liberty Reserve. En parallèle de leur arrestation, cinq noms de domaine (*celui de Liberty Reserve et ceux de quatre échangeurs*) ont été saisis et 45 comptes bancaires ont été gelés.

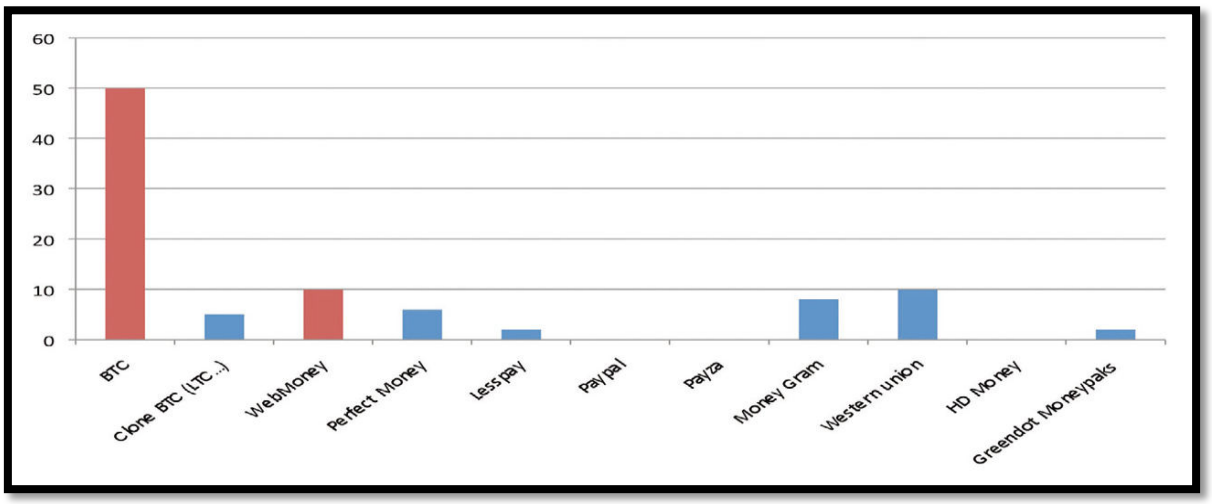
[1] Voir « *Les marchés noirs de la cybercriminalité* », CEIS, Juin 2011. Téléchargeable ici : http://www.secuinsight.fr/livre-blanc-blackmarkets/lb.pdf consulté le 16/07/2018.
[2] United States v. Liberty Reserve and al. Indictment - Redacted, voir www.ceis.com consulté le 16/07/2018.

D'après le Procureur, Liberty Reserve était devenu « *un carrefour financier du monde du cyber-crime, facilitant un vaste éventail d'activités criminelles en ligne, fraude à la carte bancaire, vol d'identité, fraude à l'investissement, piratage informatique…* »[1].

PERFECT MONEY est un système de paiement en ligne créé en 2007 qui propose également sa propre monnaie virtuelle. Les soupçons pesant sur l'usage à des fins cybercriminelles de Perfect Money se sont multipliés depuis la chute de Liberty Reserve.

Plusieurs personnes ont dénoncé son utilisation croissante par les cybercriminels, allant jusqu'à affirmer que Perfect Money avait remplacé Liberty Reserve[2].

Graphe.1. : Face à l'absence de fiabilité de Perfect Money, les cybercriminels se tournent vers d'autres outils.



Source : CEIS

Western Union et Money Gram sont toujours présents. Mais sur le plan des monnaies virtuelles, Lesspay, Webmoney, Bitcoin semblent prendre la relève.C'est Bitcoin, crypto-monnaie totalement décentralisée, en peer to peer, qui se taille la part du lion. Bitcoin est soit la seule monnaie acceptée, soit la monnaie privilégiée. La plupart, déçus de Perfect Money, encouragent vivement son usage. Ils recommandent vivement l'usage de Lesspay.cc en remplacement de Perfect Money

- **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

[1] *Ibid.*
[2] http://www.reuters.com/article/2013/08/09/net-us-cybercrime-digital-currency-idUSBRE9780GM20130809 ; consulté le 20/072018.

d'échanger des biens et services entre les utilisations sans avoir recours à la monnaie légale[1].

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*.[2]

- **Une monnaie en p2p**

Une crypto-monnaie repose sur le principe du pair-à-pair (P2P), s'appuyant sur la participation de ses utilisateurs pour valider les transactions. Celles-ci sont faites d'un portefeuille virtuel à un autre, identifié par des codes ou adresses uniques. L'anonymat des utilisateurs dépend de la traçabilité des transactions, toutes enregistrées dans un historique (*blockchain*). Bien qu'anonyme, chaque portefeuille virtuel peut donc cependant être tracé. Les transactions sont validées de manière aléatoire et tournante par un ordinateur du réseau d'utilisation.

- **Bitcoin et ses clones**

- 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 ;
- 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[3] : 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.

[1] 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.banquefrance.fr, PDF grandes dates /Focus-10-stabilite-financiere.pdf. Consulté le 20/07/2018.

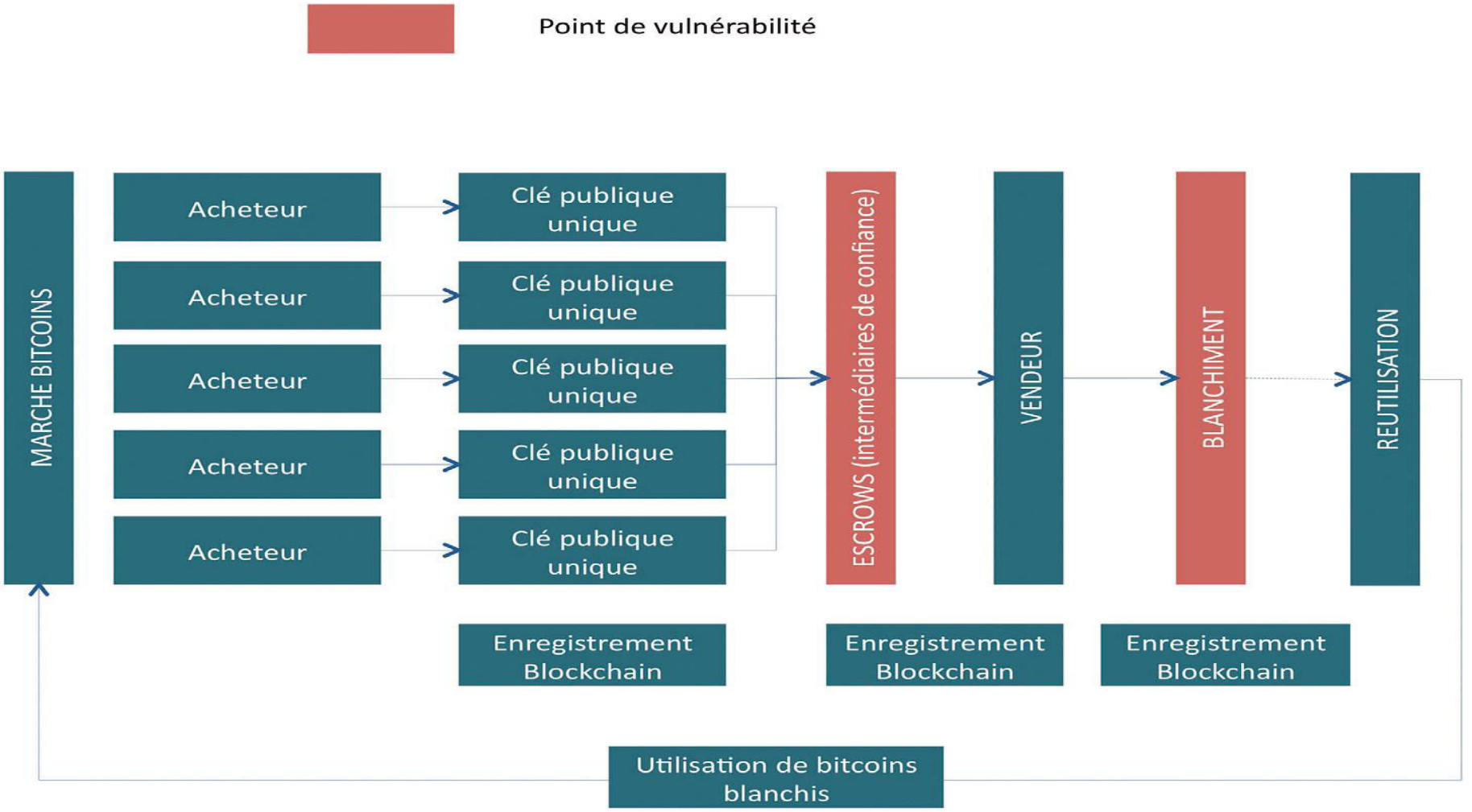
[2] Voir le document : www.woda.com , « *Money Laundering Techniques With Electronic Payment Systems*», Information &Security, Vol. 18, 2006, P.40. consulté 16/07/2018.

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

- **L'usage de Bitcoin par les cybercriminels**

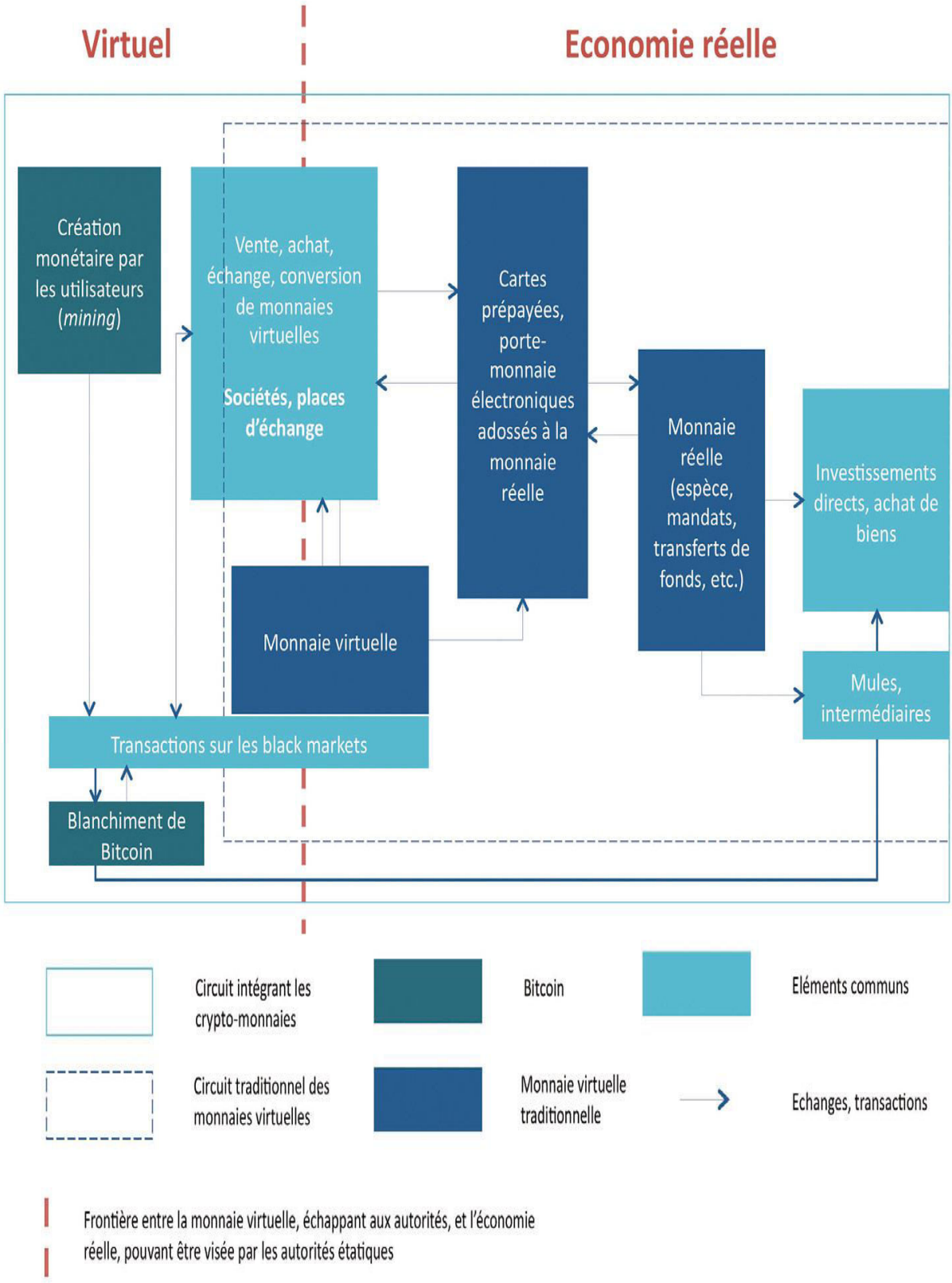
Outre sa simplicité d'accès et d'utilisation, Bitcoin répond aux principales exigences des cybercriminels. Anonyme, cette monnaie virtuelle indépendante de toute banque centrale rassure les déçus de WebMoney, Liberty Reserve puis Perfect Money. Déjà, en 2010 des sénateurs américains et des lobbyistes allemands soulevaient l'absence de traçabilité de la crypto-monnaie. Le fonctionnement de Bitcoin permet cependant de nuancer cette affirmation.

Schéma .2. : Blanchiment de Bitcoins



Source : The BTC Fog Company

Schéma.3. : Circuit de la monnaie virtuelle au cœur de la cybercriminalité



Source : www.ceis.eu

C/Le cyber-blanchiment d'argent[1]

Le blanchiment d'argent est le processus consistant à dissimuler la source de l'argent ou des biens tirés d'activités criminelles. Une grande variété d'activités illégales est motivée par le profit, notamment le trafic de stupéfiants, la contrebande, la fraude, l'extorsion de fonds, la corruption et la cybercriminalité. L'enjeu financier est important - quelque 500 milliards à un billion de dollars américains dans le monde entier chaque année[2].

Sur l'internet, les possibilités de blanchiment d'argent sont illimitées en raison de la multiplication des banques en ligne, des casinos virtuels, les possibilités de placements boursiers en ligne, et le transfert des capitaux sur le web. Les intermédiaires recrutés sont qualifiés de «*mules*» et peuvent gagner une somme d'argent considérable, en toute illégalité. Avec ces modes opératoires, les activités cybercriminelles demeurent incontrôlables et les poursuites en justice se révèlent parfois impossibles[3].

En outre, compte tenue de l'implication de la planète toute entière dans la lutte contre le financement du terrorisme international, sous l'impulsion des Etats-Unis, l'argent sale provenant des activités criminelles ne peut plus circuler librement, même dans les paradis fiscaux[4]. Par conséquent, les diverses mafias se sont logiquement tournées vers la Toile pour l'activité de blanchiment de l'argent.

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

C.1 Les casinos en ligne

Le recours aux jeux de hasard en ligne demeure une tendance sérieuse en matière de blanchiment d'argent. Les casinos en ligne sont devenus les terrains de prédilection des organisations mafieuses modernes constate le Groupe d'Action Financière[5] (*GAFI*). Ils permettent aux cybercriminels de placer en toute impunité leur argent sale, et d'encaisser en retour les gains de jeu officiels. La création de tels sites se fait en toute illégalité.

---

[1] Ali EL AZZOUZI, « *La cybercriminalité au Maroc* », Casablanca, Juin 2010.
[2] Centre d'analyse des opérations et déclarations financières au Canada (*CANAFE*). http://www.canafe-fintrac.gc.ca/intro-fra.asp consulté le 24/07/2018.
[3] Solange GHERNAOUTI-HELIE « *La cybercriminalité : Le visible et l'invisible* », collection le savoir suisse, Edition2009, Page 101.
[4] http://cybercriminalite.wordpress.com/2008/11/30/internet-jeux-en-ligne-blanchiment-dargent-un-triodevastateur
[5] Le Groupe d'Action financière (*GAFI*) est un organisme intergouvernemental visant à développer et promouvoir des politiques nationales et internationales afin de lutter contre le blanchiment de capitaux et le financement du terrorisme. http://www.fatfgafi.org/pages/0,3417,fr_32250379_32235720_33631745_1_1_1_1,00.html.Consulté le 17/07/2018.

Ceux-ci sont qualifiés de « *sauvages* », très mobiles puisqu'ils changent constamment de pays et de serveur, afin de brouiller les pistes. Selon une récente étude de McAfee, plus 87 % des sites de jeux de hasard proposés sur l'internet réalisent une activité clandestine (sans licence)[1].

L'absence de cadre juridique permet à quiconque d'enregistrer un site web dans l'anonymat puis de facturer les clients via un compte bancaire anonyme dans un paradis fiscal ou un système monétaire virtuel.

C.2 Les mules

A l'origine le mot « *mule* » est utilisé dans le jargon du trafic de stupéfiant pour désigner toute personne chargée de faire transiter des produits illicites à travers les frontières. L'économie souterraine de la cybercriminalité possède aussi ses propres mules. Il s'agit des individus recrutés via l'internet pour servir d'intermédiaires afin de récupérer les fonds illicitement. En contrepartie des opérations de transferts de fonds dont elle aura la charge, la mule reçoit à titre de commission entre 5 et 10% du montant transféré. Les fonds en question sont retirés par la mule sous forme de liquide après les avoir reçus sur son propre compte bancaire et renvoyés par la suite aux cybercriminels à l'aide de services de transfert d'argent tels que Webmoney, E-Gold, Western Union, MoneyGram, PayPal, etc.

Le recrutement des mules s'effectue généralement via l'envoi de spam. Le destinataire se voit proposer de «*devenir partenaire*» d'une société respectable. De telles offres figurent aussi de plus en plus sur des sites de recherche d'emploi parfaitement légitimes. En novembre 2008, le site www.bobbear.co.uk consacré à la dénonciation des sites frauduleux impliqués dans le recrutement de mules, recensait 193 offres d'emploi en ligne consacrées au recrutement de mules[2].

Pour mieux illustrer la mécanique derrière l'implication des mules, analysons à présent les deux scénarios suivants[3] :

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

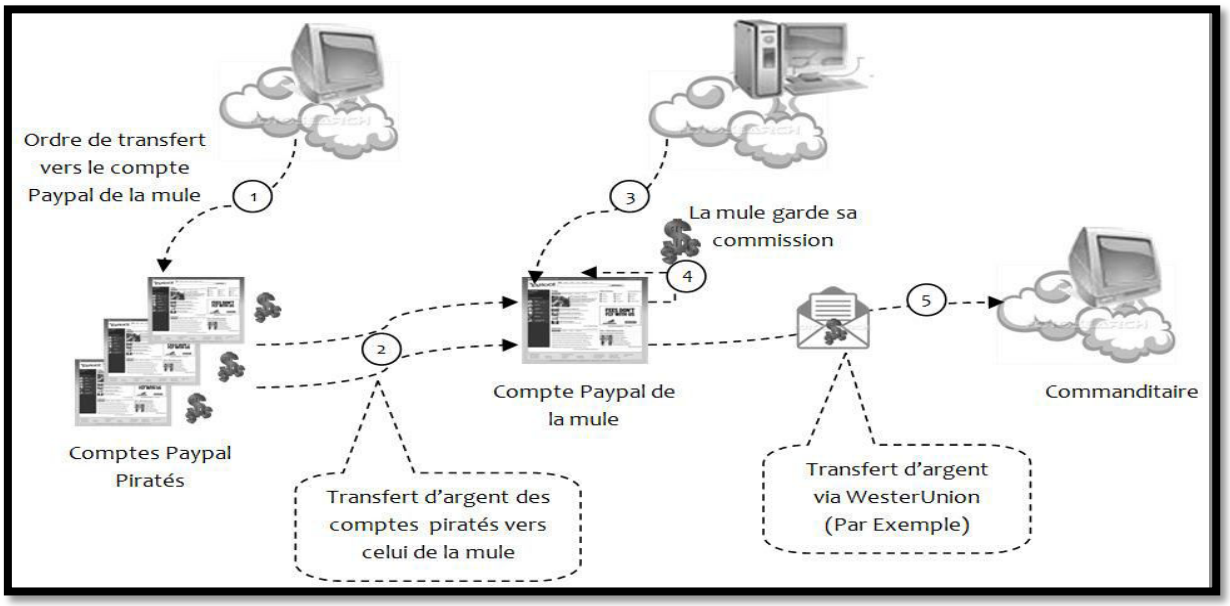
---

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

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

[3] Source : Ces deux scénarios ainsi que les schémas correspondants ont été repris intégralement à partir du blog Sécurité de Orange Business Services. Article « *Recrutement de "mules" : Petit cas d'espèce et schémas d'utilisation* », Jean-François Audenard. http://blogs.orange-business.com/securite/2009/03/recrutement-de-mules-petit-cas-despece-et-schemasdutilisation.html.consulté le 17/07/2018

Figure.1. : Exemple de blanchiment d'argent via une mule[1]



1. Le commanditaire se connecte sur les comptes PayPal volés

2. Le commanditaire transfère l'argent depuis les comptes PayPal compromis vers celui de la mule.

3. La mule accède à son compte PayPal

4. La mule provisionne son compte bancaire classique à partir de l'argent de son compte PayPal tout en gardant une commission prédéfinie.

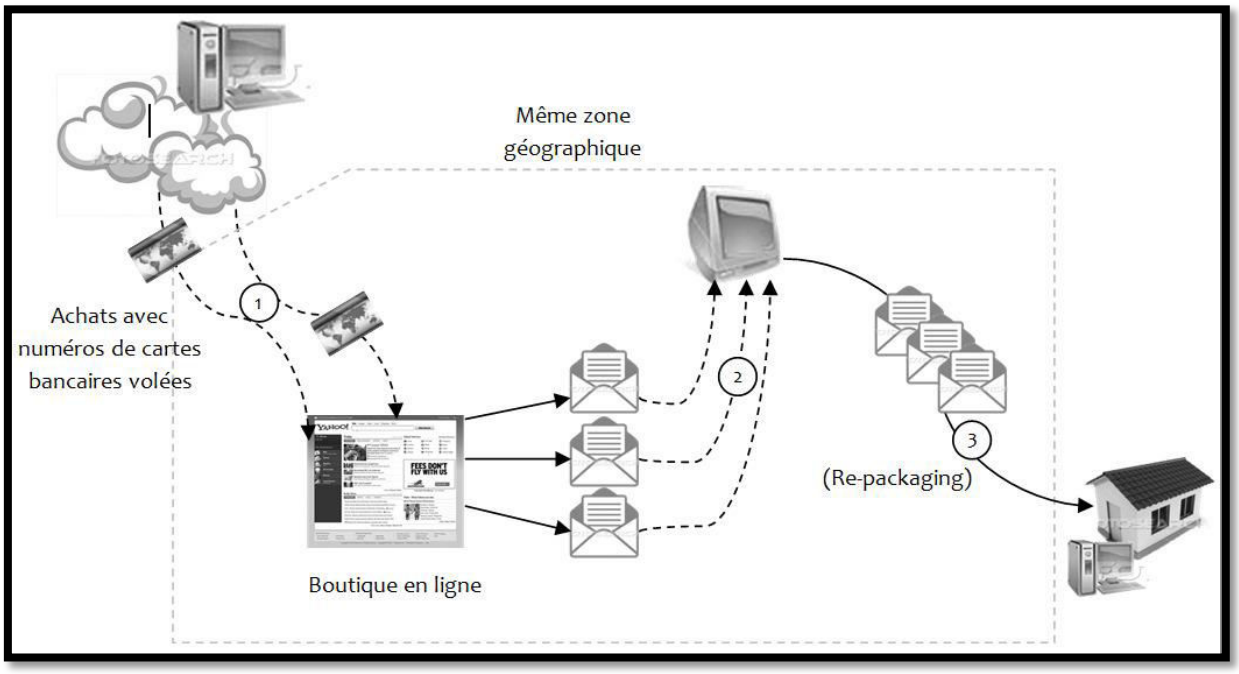
5. Elle envoie un mandat (ici via Western Union) à l'adresse indiquée par le commanditaire.

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

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

[1] Orange Business Services – Blog Sécurité – Jean-François Audenard http://blogs.orangebusiness.com/securite/ consulté le 17/07/2018.

Figure.2. : Réexpédition de marchandises "douteuses" par une mule[1].



1. Le commanditaire achète des biens ou marchandises en utilisant des numéros de cartes bancaires volés. Les marchandises sont livrées à la mule. Typiquement, la livraison est faite à une mule résidant dans le même pays que celui des cartes bancaires, ce afin de réduire la détection éventuelle.

2. La mule effectue un éventuel regroupement des marchandises (ou un déballage/réemballage sous forme de cadeaux) et les envoie au commanditaire.

3. Les frais d'envoi sont typiquement payés à la mule via un transfert d'argent depuis un compte bancaire volé.

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

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

D/ Le cyber-terrorisme

Le cyber-terrorisme est un terme controversé. Il peut être défini comme l'utilisation de l'information et du contrôle des systèmes d'information, par des groupes organisés ou par un individu, comme arme stratégique pour exercer des pressions et intimider l'adversaire[2].

[1] http://blogs.orangebusiness.com/securite/ consulté le 17/07/2018.
[2] Provient de l'Office Québécois de la Langue Française (OQLF) http://www.olf.gouv.qc.ca/ consulté le 17/07/2018

Il peut s'agir de manipulation de l'information, de désinformation, d'infiltration de réseaux, de sabotage des infrastructures télécoms, de perturbation des services publics etc.

La cybercriminalité peut donc avoir une dimension terroriste. Selon un rapport de l'Intelligence Advanced Research Projects Activity[1] (IARPA), le cyber-terrorisme peut se manifester à plusieurs niveaux. Il en a identifié cinq[2] :

1. Les communications secrètes : C'est l'un des aspects les plus visibles. Les terroristes utilisent le cyberespace comme outil de communication.
2. Entraînement: Le caractère de plus en plus réel des mondes virtuels, ainsi que leur caractère modulable (la possibilité de créer des environnements spécifiques) permet aisément aux terroristes de simuler une attaque (avant de la mettre en œuvre dans le monde réel).
3. Transfert/Blanchiment d'Argent: Il est désormais possible pour des groupes terroristes de transférer des fonds de manière virtuelle et de les convertir ensuite, au besoin, en argent réel. L'argent est ainsi blanchi par l'intermédiaire de bureaux de change, de courtiers ou agents de change, des sociétés écrans, etc…
4. Cyber-attaques: Jusqu'à une date récente, la cyber-guerre était considérée comme étant une simple vision virtuelle sans conséquences réelles.
5. Guerre Informationnelle: Les terroristes peuvent faire circuler leur propagande et recruter de nouveau membres dans un univers qui ressemble encore largement au "wild west", selon l'IARPA.

II/La cybercriminalité est un risque systémique pour la banque ?

Plus que pour les autres industries, la menace informatique constitue un danger réel pour les établissements de crédit. Or, les banques ont un devoir de sécurité vis-à-vis d'elles-mêmes, de leurs clients et du système bancaire.

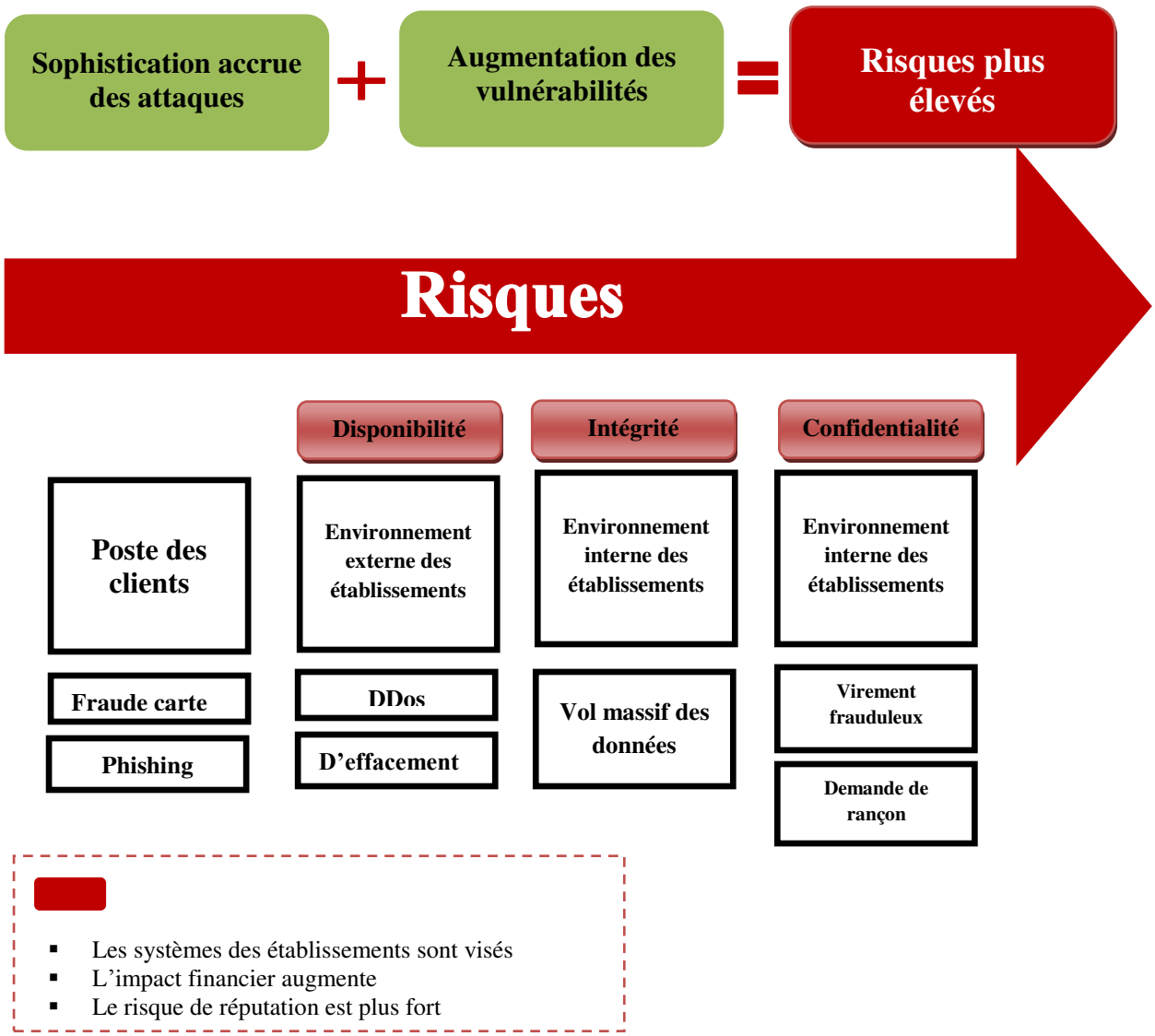
Les enquêtes réalisées, notamment par le S.G.C.B., indiquent que le niveau de sécurité des systèmes informatiques des établissements de crédit est encore perfectible vue leur exposition aux différents risques. Initialement basées sur une approche purement financière des risques, les recommandations du comité Bâle ont été profondément étendues en 2004 via l'accord Bâle II. Ces recommandations sont mises en œuvre par l'immense majorité des établissements financiers au niveau mondial.

[1] IARPA est une agence gouvernementale américaine spécialisée dans la très haute technologie de communication, équivalent de la DARPA militaire pour les services de renseignement.
[2] Solange GHERNAOUTI-HELIE, *Op*.cit. Page 88.

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

II.1. Un risque cyber qui renforce la nécessaire attention[1]

Schéma N°4 : Evolution du risque de réputation



Source : *Les attentes de l'ACPR sur le risque informatique* »
« *Cyber-sécurité & Fraude : un risque majeur pour l'industrie financière* », Paris, le 12 février 2018.

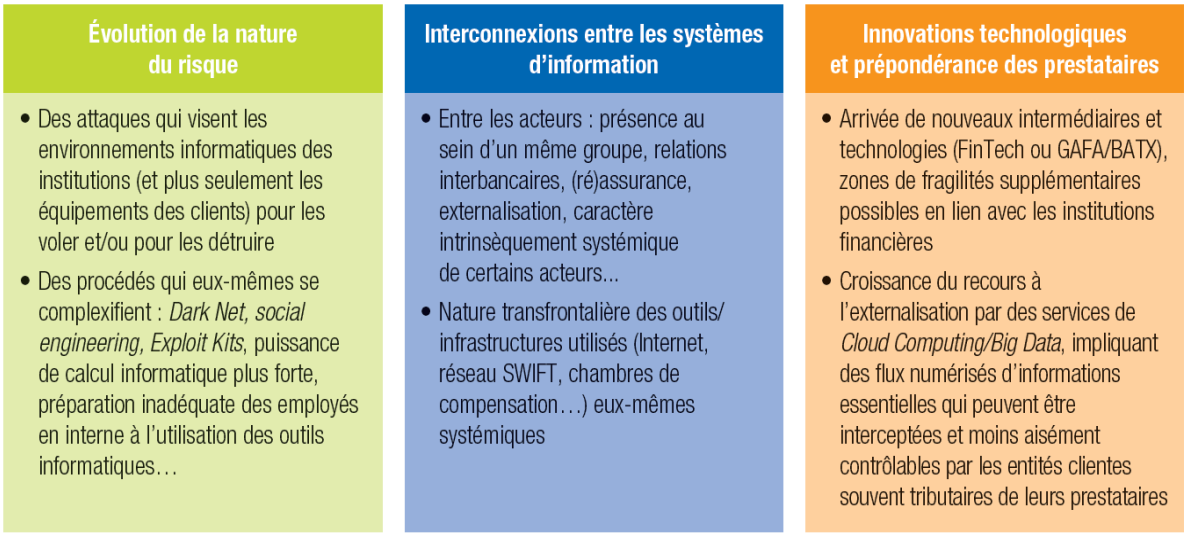
[1] Frédéric VISNOVSKY, Secrétaire général adjoint, « *Les attentes de l'ACPR sur le risque informatique* »
« *Cyber-sécurité & Fraude : un risque majeur pour l'industrie financière* », Paris, le 12 février 2018.

Pour les établissements de crédit, l'informatique est devenue un "outil de production" principal et "incontournable" : les valeurs monétaires, dématérialisées, sont contenues, stockées, transportées, valorisées grâce à elle.

De plus, l'usage de plus en plus intense des systèmes informatiques augmente les dangers d'une divulgation d'informations confidentielles : non seulement on peut prélever, plus facilement et sous une forme pouvant être traitée par un autre ordinateur, une quantité beaucoup plus importante de données, mais un accès non autorisé peut se produire sans laisser de trace apparente et les risques encourus demeurer ainsi cachés pendant un certain temps, ce qui accroît leur magnitude.

II.2.Un risque potentiellement systémique[1]

Figure N°.3. : Propagation vers un risque systémique



Source : *Banque de France - Évaluation des risques du système financier français • Décembre 2017.*

L'informatique joue un rôle stratégique dans les banques, en raison des répercussions pour l'établissement dans lequel une difficulté apparaîtrait, mais aussi pour ses clients si les problèmes rencontrés sont suffisamment importants pour que des données disparaissent ou, plus grave, que les règlements de toute nature et notamment le remboursement des dépôts soient compromis.

Les risques induits par les défaillances informatiques sont plus élevés dans les établissements de crédit que pour d'autres secteurs de l'économie parce qu'ils peuvent également entraîner des conséquences fâcheuses pour les autres établissements qui sont en relation avec lui, et même, à la limite, avoir des répercussions pour la place et pour l'économie nationale si l'incident était de nature à provoquer un "risque systémique".

[1] Banque de France - Évaluation des risques du système financier français • Décembre 2017.

Si une entreprise industrielle perd son informatique, il lui restera, en stock, sa production, qu'elle pourra toujours vendre en attendant de rebâtir un nouveau système informatique : celui-ci étant moins intégré au mode de production, une reprise plus ou moins totale de l'activité de l'entreprise pourra intervenir.

En revanche, la banque possède la particularité d'avoir l'argent en "*Input*" et en "*Output*". Si elle perd toute son informatique, comme sa matière première est "l'argent x Information", -ce qui est immatériel-, elle aura perdu et son outil de production principal, et sa mémoire. Ce sont l'information, la valorisation et le transfert d'une forme financière à une autre qui construisent sa valeur ajoutée.

En outre, une banque travaille avec l'argent des autres agents économiques et financiers. Ses difficultés, nécessairement connues si elles sont graves, risquent très vite d'amener les autres établissements de crédit à lui couper ses lignes de refinancement, ou ses clients à retirer ou à ne pas renouveler leurs dépôts, ce qui entraînerait une crise de liquidité rapide. Comme les masses financières en jeu peuvent être très importantes et que les systèmes bancaires sont très interdépendants, une difficulté technique rencontrée par une banque risque de se répercuter rapidement sur ses contreparties, confrères ou clientèle, voire, dans les cas extrêmes, sur l'ensemble du système financier.

Assurer la sécurité des systèmes d'information, de traitement, de conservation et de transferts des flux financiers est donc impératif dans les économies interdépendantes où les "chocs" sont susceptibles d'avoir très rapidement des conséquences importantes et de constituer l'un des vecteurs possibles de transmission du risque, pouvant, à la limite, créer un risque systémique. De ce fait, la sécurité de l'information est devenue une exigence essentielle.[1]

[1] www.commissionbancaire.fr , le livre blanc, France, 1996.

Conclusion

Les attaques contre le secteur financier ne sont pas une nouveauté, il s'agit même d'un secteur de prédilection *(voir annexe n°8)* pour les pirates agissant à des fins vénales. Mais ces dernières années nous avons assisté à une diversification et à une intensification de ces attaques. En effet, au cours des années passées, plusieurs attaques majeures, motivées par l'attrait de gains financiers importants, ont été réalisées contre des banques de détail et d'investissement mais également contre des banques centrales.

Depuis l'existence d'Internet, les failles des systèmes accessibles directement aux clients ont été largement exploitées par les cybercriminels qui ont continué à faire évoluer leurs techniques.

En évolution permanente, à l'image de l'informatique mais aussi du digital, la cybercriminalité laisse constamment apparaître de nouvelles menaces qui nécessitent de trouver de nouvelles réponses contre un risque désormais considéré comme systémique pour le secteur financier lié notamment aux opérations de blanchiment de l'argent électronique et au financement du terrorisme.

Section 2 : Activités de veille pour lutter contre la cybercriminalité.

Les attaques dirigées contre les institutions financières sont restées jusqu'ici relativement limitées dans leurs effets, ce qui peut s'expliquer par une mobilisation forte des établissements tant dans le domaine de la prévention que dans celui de la réaction.

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

I/ La sécurité du système d'information

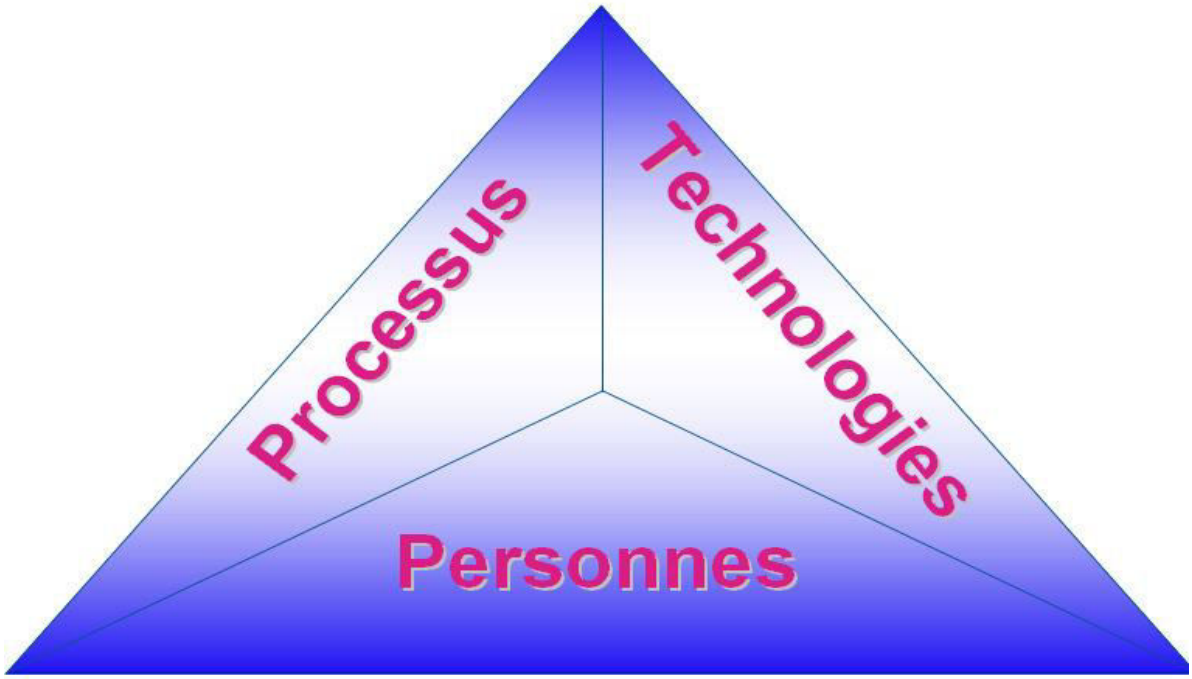
Pour de nombreuses organisations, assurer la sécurité du système d'information (SI) se limite à la mise en place d'un pare feu et d'un antivirus. Or, ces dispositifs ne sont pas d'une grande utilité quand il s'agit par exemple d'attaques type « Ingénierie sociale » qui connaît ces dernières années une évolution spectaculaire.

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

Certes, investir en matière technologique est inévitable pour mettre en place les outils nécessaires à la prévention, détection et correction des failles de sécurité. Cependant, l'aspect organisationnel qui consiste à mettre en place une politique de sécurité de l'information, une charte d'utilisation des ressources et l'ensemble des processus et procédures opérationnels permettant d'assurer un niveau de sécurité minimal est aussi important voir vital pour l'organisation. D'ailleurs, souvent lors des audits de sécurité, nous constatons que le volet technologique est plus ou moins maîtrisé. La nature des failles que nous identifions est plutôt organisationnelle. L'absence de politique de sécurité, le manque de formalisation du mode opératoire de la sauvegarde, le manque de l'inventaire des actifs critiques sont quelques exemples de lacunes en matière de sécurité organisationnelle.[1]

[1] Ali EL AZZOUZI, *Op*.cit., P22.

Figure N°4. : Les trois dimensions de la sécurité



Source : Ali EL AZZOUZI, « *la cybercriminalité au Maroc* » Casablanca, Maroc, 2010.

La sécurité des SI repose sur les quatre piliers suivants :

- La disponibilité qui se manifeste en termes d'accessibilité aux ressources du SI (*Ordinateurs, Serveurs, Bases de données, Réseaux, services, etc…).*
- L'intégrité des données qui comprend quatre éléments : l'intégralité, la précision, l'exactitude/authenticité et la validité[1].
- La preuve est la garantie de ne pas pouvoir réfuter une transaction avec possibilité de pouvoir auditer les résultats fournis (*exemple : un virement de fonds et la vérification du journal comptable à partir des informations d'entrée*).
- La confidentialité demeure le pilier le plus difficile à cerner. En effet, une atteinte à la confidentialité est irréversible. On ne peut procéder à un « *Lavage des cerveaux* » des personnes ayant eu un accès accidentel ou illicite à une information confidentielle. Alors qu'une atteinte à la disponibilité, intégrité ou à la preuve peut être redressée.

I.1. Faire de la sécurité, c'est être « fermé » dans un environnement complètement ouvert

S'ouvrir, attire plus d'opportunités. Mais, ceci ramène aussi de nouvelles menaces auxquelles il faudra faire face. En opérant dans un environnement ouvert, les organisations se trouvent exposées à des attaques qui ne peuvent avoir lieu dans un environnement complètement fermé.

[1] http://fr.wikipedia.org/wiki/Intégrité_des_données consulté le 16/07/2018.

Une entreprise qui propose à ses clients des services transactionnels sur son site Web, se voit contrainte d'investir en sécurité pour mieux protéger ses intérêts et ceux de ses clients.

Dans cette perspective, continuer à sécuriser son SI reviendra à être « fermé » dans un environnement complètement ouvert. Ce qui est loin d'être simple. Cet équilibre est très difficile à aller chercher.

- **La sécurité péri métrique :** La première chose à laquelle nous pensons pour sécuriser le SI d'une organisation est le périmètre externe. Déployer un Pare-feu, mettre en place des mécanismes de filtrage de contenu et de filtrage URL, installer un système de détection et de prévention d'intrusion, sont quelques exemples de la sécurité péri métrique.
- **L'accord Bâle II** : vise à mettre sous contrôle l'ensemble des risques auxquels sont soumis les établissements financiers, et non plus seulement les risques financiers directement liés à leur activité. Tout en restant spécifiquement adapté au secteur bancaire, et notamment à sa grande maturité en matière de gestion des risques, il se rapproche ainsi de réglementations plus génériques comme la loi Sarbanes-Oxley
- **PCI DSS :** Tous les acteurs économiques qui traitent, stockent et transmettent des données et transactions de cartes bancaires, doivent intégrer la norme PCI DSS (Payment Card Industry Data Security Standard). Cette norme est encadrée par le PCI Security Standards Council, une organisation fondée en 2005 par les principaux acteurs du secteur des cartes bancaires : MasterCard, Visa, American Express, Discover Financial Services et JCB.

La norme PCI est présentée comme la garantie d'un haut niveau de sécurité. Elle correspond à une série de douze exigences auxquelles sont assujetties les organisations dont les réseaux, les serveurs et les applications entrent en contact avec les données des titulaires de carte. Concrètement, ces organisations doivent[1] :

1. Installer et gérer une configuration de pare-feu afin de protéger les données des titulaires de carte ;
2. Ne pas utiliser les paramètres par défaut du fournisseur pour les mots de passe et les autres paramètres de sécurité de système ;
3. Protéger les données des titulaires de cartes stockées ;
4. Crypter la transmission des données des titulaires de carte sur les réseaux publics ouverts ;
5. Utiliser et mettre à jour régulièrement un logiciel antivirus ;
6. Développer et gérer des applications et systèmes sécurisés ;

[1] Ali ELAZZOUZI, *Op*.cit., p24.

7. Limiter l'accès aux données des porteurs de carte aux cas de nécessité professionnelle absolue ;
8. Attribuer une identité d'utilisateur unique à chaque personne disposant d'un accès informatique ;
9. Limiter l'accès physique aux données des titulaires de carte ;
10. Suivre et surveiller tous les accès aux ressources du réseau et aux données des titulaires de carte ;
11. Tester régulièrement les systèmes et procédures de sécurité ;
12. Disposer d'une politique régissant la sécurité de l'information.

- **Loi SARBANES OXLEY :** La loi SARBANES OXLEY (SOX), du nom respectif des deux sénateurs Paul SARBANES et Michael G. OXLEY, a été adoptée par le congrès américain en Juillet 2002. Elle a vu le jour suite aux multiples scandales comptables et financiers : Enron, Tyco International ou encore WorldCom. Plusieurs points liés à la sécurité des SI doivent faire l'objet d'un contrôle strict au sens de SOX. Il s'agit notamment de[1] :

1) La gestion des mots de passe

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

2) L'étude de réseau informatique

- Vérification de l'authentification des accès VPN ;
- Protection du réseau interne par 2 niveaux de pare-feux ;
- Contrôle et journalisation des accès à Internet ;
- Signature d'une charte de bon usage d'Internet ;
- Authentification des utilisateurs pour accéder à Internet ;
- Révocation des certificats lors du départ des collaborateurs ;
- Filtrage des emails vis-à-vis des menaces connues : virus, chevaux de Troie, etc.

[1] Ali ELAZZOUZI, *Op*.cit. p25.

3) Plan de reprise en cas de désastres

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

4) La journalisation & Audits

- Mener des audits internes afin d'assurer le bon fonctionnement des mesures de sécurité prises par l'entreprise ;
- Vérification de l'existence des fichiers de logs des serveurs mails, des navigateurs internet et des accès VPN ;
- Traçabilité des accès aux applications financières et ressources humaines ;
- Sauvegardes des emails conservées durant 1 mois minimum (destinataire, l'envoyeur, le sujet, la date et l'heure et l'IP).
- **Le RSSI : un nouveau métier :** S'il y a quelques années, la fonction de sécurité n'était, au mieux, qu'un ensemble de tâches réalisées par le responsable des réseaux, aujourd'hui elle s'impose comme un métier à part.

  Une organisation ayant atteint une taille minimale en termes de nombre d'ordinateurs (plus de 500 postes de travail) dans son parc informatique, ne peut continuer à traiter la fonction de la sécurité d'une façon éparpillée. En effet, en remettant la sécurité aux mains de l'expert informatique (généralement le responsable des réseaux ou le responsable de l'exploitation), seulement l'aspect technologique de la sécurité est pris en compte. Souvent, assurer la sécurité dans une telle configuration se limite à l'acquisition de logiciels adéquats. Les risques purement organisationnels et humains ne peuvent être pris en charge dans un tel contexte. Beaucoup d'organisations ont bien saisi les limites d'une telle approche. Elles disposent aujourd'hui d'une fonction entièrement dédiée à la sécurité prise en charge par ce qui est communément appelé RSSI (Responsable de Sécurité des Systèmes d'Information).
- **La sécurité est une question de gouvernance :** La sécurité de l'information a été longtemps épargnée des mouvements de meilleures pratiques et de référentiels. Les RSSI se trouvaient souvent désarmés face à la bonne canalisation des énergies en matière de sécurisation SI. L'absence de repère en la matière compliquait constamment leurs tâches. Aujourd'hui, grâce à l'émergence de plusieurs référentiels de sécurité, notamment la famille des normes ISO 27000, les RSSI disposent de la matière pour mettre en place la gouvernance de la sécurité de l'information.

I.2. Les dispositifs légaux internationaux de lutte contre la cybercriminalité[1]

A. Travaux de l'ONU

La criminalité liée aux réseaux informatiques a suscité l'intérêt des Etats membres de l'Organisation des Nations Unis dès 1990, à l'occasion de la tenue du huitième Congrès de l'organisation pour la prévention du crime et le traitement des délinquants, qui a eu lieu à la Havane (*Cuba*) du 22 août au 7 septembre 1990, et qui a recommandé la création d'une commission intergouvernementale pour la prévention du crime et la justice pénale qui serait le principal organe directeur de l'ONU en la matière.

Dès sa création en 1992, ladite commission s'est engagée dans la promotion des efforts internationaux dans le domaine de lutte contre la criminalité informatique, à travers l'élaboration d'un ensemble de principes et de normes destiné à mieux orienter ces efforts. Cet engagement a eu pour premier résultat la publication en 1994 d'un manuel sur la prévention et la répression de la criminalité informatique.

En 2000, un atelier de travail a été consacré aux « *délits liés à l'utilisation du réseau informatique* ». Le 4 décembre 2000, l'Assemblée Générale des Nations Unis a adopté une résolution à travers laquelle elle a, entre autres, noté avec satisfaction les efforts déployés pour lutter contre l'exploitation des technologies de l'information à des fins criminelles.

En 2001, le Secrétaire Général a présenté Conformément à la résolution 1999/23, son rapport à la commission pour la prévention du crime et la justice pénale à sa dixième session. Parmi les propositions les plus marquantes de ce rapport, nous citons : l'élaboration d'un instrument international pour la prévention et la lutte contre les délits informatiques, ainsi que la mise en place d'une stratégie mondiale sous l'égide de l'ONU contre ce type de délits.

L'élaboration d'un instrument international contre les délits informatiques, a été reproposée par de nombreux Etats, notamment dans le cadre du douzième congrès des NU pour la prévention du crime et le traitement des délinquants qui s'est tenu au Salvador(Brésil) du 12 au 19 avril 2010.

Les activités de l'ONU dans le domaine de la lutte contre la criminalité informatique restent ainsi limitées à des études, des plans d'actions et des propositions de mesures à mettre en œuvre tant au niveau national qu'international. On ne peut pour autant négliger son impact considérable sur les stratégies de lutte contre la criminalité informatique mises en œuvre notamment au niveau national et régional.

[1] www.cerist.dz consulté le 25/06/2018.

B. La convention de Budapest sur la cybercriminalité

La convention de l'organisation du conseil de l'Europe sur la cybercriminalité, communément appelée « *Convention de Budapest* », est le premier instrument international contraignant en la matière.

Adoptée en 2001 et entrée en vigueur en 2004, cette convention vise pour l'essentiel à :

- Harmoniser le dispositif pénal matériel des Etats membres en énumérant les actes devant être érigés en infractions pénales au niveau national à savoir : l'accès illégal, l'interception illégale, l'atteinte à l'intégrité des données et du système, la falsification informatique, la fraude informatique, etc.
- Renforcer le droit pénal procédural national des Etats membres, à travers l'instauration de pouvoir et procédures adaptés à la nature des cyber-délits et leur environnement immatériel, telle que : la conservation rapide de données informatiques stockées, la conservation et divulgation rapide de données relatives au trafic, la perquisition et saisie de données informatiques stockées, la collecte en temps réel de données informatiques, l'interception de données relatives au contenu.
- Mettre en place un régime rapide et efficace de coopération et de coordination internationale dans le domaine des enquêtes et des poursuites judiciaires.
- En dépit de son caractère régional, cet instrument est considéré comme ayant la plus large portée au niveau international. Puisqu'il permet en vertu de son article 37 aux Etats non membres du conseil de l'Europe d'y adhérer. Il est également reconnu par différentes organisations internationales. Plusieurs pays se sont aussi inspirés de cette convention pour élaborer leur législation contre la cybercriminalité, sans y adhérer officiellement, tels que l'Argentine, le Nigeria, l'Egypte et l'Algérie.

C. La convention arabe sur la cybercriminalité

Le monde arabe s'est, à son tour, doté d'une convention pour la lutte contre la criminalité informatique dans le cadre de la ligue des Etats arabes. Adoptée en 2010, cette convention vise à renforcer la coopération entre les pays arabes dans ce domaine, afin de pouvoir faire face aux conséquences néfastes de ce type de criminalité sur la sécurité et les intérêts de ces Etats et de leurs sociétés nationales.

D. Le Comité de Bâle

Dans son document sur les Principes fondamentaux pour un contrôle bancaire efficace, a pris position quant à la question de la fraude dans son principe 15 qui précise : « *Il s'agit notamment de prévenir et de repérer les actes délictueux ou frauduleux et d'informer les autorités compétentes des faits soupçonnés. En plus d'informer les autorités*

judiciaires compétentes, les banques signalent à l'autorité de contrôle les activités litigieuses et tout cas important de fraude vis-à-vis de la sécurité, de la solidité ou de la réputation de la banque. » .

Le Comité de Bâle a identifié la complexité croissante des opérations bancaires comme une source significative de risque de fraude et a replacé la question de la fraude en milieu bancaire au premier plan des préoccupations des banques, en nommant explicitement la fraude comme composante du risque opérationnel.

Les accords de Bâle II, adoptés en 2006 et entrés en vigueur en France avec l'arrêté du 20 février 2007 transposant la directive CRD[1], ont introduit des exigences en fonds propres au titre du risque opérationnel, qui englobent notamment les pertes éventuelles relatives à la cybercriminalité.

L'application de ces dispositions doit permettre aux établissements de se prémunir contre le risque de fraude. Ces derniers doivent identifier, évaluer et suivre le risque de fraude afin de proposer l'affectation d'une partie de leurs fonds propres à la couverture de ce risque.

II/ Dispositifs et activités de veille adaptées les banques

II.1. L'adaptation des banques au risque de cyber-attaques

En application de la réglementation bancaire, les établissements ont ainsi dû définir leur stratégie informatique, sous la responsabilité de leurs instances dirigeantes, en tenant compte des exigences de sécurité nécessaires à la protection de leurs systèmes. Ils ont dû établir un cadre général de mesure et de réduction des risques, qui englobe le risque informatique et la sécurité du système d'information. Leur responsable de la sécurité des systèmes d'information (*RSSI*) élabore des politiques de sécurité et recommande des mesures techniques (*cryptage des données, gestion des accès, etc*.). Des dispositifs de contrôle interne et de recensement des incidents ont été également mis en œuvre pour veiller à l'adaptation des mesures destinées à maîtriser ces risques. En parallèle, des plans de continuité de l'activité ont dû être établis et régulièrement testés.

Les quelques établissements ayant opté pour des approches de mesure avancée du risque opérationnel ont en outre la possibilité de spécifier des scénarios de risque afin de mieux quantifier les charges en capital nécessaires à la couverture du risque résiduel.

[1] Directive 2013/36/UE du Parlement européen et du Conseil européen du 26 juin 2013 concernant l'accès à l'activité et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, dite en anglais « *CRD IV* » (*Capital Requirements Directive IV*).

La mise en place effective de ces dispositions réglementaires, qui constituent l'ossature des exigences prudentielles en matière de sécurité informatique, est généralement bien établie. L'émergence des nouvelles techniques de cybercriminalité conduit cependant les banques à devoir adapter et renforcer leurs dispositifs. De nouvelles politiques et de nouvelles solutions doivent être élaborées en conséquence, visant en particulier le renforcement de l'expertise et la sensibilisation de l'ensemble du personnel ainsi que la mise en œuvre régulière d'exercices de crise avec des tests sur les dispositifs de gestion.

À cet égard, la participation des principales banques françaises à des tests de place constitue l'une des initiatives concrètes dans le domaine de la prévention des risques liés à la cybercriminalité. L'exercice conduit en novembre 2012 avait permis aux banques françaises d'évaluer l'impact d'une cyberattaque sur leurs processus critiques, en y associant les grandes infrastructures de marché. Ce type d'exercice collectif permet de vérifier que les différents plans de continuité offrent une cohérence d'ensemble et sont bien adaptés à des menaces en constante évolution. [1] *(voir annexe n °9 et 10)*

Cependant, la mise en place de dispositifs de protection ayant pour objectif l'inviolabilité des systèmes n'est ni réaliste ni suffisante pour gérer adéquatement les risques liés aux cyber-attaques. C'est pourquoi les banques doivent désormais adopter des stratégies de protection proactives qui comportent à la fois une activité de veille afin de repérer les cyber-menaces dans l'environnement et une activité de prévention opérationnelle pour définir les moyens qui permettraient de contrer les attaques.

Pour lutter efficacement contre la fraude, il est nécessaire de bénéficier d'un maximum d'informations et d'opposer des Pare-feu technologiques toujours plus efficients. La disparité des niveaux de sécurité des opérations bancaires selon les pays fragilise fortement la sécurité globale. Seules 13% des transactions menées sur le territoire français sont protégées contre les fraudes à la carte bancaire et au vol de données personnelles alors que le taux de protection va au-delà de 95% dans certains pays comme le Royaume-Uni[2].

Les banques renforcent en permanence la sécurité des systèmes de paiement et des sites de banque en ligne dont les dispositifs d'authentification forte, les dispositifs d'authentification à code non ré jouable (code unique envoyé par SMS, généré par une calculette, etc.) renforcent la sécurité des paiements sur internet.

[1] Édouard FERNANDEZ BOLLO, *O*p.cit., P187.
[2] Les actes du forum, 5e Forum international de la cyber-sécurité, cyberespace, enjeu de souveraineté et de sécurité, FIC2013.

Le système CB dispose d'une base de données alimentée en permanence : le Système d'Information Cartes Bancaires (SICB).

La mise en œuvre en Europe des spécifications EMV (Europay, Mastercard, Visa) pour la carte à puce représente un enjeu majeur dans la lutte contre la fraude transfrontalière. Elle concerne non seulement les cartes elles-mêmes, mais aussi leurs dispositifs d'acceptation (terminaux, automates de paiement et de retrait) qu'il convient de migrer vers les nouvelles spécifications pour pouvoir bénéficier d'un niveau de protection égal partout en Europe. Les banques européennes s'étaient engagées à achever cette migration pour fin décembre 2010, et malgré un léger retard, cet objectif est sur le point d'être atteint.

La course technologique contre les cyber-fraudeurs se gagnera aussi en mettant en place une traçabilité des flux financiers criminels en développant les collaborations européennes institutionnelles et scientifiques.

La Convention sur la cybercriminalité de Budapest du 21 novembre 2001 constitue aujourd'hui le texte de référence en matière de coopération internationale dans la lutte contre la cybercriminalité. L'union vient aussi de se doter d'un nouveau Centre européen de lutte contre la cybercriminalité (EC3). Sa mission consiste à cartographier et à suivre les sources de cyber-attaques à l'extérieur de l'UE. Il a pour vocation d'apporter son expertise aux enquêtes de police et de coordonner les informations, mais n'a pas pour mission d'élucider les crimes à la place des polices nationales.[1]

A. Le rôle des pouvoirs publics ; la banque centrale et des superviseurs bancaires face à la cybercriminalité[2]

Le secteur financier est particulièrement exposé avec le développement soutenu de la dématérialisation : les évolutions technologiques ont permis de réduire certains risques opérationnels (*notamment d'exécution*) mais avec

- L'expansion des réseaux et des technologies,
- L'ouverture des systèmes d'information aux échanges extérieurs,
- La croissance des transactions électroniques,…

[1] Les actes du forum, *O*p.cit

[2] Frédéric VISNOVSKY, Secrétaire général adjoint, « *Quel rôle pour les superviseurs bancaires face à la cyber criminalité* », Paris, 27mars 2015.

Le secteur financier est une cible de prédilection des attaques des cybers criminels		
Sécurité publique	**Stabilité financière**	**Sécurité des banques**
Pouvoirs publics	**Banque centrale**	**Superviseurs**

- **Rôle des pouvoirs publics**
  - Parvenir au cyber résilience ;
  - faire reculer considérablement la cybercriminalité ;
  - développer une politique et des moyens de cyber défense en liaison avec la politique de sécurité et de défense commune ;
  - développer les ressources industrielles et technologiques en matière de cyber sécurité.
- **Rôle de la banque centrale**
  - **Améliorer l'efficience** : consolider les dispositifs internes des établissements en situation de stress.
  - **Maîtriser les externalités** : besoin de coordination et de solidarité entre acteurs
  - **Gérer l'incertitude** : le caractère évolutif des menaces exige une actualisation permanente des scénarios et des répondes à y apporter.
  - **Améliorer la capacité** de la Place financière à surmonter les chocs affectant des fonctions critiques telles que les systèmes de paiement, la gestion de la liquidité, le financement de l'économie
  - **Renforcer l'attractivité** de la Place financière en montrant sa capacité à faire face à une crise opérationnelle majeure.
- **Assurer la continuité en cas de crise :**
  - Détecter et identifier les alertes pour mettre en place les mesures appropriées ;
  - Etablir un état des lieux de la Place financière et informer les membres ;
  - Etablir un dialogue permanent avec les services de l'Etat ;
  - Prendre les décisions et les plans d'actions suite à une consultation collective ;
  - Gérer la communication de crise.
- **Rôle des superviseurs bancaires**

Les outils de supervision

- Contrôles sur place ;
- Rapports internes des banques ;
- Analyses transversales.

- **Cadre de contrôle**
  - **Sensibilisation :** Gouvernance et stratégie, Identification des menaces ;
  - **Prévention :** Politiques de sécurité, Cartographie des systèmes IT, Evaluation des risques, tests de vulnérabilité, Mesures de sécurité, Formations, gestion de crise ;
  - **Détection :** Outils de détection, Analyses, Information du management => reporting aux superviseurs ;
  - **Réponse :** Contre-mesures, Plans de continuité et de rétablissement.

II.2. La notion de cyber-sécurité[1]

Les menaces auxquelles sont confrontées les infrastructures en réseau ne cessent d'augmenter. Les pays commencent à comprendre ces menaces et évoquent le besoin de protéger les infrastructures et les données, de défendre leur patrie et de recourir à des systèmes de description des menaces. Une stratégie de cyber-sécurité nationale complète doit présenter aux pays les différentes menaces sur le plan économique, et doit indiquer les programmes et les étapes à suivre ainsi que les initiatives qui doivent être mises en place pour répondre à ces menaces et protéger la connectivité Internet et les TIC utilisées par les particuliers et les entreprises publiques et privées. La stratégie doit être étayée par le potentiel économique que représente l'adoption d'Internet et des TIC; elle doit également inclure les projets qui permettront d'atténuer l'érosion du PIB provoquée par les cyber-menaces et d'améliorer globalement la sécurité et la résilience des pays.

Les stratégies de cyber-sécurité nationales doivent refléter l'importance économique de la cyber-sécurité. Concevoir une stratégie de cyber-sécurité nationale judicieuse ne suffit pas. Il faut pouvoir la mettre en pratique. Aujourd'hui, les principaux thèmes abordés dans la plupart des stratégies incluent : la présentation de l'autorité responsable et sa position au sein du gouvernement.

Une stratégie de cyber-sécurité nationale complète doit inclure les volets suivants :

- **Déclaration :** A la publication d'une stratégie de cyber-sécurité nationale incluant les débouchés et les risques économiques associés à l'adoption des TIC ;
- **Organisation**

A. La désignation d'une autorité compétente et la définition claire de son pouvoir positionnel.

B. L'identification des principales entités gouvernementales affectées par et/ou responsables de la mise en œuvre de la stratégie de cyber-sécurité nationale ;

[1] Document mitre www.mitre.org/publication/all/ten-strategie-off-a-world-class-cybersécurité-operation-center; consulté le17/07/2018 « *supervision de la sécurité du système d'information dans les secteurs banque et assurance* », juin 2016.

C. L'identification des entités du secteur commercial affectées par et/ou responsables de la mise en œuvre de la stratégie de cyber-sécurité nationale (en reconnaissant les dépendances au sein du secteur commercial).

- **Ressource**

A. L'identification des ressources financières et humaines requises et allouées dans le cadre de la mise en œuvre de la stratégie ;

B. La présentation du pourcentage du PIB que la mise en œuvre de la stratégie est censée produire (à la hausse ou à la baisse, et approximativement).

- **Mise en œuvre**

A. L'identification des systèmes requis pour protéger les cyber-infrastructures critiques et assurer l'adoption des TIC ;

B. L'identification des services critiques (et non pas des infrastructures critiques) que la stratégie prévoit de protéger et de rendre plus résilients ;

C. L'identification des normes nationales relatives aux accords sur la continuité des services (24 heures sur 24, 7 jours sur 7) et des conditions de signalement des interruptions concernant chaque service, industrie et infrastructure critique.

A. Les équipes de sécurité

Les principaux établissements du secteur financier en France participent à ces réseaux d'échanges et disposent d'équipes capables d'intervenir.il existe deux types d'équipe : Les centres opérationnels de sécurité (*COS*) et les équipes de réponse aux incidents de sécurité informatique(*CSIRT*).

A.1.Les centres opérationnels de sécurité (COS)

Un SOC est une équipe d'experts en sécurité chargée de surveiller, détecter, analyser et qualifier les évènements de sécurité. Cette équipe assure le pilotage des réactions appropriées aux incidents avérés de sécurité. Elle a pour objectif de réduire à la fois la durée et l'impact des incidents de sécurité qui tirent profit, perturbent, empêchent, dégradent ou détruisent les systèmes dédiés aux opérations habituelles et standards. Cet objectif est atteint grâce à une surveillance efficace et à un suivi des incidents de bout en bout.

Selon les choix organisationnels, le SOC peut également assurer les missions suivantes :

- Suivi des vulnérabilités (de la détection à la correction) ;
- Veille en sécurité informatique ;
- Sensibilisation des utilisateurs en fonction des observations faites sur le SI ;
- Expertise et conseil auprès des équipes informatiques ;
- Pilotage de la mise en œuvre des correctifs de sécurité .

Compte tenu de la variété des missions, des impacts technologiques ainsi que des impacts organisationnels majeurs, la mise en œuvre d'un SOC représente un réel investissement en temps et ressources pour l'Entreprise concernée.

A.2.Les équipes de réponse aux incidents de sécurité informatique(*CSIRT*)

Les équipes de réponse aux incidents de sécurité informatique, plus connues sous leur acronyme anglais CSIRT (computer Security incident réponse teams), sont, quant à elles, chargées d'intervenir en cas d'incident.

Les CSIRT exploitent donc les alertes produites par les COS, ainsi que d'autres alertes reçues par d'autres canaux pouvant signaler des anomalies.

Les missions de CSIRT sont :

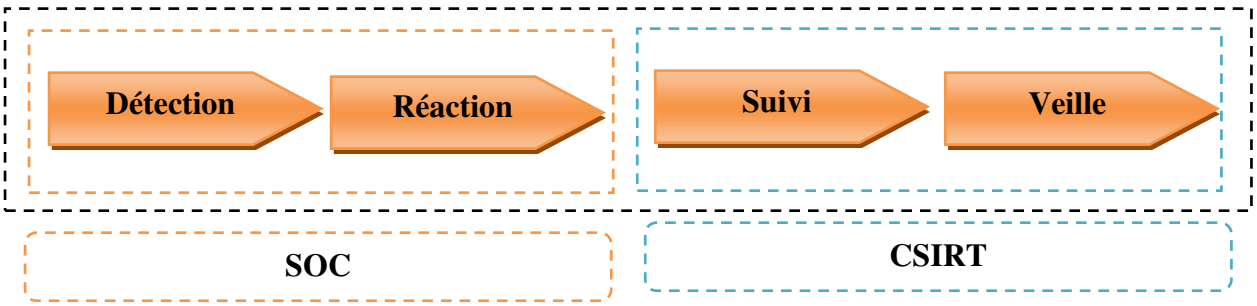
- De fournir l'ensemble des services suivants aux parties prenantes inclues dans son périmètre d'action ;
- Fournir un mécanisme de réponse aux incidents de cyber sécurité et de la sécurité de l'information Assurer la coordination et la communication entre les différentes équipes de réponse 'incidents' ;
- Fournir une expertise et de conseil sécurité.

A.3. Les principales différences entre le (*COS*) et (*CSIRT*)

La limite entre SOC et CSIRT n'est pas toujours évidente à tracer. Seul un modèle de gouvernance et des responsabilités clairement établies permettent de partager détection, réaction et suivi des incidents.

Les adhérences entre le modèle de sécurité de l'Entreprise et l'organisation de l'Entreprise peuvent constituer un frein supplémentaire au partage des tâches et responsabilités (il n'est pas rare que les fonctions/rôles des deux entités soient portés par les mêmes.

Figure.5. : Les 4 grandes activités de la sécurité opérationnelle



Source : Document mitre www.mitre.org/publication/all/ten-strategie-off-a-world-class-cybersécurité-operation-center; « supervision de la sécurité du système d'information dans les secteurs banque et assurance », juin 2016.Consulté le 20/06/2018.

La sécurisation d'un système d'information doit être abordée selon les 4 volets suivants :

a) **Gouvernance** : Définition et mise en place de la gouvernance, c'est-à-dire identifier les acteurs, les rôles, les règles et les processus qui régissent la sécurité du système d'information. Détermination de la cible de sécurité que l'entreprise se choisit.
b) **Protection:** Sélection puis mise en place des mesures de protection organisationnelles et techniques nécessaires pour mitiger les risques afin que la sécurité du SI ainsi implémentée soit conforme à la cible de sécurité que l'entreprise s'est choisie et aux multiples exigences réglementaires auxquelles elle est soumise.
c) **Détection/Réaction:** Sélection puis mise en place des mesures de sécurité relatives à la surveillance des incidents de sécurité et à leur traitement.
d) **Remédiassions/Reconstruction :** Reconstruction de tout ou partie du SI après une attaque réussie.

Conclusion

La sécurité et la lutte contre la cybercriminalité sont des enjeux majeurs pour le secteur bancaire. Le socle de la relation entre la banque et son client c'est la confiance, et il est essentiel de la préserver en mettant en œuvre tous les moyens nécessaires pour la sécurité des informations.

Du point de vue économique[1] 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

Les banques déjouent quotidiennement les tentatives de cyber-attaques ou attaques de cybercriminels. Les sites internet des banques ou les ordinateurs des collaborateurs peuvent être des cibles. C'est pourquoi depuis des années, les banques réalisent d'importants investissements pour se prémunir de tels risques, pour maintenir un degré de sécurité élevé ainsi que pour respecter les nouvelles règlementations.

Les systèmes informatisés des institutions bancaires et des places boursières, font certainement l'objet de mesures de cyber-sécurité. Mais cela n'empêche pas les contournements de ces mesures.

[1] Rapport de l'UIT, « *Guide sur la cyber-sécurité pour les pays en développement* »t, P.16.

Conclusion

Face aux enjeux posés par les cyber-attaques, les banques et les établissements financiers émanent à développer les outils de détection de fraudes et la mise en place des dispositifs de cyber-sécurité ; tel que les dispositifs de prévention d'une part et de gestion des risques avéré et des crises d'autres part, qui sont surveillé et contrôlé par l'ACPR[1] afin de rassurer leur solidité et efficacité en cas d'attaque.

Les menaces auxquelles sont confrontés les systèmes et infrastructures en réseau sont bien réelles. Elles ne cessent d'augmenter et représentent un coût économique pour les pays et les sociétés. Les programmes économiques et de sécurité nationale doivent être harmonisés afin d'instaurer une certaine transparence dans le domaine de la cyber-sécurité. Dévoiler cette association étroite suscitera peut-être un intérêt national et mondial qui permettra d'atténuer cette érosion économique.

Avec la multiplication des attaques, les révélations et les actions des États dans leur cyber-défense, s'offre une opportunité pareille pour maitriser le sujet de la cybercriminalité en profondeur. Certains Etats, comme l'Algérie, ne sont plus en 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.

[1] www.acpr.com consulté le 17/07/2018 L'ACPR (*autorité de contrôle prudentiel et de résolution*), focalisent leur attention sur la cyber-sécurité des institutions supervisées

Introduction

La maitrise et l'usage des technologies de l'information et de la communication (*NTIC*) constituent aujourd'hui un grand défi dans le processus d'édification de la société d'information et le développement de la nouvelle économie fondée sur le savoir. Les NTIC constituent un enjeu majeur pour les pays en voie de développement dans le but d'accélérer la modernisation de leur économie et de combler les écarts qui se creusent de plus en plus avec les pays développés.[1]

A cet égard, l'Algérie a multiplié depuis quelques années les initiatives tendant à favoriser l'accès à ces technologies en tant qu'outils modernes de communication et d'échanges, dont 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]

Les progrès réalisés dans le domaine de l'information et de la communication ces derniers temps, ont imposés un nouvel espace, « *le cyber espace* » ou circulent des flux d'information numériques et dans lequel s'effectuent tous types de transactions et prestations électroniques[4]qui accueillent des comportements illicites, et dans cela qu'un nouveau phénomène est né « *la cybercriminalité* ».

Selon un rapport publié par la société privée spécialisée dans la sécurité des systèmes d'information, kaspersky Lab l'Algérie est le premier pays ciblé d'attaques informatiques industrielles dans le monde durant le deuxième trimestre de l'année 2016, avec un taux de 52.9%, suivi par le Viet Nam (50%) et le Maroc (48%) .[4]

Cette évolution numérique a poussé la plupart des pays du monde de réagir et à mettre des dispositifs juridiques réglementaires appropriés aux différentes utilisations de l'outil informatique. Pour faire face à la délinquance informatique et aussi aux nouvelles formes de criminalité qui sont en évolution , incitant donc l'Algérie à se doter d'un arsenal juridique et adopter des lois spécifiques relatives à la prévention et à la lutte contre les infractions liées aux TIC, celle de 2009,venu compléter celle de 2004 en modifiant et complétant le code pénal.

---

[1] Lamri DOUDI, département d'informatique, université de Sétif « *place de l'Algérie dans le monde des TIC* » http:/manifest.univ-ouargla.dz. Consulté le 4 Aout 2018, p 01.
[2] Nadia Chettab, « *Economie, TIC et bonne gouvernance en Algérie* », papier imprimé, université, Badj Mokhtar Annaba, page4.
[3] Rapport de la CNUCED, 2014. Consulté le 4 Aout 2018
[4] L'Algérie le pays le plus ciblé par les attaques informatiques : https://www.algerie24.dz, consulté le 09Aout 2018.

Section 1 : L'Algérie face au phénomène de la cybercriminalité

Les fortes mutations en Algérie liées aux évolutions des attentes des usagers et des TIC, avait comme fondement une ambition qui était celle de permettre aux usagers de bénéficier de services bancaires automatisés, rapides et sécurisés, dans un délai de dix-huit (18) mois, au travers de dispositifs techniques et métiers que devaient mettre en œuvre , de manière communes, les banques, la poste, et le trésor public, dans un objectifs d'efficiences des services.

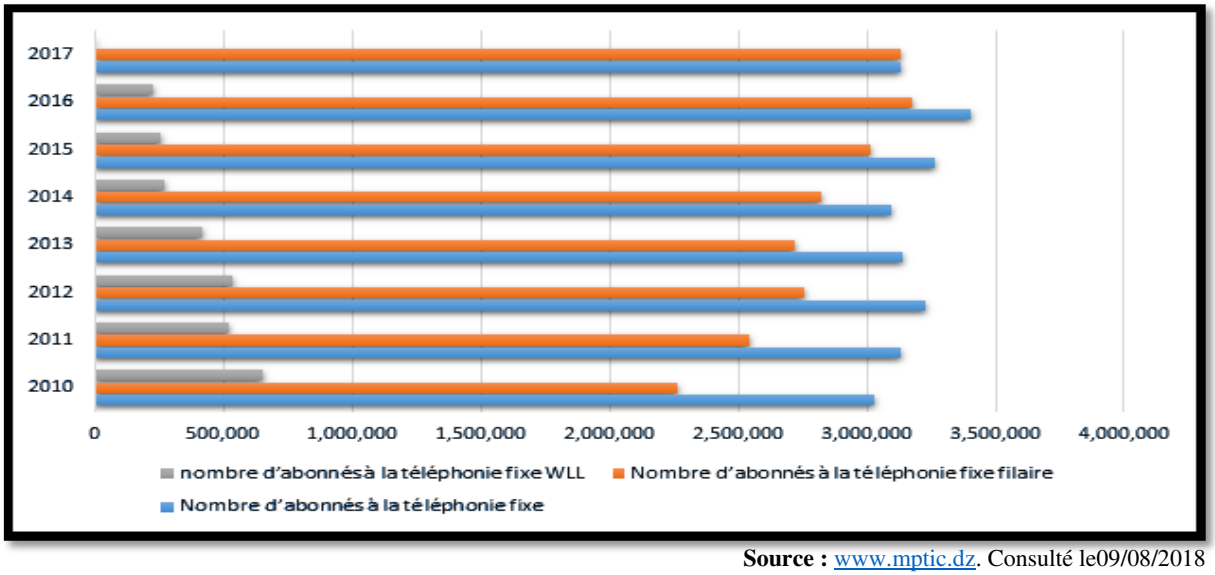
I/ Etat des lieux des TIC en Algérie

I.1. Indicateurs du développement de la société de l'information[1]

A. Réseau de téléphonie fixe

Le marché des télécommunications en Algérie connait une forte croissance, notamment en matière de téléphonie fixe, ce dernier a progressé tant en qualité de service qu'en nombre d'abonnés depuis les années 2000.

Graphe N°01 : Evolution du nombre d'abonnés à la telephonie fixe

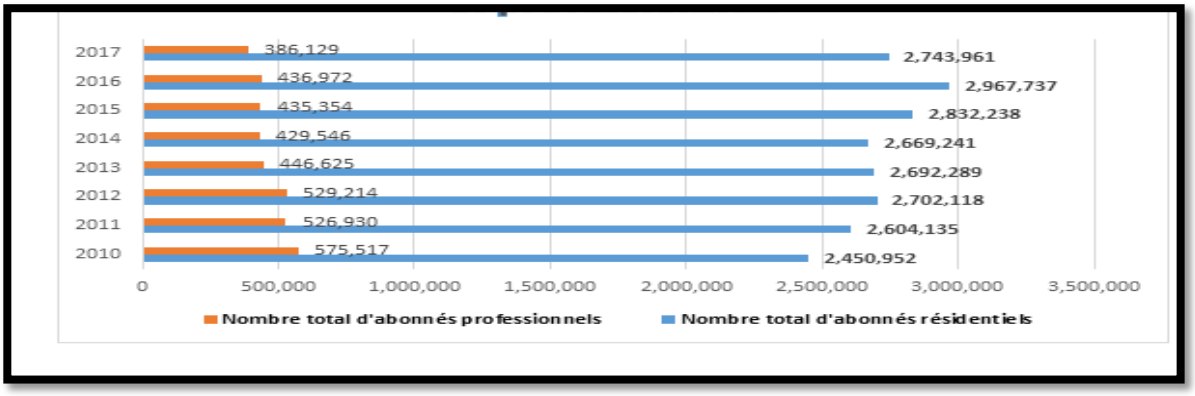


Source : www.mptic.dz. Consulté le09/08/2018

L'évolution du nombre d'abonnés à la téléphonie fixe en Algérie, tend ces trois dernières années vers une stabilité avec plus de trois millions d'abonnés depuis , par ailleurs en 2017, il a été décidé d'éliminer la technologie de téléphonie fixe sans fil (*WLL*), destiné au zone rurale, cela est conforme à la stratégie de l'État visant à doter ces zones d'une infrastructure de communication plus efficace. En 2017, la densité de la téléphonie fixe est de 7,50%, contre 8,26 % en 2016, Cette baisse est due à l'approche citoyenne au téléphone mobile.

[1] www.mptic.dz consulté le 09/08/2018

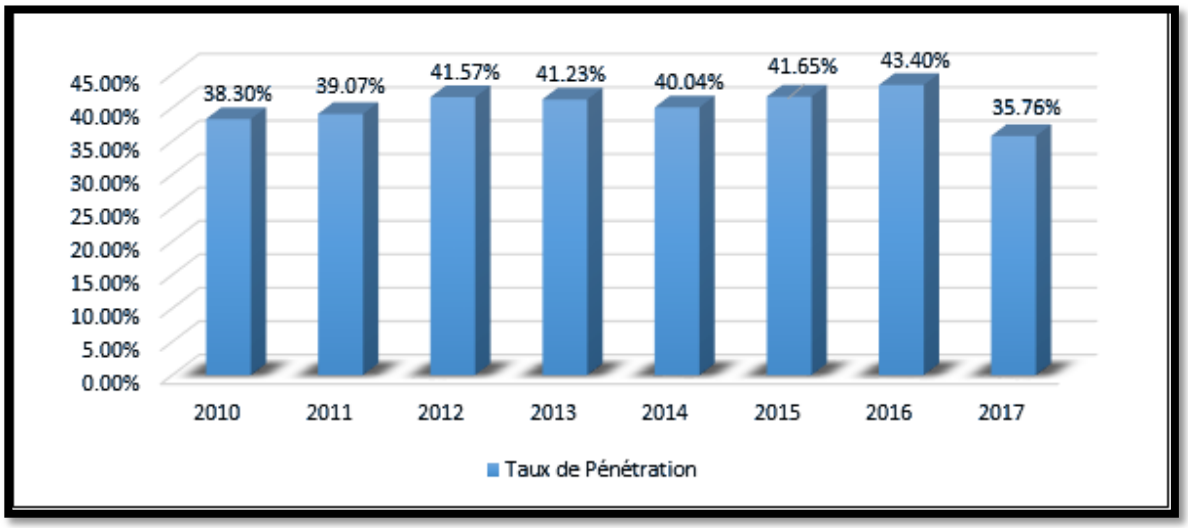
Graphe N°2 : Evolution du nombre d'abonnés résiduels et professionnels



Source : www.mptic.dz. Consulté le 09/08/2018

Les abonnements à la téléphonie fixe ont toujours étaient dominés par les abonnés résidentiels qui représentent en 2017 un taux de 87,66 % du total d'abonnés. Le nombre d'abonnements professionnels de téléphonie fixe est en légère baisse, ce qui est dû à la tendance vers la technologie mobile.

Graphe N° 3 : Taux de pénétration



Source : www.mptic.dz. Consulté le 09/08/2018

L'histogramme ci-dessus illustre l'évolution du taux de pénétration de la téléphonie fixe qui enregistre une forte croissance en 2016 à un taux de 43.4%. A la fin de l'année 2017 le taux de pénétration à la téléphonie fixe a connus une baisse de 8% (soit 35.76%).

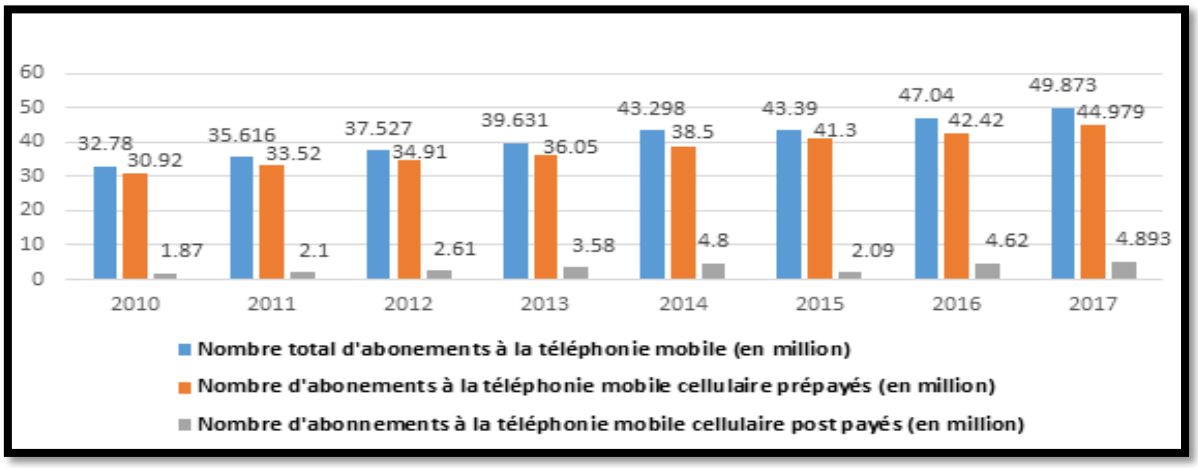
B. Réseau mobile cellulaire

Le marché de la téléphonie mobile a été ouvert à la concurrence en Algérie suite à la promulgation de la loi générale n° 2000-03 du 05 août 2000 fixant les règles générales

relatives à la poste et aux télécommunications, actuellement trois opérateurs de la téléphonie mobile activent sur le marché algérien.

Les services de la téléphonie mobile en Algérie ont connus une nette amélioration, ainsi le taux de la population couverte par le réseau mobile cellulaire a dépassé 98% en 2017, ce qui justifie en partie le nombre d'abonnés qui n'a cessé d'évoluer, atteignant plus de 49.87 millions d'abonné en 2017 contre 47,04 millions d'abonné en 2016, soit une hausse de 6,02%.

Graphe N°4 : Evolution du nombre d'abonnés à la téléphonie mobile par type de payement



Source : www.mptic.dz . Consulté le 09/08/2018.

Le service de la téléphonie mobile 3G a été lancé en Algérie le mois de décembre 2013. En un seul mois 308 019 abonnés ont été enregistrés, ce chiffre s'est multiplié par 27 en 2014, et a atteint plus de 23 millions d'abonnés en 2017.

Dans le cadre de la modernisation et du déploiement du réseau des télécommunications sur le territoire national, et la tendance à l'économie numérique, le 01 Octobre 2016, le lancement officiel de la téléphonie mobile de quatrième génération (4G) est bien réel en Algérie. Après une année, 10 968 492 abonnés ont été enregistrés dont 87,95% des abonnements sont en mode de prépayés.

Tableau N°01 : Nombre d'abonnés à la 3G et 4G de 2012 au 2017

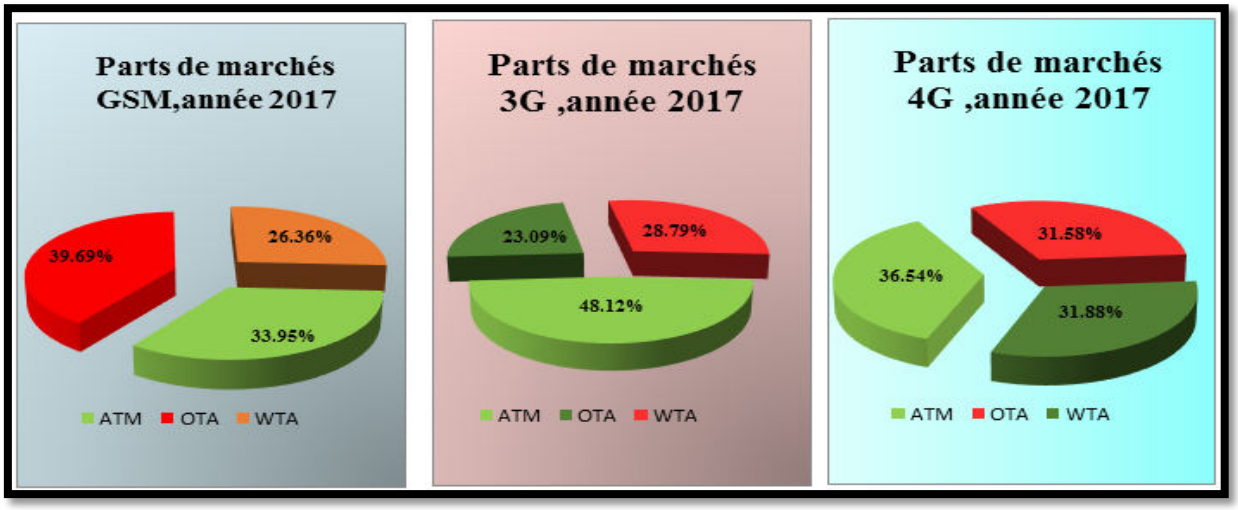
Indicateurs	2012	2013	2014	2015	2016	2017
Nombre des abonnements à téléphonie mobile 3G	/	308 019	8 509 053	16 684 561	25 214 732	23 701 023
Nombre des abonnements à téléphonie mobile 4G	/	/	/	/	1 464 811	10 968 495

Source : www.mptic.dz .Consulté le 09/08/2018

Taux de pénétration aux réseaux mobiles	99.28%	102,40 %	109,62 %	107,40 %	113,35%	121.05%

A propos de la répartition des parts de marché entre les opérateurs, l'ordre n'a pas changé au fil des années. Pour la téléphonie GSM, l'opérateur Orascom Télécom Algérie détient en 2017 la grande part avec 39,69%, suivie par Algérie Télécom Mobilis et Wataniya Télécom Algérie respectivement. Quant au marché de la 3G et la 4G, Algérie Télécom Mobilis vient en tête avec 48,12% et 36,54 % des parts respectivement.

Graphe N°5 : Nombre d'abonnés à la 3G et 4G en 2017



Source : www.mptic.dz. Consulté le 09/08/2018

C. Internet

- Dans le cadre de la modernisation des infrastructures et de l'amélioration des services, les efforts pour le raccordement à la fibre optique se poursuivent. A la fin de 2017, toutes les communes ont été raccordées à la fibre optique. Le tableau n°2 nous montre les indicateurs d'infrastructure passive en Algérie.

Tableau N°2 : Indicateurs : infrastructure passive

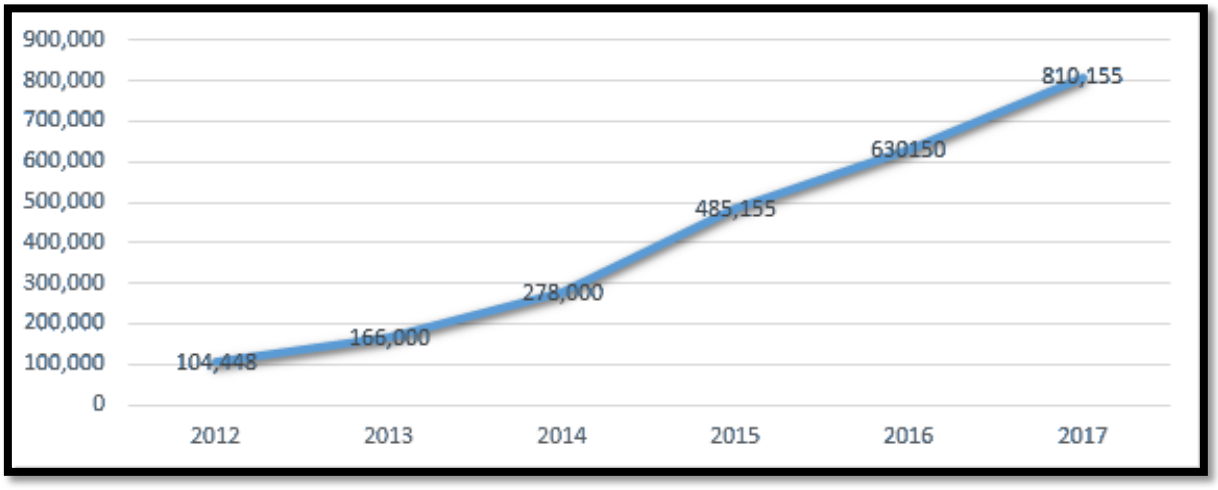
Indicateurs : infrastructure passive	2012	2013	2014	2015	2016	2017
Longueur de la Fibre optique (KM)	46 231	50 800	61 556	70 700	76.514,56	81 872
Nombre de communes raccordées à la Fibre Optique (FO)	1 000	1 081	1 229	1 321	1 477	1 541
Largeur de bande internet nationale en Mbit/s	130 000	172 021	348 000	390 000	--	801 000

Largeur de bande internet internationale en Mbit/s	104 448	166 000	278 000	485 155	630 150	810 155

Source : www.mptic.dz. Consulté le 09/08/2018

- Afin de répondre aux besoins de l'internaute algérien et offrir un service de qualité, la largeur de bande internationale, n'a cessé de croitre, et a atteint 810 155 Gbit/s fin 2017(graphe n°6).

Graphe N°6 : Largeur de bande internet internationale en Mbit/s



Source : www.mptic.dz. Consulté le 09/08/2018

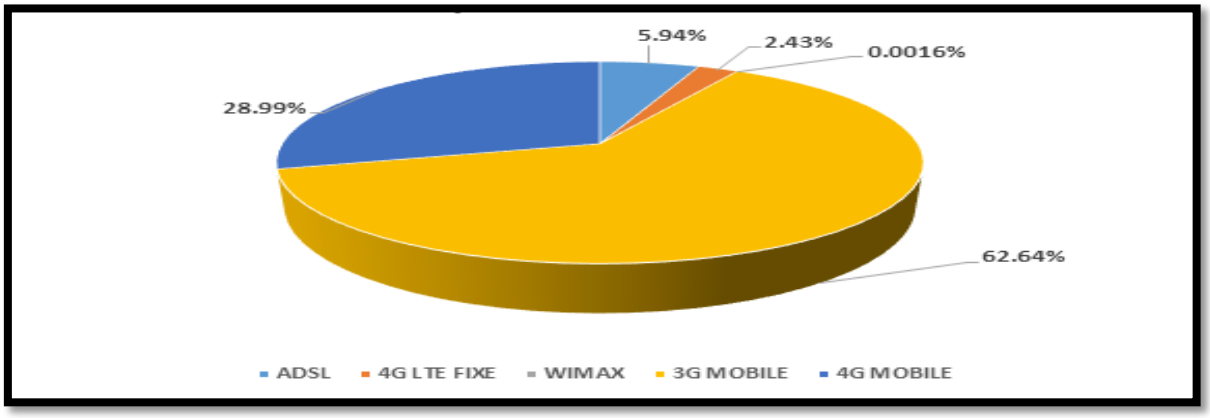
Les indicateurs d'abonnement à internet ainsi la répartition des abonnés internet par type de technologie sont présentés dans le tableau et le graphe comme suit.

Tableau N°3 : Indicateurs : Abonnés Internet

Indicateurs : Abonnés Internet	2013	2014	2015	2016	2017
ADSL	1283241	1518629	1838492	2 083 114	2 246 918
4G LTE fixe	--	80693	423280	775 792	919 368
WIMAX	179	216	233	661	621
3G mobile	308019	8509053	18021881	25 214 732	23 701 023
4G mobile	--	--	--	1 464 811	10 968 495
Internet fixe (ADSL+4G LTE fixe+ WIMAX)	1 283 420	1 599 538	2 262 005	2 859 567	3 166 907
Internet mobile (3G+4G)	308 019	8 509 053	18 021 881	26 679 543	34 669 518
Total d'abonnés internet (Fixe et Mobile)	1 591 439	10 108 591	20 283 886	29 539 110	37 836 425

Source : www.mptic.dz. Consulté le 09/08/2018

Graphe N°7 : Répartition d'abonnés internet par type de technologie pour l'année 2017



Source : www.mptic.dz.Consulté le 09/08/2018

- A propos du réseau internet en Algérie, le nombre d'abonnés est de 37,83 millions en fin d'année 2017, dont 34 millions enregistrés pour l'internet mobile, le chiffre est vu à la hausse avec l'introduction de la technologie haute débit sans fil en mode fixe (4 G LTE).

Tableau N°4 : Indicateurs : abonnés par débit

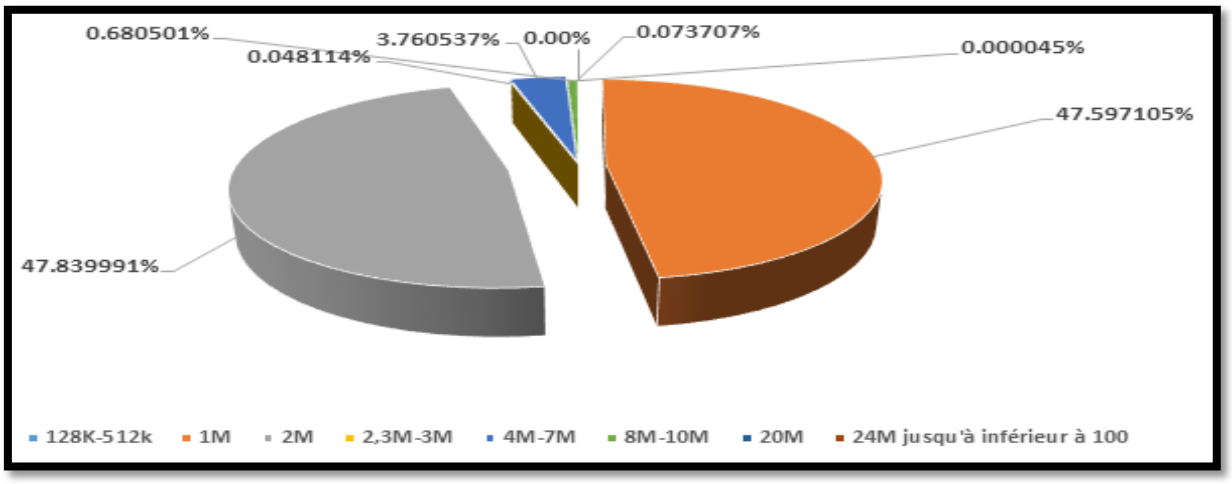
Indicateurs : abonnés par débit	2012	2013	2014	2015	2016	2017
128K	15 001	7 497	2 608	1 3z18	265	0
256K	252 303	158 181	48 599	26 048	14 168	0
512K	495 289	589 042	92 843	56 847	39 324	0
1M	381 180	511 386	832 535	990 988	1 050 288	1 069 377
2M	9 473	13 997	523 547	728 009	917 808	1 074 834
2,3M	807	1 003	1 617	1 677	1 500	1 080
3M	5	11	--	--	--	1
4M	483	1 465	10 631	24 522	47 067	84 488
7M	8	10	1	1	1	1
8M	185	602	6 050	8 805	11 703	15 288
10M	7	18	1	531	1	1
20M	5	28	195	531	972	1 656
24M jusqu'à inférieur à 100	2	1	2	531	1	1
Total	**1 154 748**	**1 283 241**	**1 518 629**	**1 838 746**	**2 083 098**	**2 246 727**

Source : www.mptic.dz. Consulté le 09/08/2018

- Les statistiques ci-dessus indiquent qu'il n'y a pas d'abonnés Internet dans les catégories inférieures de 1 Mo/s, en raison de la politique sectorielle visant à fournir un débit élevé

conforme aux aspirations du citoyen algérien, en 2017 les abonnements internet avec un débit 1 Mbit/s représentent plus 50% du nombre total d'abonnés comme le montre le graphe n°8 suivant.

Graphe N°8 : Répartition des abonnements internet par débit



Source : www.mptic.dz.Consulté le 09/08/2018

D. Site web et service en ligne

- Dans l'objectif du développement de l'administration électronique, des sites web institutionnels ont été mis en ligne, afin de permettre aux citoyens d'accéder aux différentes informations utiles, d'interagir avec l'administration, et de réaliser quelques procédures en ligne (tableaun°7).

Tableau N°5 : Indicateurs de Site web et service en ligne

Indicateurs	2015 (1er semestre)
Nombre de sites web .dz	**7148**
Nombre de sites web institutionnels (ministères et organismes rattachés)	**587**
Nombre de formulaires disponibles	**265**
Nombre de procédures en ligne disponibles	**29**

Source : www.mptic.dz. Consulté le 09/08/2018

E. Nombre d'opérateurs et de prestataire du segment télécom

L'activité des fournisseurs d'accès à l'internet (FAI) poursuit sa progression en Algérie avec l'intégration de trois nouveaux FAI dans le marché durant l'année 2015 et cinq d'autres au cours de l'année 2016. Le tableau suivant nous montre les indicateurs d'opérateurs du segment télécom.

Tableau N°6 : Indicateurs d'opérateurs et de prestataire du segment télécom

Indicateurs	2014	2015	2016
Nombre de KMS	24786	24052	---
Nombre de cyber café	--	5548	--
Nombre de centre d'appel	164	69	86
Audiotex	07	08	08
FAI	20	23	28
Opérateur VoIP	03	03	03
GMPCS	30	03	02
VSAT	03	03	03
Téléphonie fixe	01	01	01
Téléphonie mobile GSM	03	03	03
Téléphonie mobile 3G	03	03	03

Source : www.mptic.dz. Consulté le 09/08/2018

- On constate que le nombre de kiosque multiservices (KMS), a diminué en 2015, ceci cède à une tendance mondiale qui voit le nombre de KMS régresser devant la démocratisation et la généralisation des services de la téléphonie mobile.
- A l'inverse de l'année 2015 où le nombre de centre d'appel était en net régression, l'activité des centres d'appel chez les entreprises algériennes a progressé en 2016 avec l'intégration de 17 nouveaux centres.
- Suite à une enquête menée sur le territoire national, par le ministère de la poste et des technologies de l'information et de la communication à travers ses directions de wilayas, 5548 cybers café actifs ont été recensés.

I.2. Indicateurs des infrastructures et services postaux en Algérie[1]

A. Indicateurs des infrastructures postales

Les bureaux de poste hors service sont soit des bureaux de poste récemment réceptionnés qui ne sont pas encore ouverts au public ou bien des bureaux fermés pour réhabilitation et modernisation.

La densité postale s'est stabilisé à quelque dix mille personnes par bureau de poste en 2017 ainsi que les années précédentes, et ce malgré les efforts consentis afin de la réduire. Le tableau n°7 et le graphe n°9 nous donne plus d'informations.

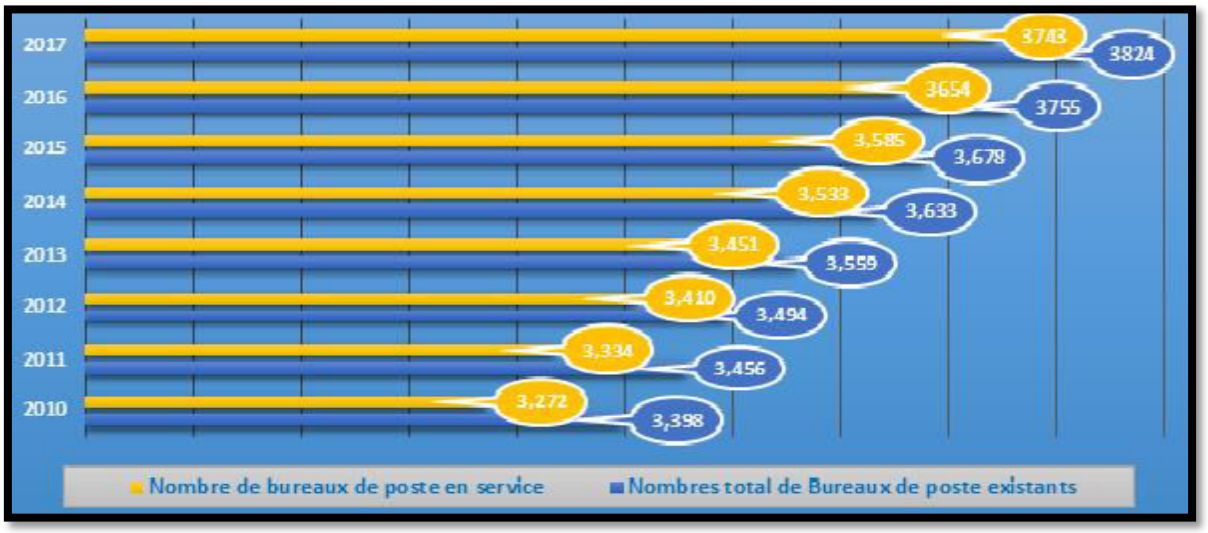
[1] www.mptic.dz Consulté le 9/08/2018.

Tableau N°7 : Les infrastructures postales

Indicateurs	2010	2011	2012	2013	2014	2015	2016	2017
Nombres total de Bureaux de poste existants	3 398	3 456	3 494	3 559	3 633	3 678	3755	3824
Nombre de bureaux de poste en service	3 272	3 334	3 410	3 451	3 533	3 585	3654	3743
Nombre de bureaux réhabilités	94	101	43	103	167	168	152	314
Nombre de bureaux de poste connectés	3272	3 334	3 410	3 451	3 533	3 591	3654	3743
Densité Postale	10 471	10 936	10 508	10 502	10 489	10 547	10 517	10 904

Source : www.mptic.dz. Consulté le 09/08/2018

Graphe N°9 : Représentation des infrastructures postales



Source : www.mptic.dz. Consulté le 09/08/2018

Les chiffres et graphique ci-dessus montrent une évolution du nombre total de bureaux de poste existants qui tend vers une croissance continue, passant de 3755 bureau en 2016 à 3824 bureau en 2017, soit une évolution de 1.83 %, Il y a lieu de noter que plus de 97% des bureaux de poste étaient actifs durant l'année 2017, soit 3% seulement des bureaux étaient hors service.

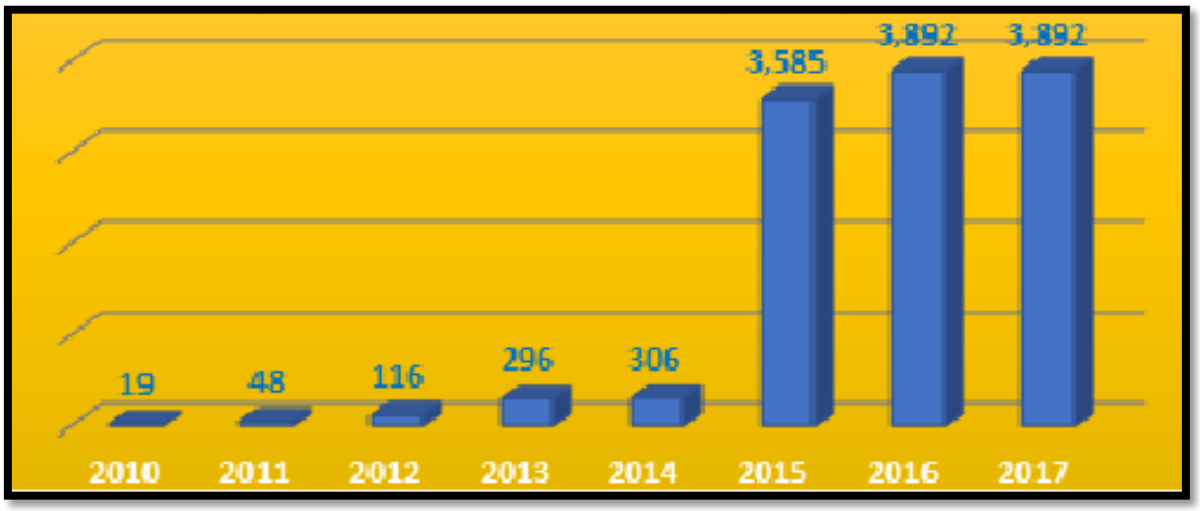
Dans le cadre de l'amélioration de la qualité de service destiné à toutes les franges de la population algérienne, 3 892 guichets ont été aménagés pour les personnes à besoins spécifiques en 2017 comme le montre le tableau n° 8 et le graphe n°10 suivant.

Tableau N°8 : Nombre de guichet

Indicateurs	2010	2011	2012	2013	2014	2015	2016	2017
Nombre de guichets existants	10 752	10 877	11 043	11 205	11 339	11 459	11 641	11 857
Nombre de guichets aménagés pour les personnes à besoins spécifiques	19	48	116	296	306	3 585	3 892	3 892

Source : www.mptic.dz. Consulté le 09/08/2018

Graphe N°10 : Nombre de guichets aménagés pour les personnes à besoins spécifiques



Source : www.mptic.dz.Consulté le 09/08/2018

B. Indicateur des services postaux

Tableau N°9 : Nombre de compte CCP

Indicateurs	2010	2011	2012	2013	2014	2015	2016	2017
Nombre de comptes CCP	**13 551 743**	**15 096 025**	**16 259 811**	**17 082 673**	**18 080 469**	**19 118 250**	**20 044 782**	**20 413 478**
Nombre d'opérations CCP (débit crédit)	**363 151 449**	**409 770 454**	**450 581 628**	**442 384 737**	**498 959 868**	**500794956**	**506 000000**	**536 633 686**

Nombre de comptes CNEP	**3 960 523**	**4 011 051**	**4 065 000**	**4 107 000**	**4 150 924**	**4194057**	**4 231 737**	**4 125 870**
Nombre d'opérations CNEP (vers+Rem)	**2 983 189**	**2 765 842**	**2 786 746**	**2 504 116**	**2 484 240**	**2 373 643**	**2 260 538**	**2 148 753**

Source : www.mptic.dz. Consulté le 09/08/2018

Nous remarquons que le nombre de comptes CCP est en augmentation continue chaque année, en raison de l'amélioration observée par le citoyen algérien concernant les services fournis par Algérie poste ainsi que l'existence des services postaux dans la plupart des régions du pays. Par ailleurs l'évolution du nombre de compte CNEP est en baisse.

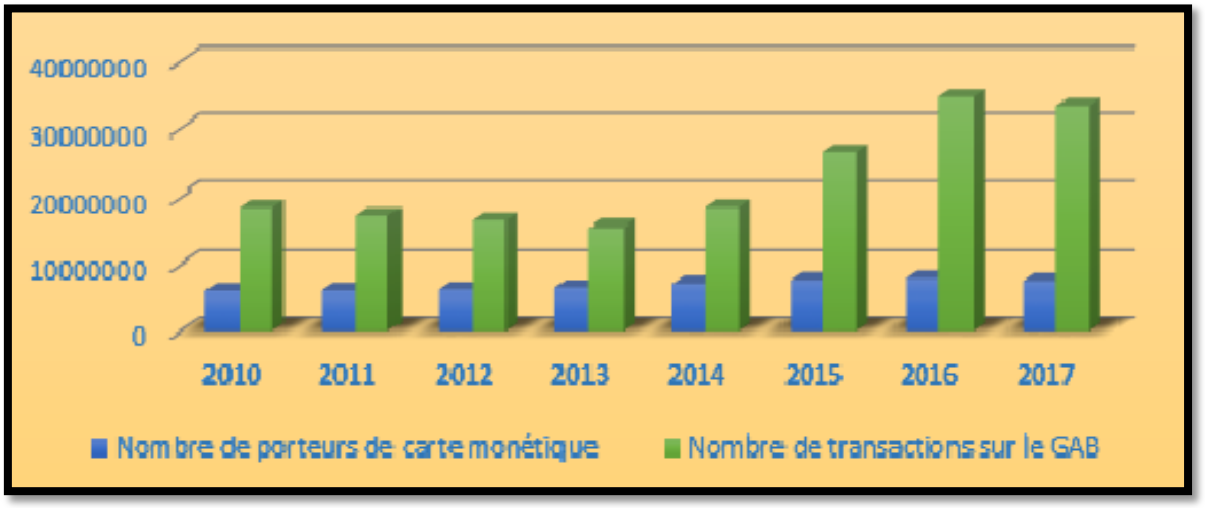
Tableau N°10 : nombre de CIB et GAB

Indicateurs	2010	2011	2012	2013	2014	2015	2016	2017
Nombre de GAB en service	674	684	686	694	898	1 079	1122	1412
Nombre de bornes multimédia	0	230	173	192	192	192	192	186
Nombre de lecteurs CIB	0	0	1000 Pin Pad	1000 Pin Pad	1000 Pin Pad	6000	10 042	
	--	--	472 TPE	472 TPE	472 TPE	472 TPE	472 TPE	472 TPE
Nombre de porteurs de carte monétique	5 837 955	5 899 388	6 050 338	6 369 446	7 043 699	7 642 718	7924142	7492508
Nombre de transactions sur le GAB	18 457 736	17 202 407	16 439 375	15 479 447	18 524 113	26 462 283	34978212	33 488 50

Source : www.mptic.dz. Consulté le 09/08/2018

Algérie poste veille à la généralisation des cartes monétiques, en 2017 le nombre de porteurs de carte a atteint 7 492 508 personnes, et le nombre de Guichet Automatique de banque en service tend vers une progression passant de 674 en 2010 à 1 412 en 2017.

Graphe N°11 : Evolution de porteurs de carte monétique et nombre de transactions sur le GAB



Source : www.mptic.dz.Consulté le 09/08/2018.

I.3. La place des TIC dans les banques algériennes

L'évolution technologique dans le secteur financier, en général, et le secteur bancaire, en particulier a créé une dynamique de renouveau dans l'économie bancaire, mettant en jeu l'ouverture vers l'extérieur tout en gardant la maitrise de son environnement.

Le processus de changement dans le système bancaire et financier qui s'est déroulé en Algérie entre 2004 et 2006 a pour objectif principal de simplifier et de renforcer l'accès aux usagers, à des services répondant à leurs besoins, à travers une offre multi-produit et multicanal, articulée autour de :[1]

- L'innovation de produit qui s'est accompagnée à la fois par l'apparition de nouveaux produits (e-paiement et Télépaiement), et par l'amélioration de ceux déjà existants (Chèque, Virement, Effet de Commerce, Prélèvement) ;
- L'innovation de procédé qui s'est traduite par l'apparition de nouvelles techniques et méthodes de traitement et de production de l'information ;
- L'innovation organisationnelle qui a induit l'apparition d'une nouvelle organisation du travail.

A ce titre, il a été préconisé ce qui suit :

- Un rôle déterminant de la Banque d'Algérie dans la modernisation des systèmes de paiement, avec l'entière adhésion des banques ;

[1] www.ubmonline.org /wp-content/uploads/.../L'Iintégration-digitale-par-Mr-Said-TALEB .pdf. Consulté le 09/08/2018.

- Une forte coopération interbancaire qui est un gage de réussite des projets dans le domaine des systèmes de paiement, tout en gardant à l'esprit la nécessité d'un équilibre adéquat entre la coopération et la concurrence, dans un cadre totalement ouvert ;
- Une approche pragmatique de la réalisation d'un projet à plusieurs composantes tel que celui des systèmes de paiement, consiste à bien sérier les différents domaines et à procéder à une exécution du projet, composante par composante, en veillant toutefois à assurer la cohérence d'ensemble ;
- L'implication de la communauté bancaire à tous les niveaux de la réalisation du projet a été une condition de sa réussite. Pour cela, une coopération soutenue entre les banques et la Banque d'Algérie s'est concrétisée par des actions concrètes (*structures de coordination, échange d'informations, groupes de travail etc*…).

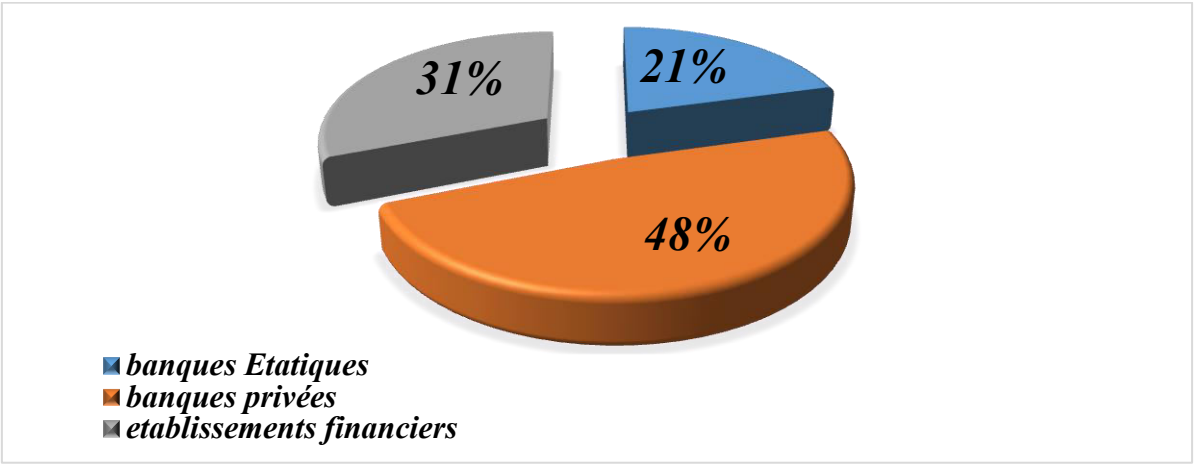
A. Contexte bancaire actuel en Algérie

La place bancaire compte actuellement un total de 29 banques et établissements financiers en activité en Algérie, selon une décision de la Banque d'Algérie portant publication des deux listes des banques et établissements financiers agréés au 2 janvier 2018, publiées au Journal officiel N° 4.

Au nombre de vingt (20), les banques sont composées de la Banque extérieure d'Algérie (BEA), Banque nationale d'Algérie (BNA), Crédit populaire d'Algérie (CPA), Banque de développement local (BDL), Banque de l'agriculture et du développement rural (BADR), Caisse nationale d'épargne et de prévoyance (CNEP Banque), Banque Al Baraka d'Algérie, Citibank N.A Algeria (succursale de banque), Arab Banking Corporation-Algeria, Natixis-Algérie, Société Générale-Algérie, Arab Bank Plc-Algeria (succursale de banque), BNP Paribas Al-Djazair, Trust Bank-Algeria, The Housing bank for trade and finance-Algeria, Gulf Bank Algérie, Fransabank Al-Djazair, Crédit agricole corporate et investment Bank-Algérie, HSBC-Algeria (succursale de banque), et Al Salam Bank-Algeria**.**

Quant aux établissements financiers, ils sont au nombre de neuf (9). Il s'agit de la Société de refinancement hypothécaire (*SRH*), la Société financière d'investissement, de participation et de placement (Sofinance-Spa), Arab Leasing Corporation (*ABC*), Maghreb Leasing Algérie (MLA), Cetelem Algérie, Caisse nationale de mutualité agricole (**CNMA**), Société nationale de leasing, Ijar leasing Algérie et El Djazair Ijar**.**

Figure N°1 : Le contexte bancaire actuel en Algérie



Source : élaboré par nos soins à base des données du site www.fce.dz. Du 11 février 2018.

B. Utilisation des TIC par les banques

Les banques Algériennes, ont instauré un nouveau moyen de paiement (une solution monétique). Le paiement électronique dit aussi le paiement par carte bancaire, qui n'est pas encore globalisé au sein de la population. Ce moyen de paiement électronique constitue la base du e-commerce, car l'internaute va entrer les informations de sa carte bancaire (en plus d'un mot de passe confidentiel) quand il effectuera un achat sur un site marchand.

B.1.La solution monétique[1]

La solution installée et gérée par la SATIM *(Voir annexe N°11)* repose sur une infrastructure et des équipements techniques sécurisés et connectés aux sites informatiques et / ou monétiques des banques.

Elle répond aux exigences des normes internationales EMV et permet de se prémunir de toute tentative de fraude connue à ce jour.

La solution monétique prend en charge le paiement domestique et le retrait d'espèces dans un cadre interbancaire, elle est constituée de :

- Front Office, qui assure la connexion avec les banques, les Terminaux de Paiement Électroniques et les Distributeurs Automatiques de Billets ;
- Back Office, qui permet les traitements de pré-compensation ;
- Plate-forme de télécommunication sécurisée qui permet d'effectuer les échanges entre les différents acteurs du réseau monétique ;
- Réseau d'acceptation DAB et TPE ;
- Les modules de prévention contre la fraude.

[1] www.SATIM.dz consulté le 09/08/2018.

Les avantages liés aux fonctionnalités :

- Interbancaires totale (Banques et Algérie poste) ;
- Disponibilité du service (système opérationnel 24/24 et 7/7) ;
- Disponibilité de l'argent à tout moment ;
- Diminution de la circulation du cash ;
- Elimination du risque d'encaissement de faux billets ;
- Diminution du risque de vol ou de perte de liasse d'argent ;
- Utilisation d'une carte multifonctions (Retrait et paiement) ;
- Sécurité.

Processus d'une transaction monétique : *(voir annexe N°12)*

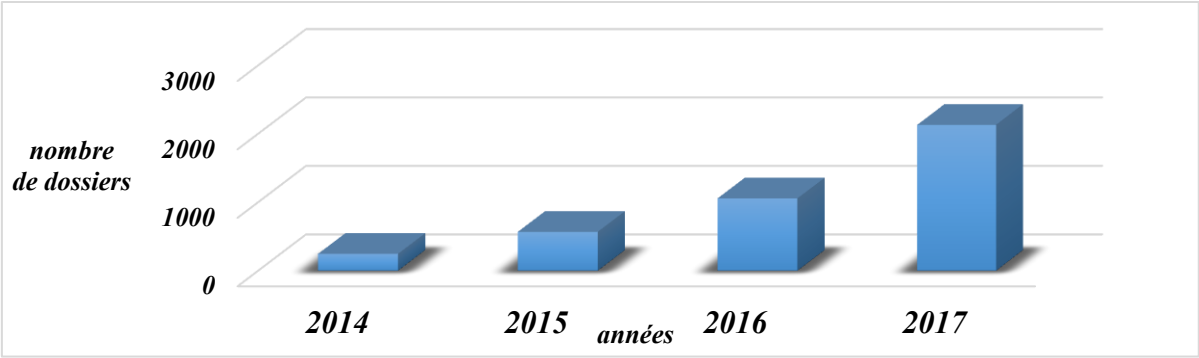
- Introduction de la carte dans le terminal par le porteur (DAB, TPE) ;
- Demande d'autorisation à l'émetteur. Réponse à la demande d'autorisation ;
- Collecte de la transaction par l'acquéreur.
- Présentation par l'acquéreur de la transaction en compensation ;
- Débit du compte du porteur et crédit du compte de l'acceptant.

II/ Etat des lieux de la cybercriminalité en Algérie

II.1. Evolution de la cybercriminalité en Algérie

Le nombre d'affaires résolues liées à la cybercriminalité est de 1.750, sur un total de 2.130 affaires traitées durant l'année 2017, selon un bilan rendu public mardi à Alger par la Direction générale de la Sûreté nationale (DGSN).

Graphe N°12 : Evolution de la cybercriminalité entre 2014-2017



Source : établi par nos soins à partir des données relevées du site http://www.radioalgerie.dz/news/fr/article/20180221/134543.html, consulté le 09/08/2018

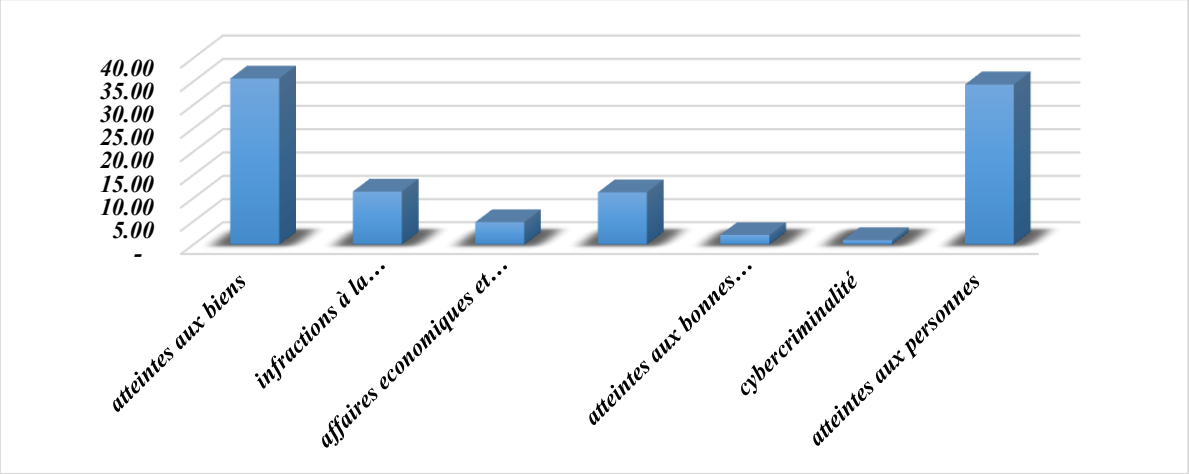
Une évolution significative du nombre de dossiers judiciaires formalisés allant de 246 dossiers en 2014, à 567 en 2015 et 1.055 dossiers en 2016, pour atteindre 2.130 affaires en 2017, soit une augmentation de 102% par rapport à l'année 2016.

Il est à relever que sur les 2.130 affaires liées à la cybercriminalité traitées, 1.570 affaires ont été résolues en 2017, soit un taux de 73,71% (63,98% en 2016).

Sur un autre plan, 228.793 affaires criminelles ont été enregistrées en 2017, avec un taux de résolution de près de 68%.

A. La place de la cybercriminalité

Graphe N°13 : La place de la cybercriminalité en Algerie.



Source: établi par nos soins à partir des données relevées du site http://www.radioalgerie.dz/news/fr/article/20180221/134543.html, consulté le 09/08/2018

Nous remarquons que la cybercriminalité n'atteint presque le 1%(0,93%) des infractions commises sur le territoire algérien en la comparant aux criminalités classiques tels les affaires qui portent sur les atteintes aux biens 35,60%, 11,04 sur les infractions à la législation des stupéfiants, 4,82% relèvent d'affaires économiques et financières, 11,22% sur les atteintes à la chose publiques, 2,05% sur les atteintes aux bonnes mœurs, liées à et 34,34% sont des atteintes aux personnes.

B. Les cyberattaques contre l'Algérie

Selon une étude faite par Kaspersky Lab sur les cybers attaques publié dans le magazine américaine Forbes, l'Algérie est arrivée au 3e rang dans le classement des pays arabes les plus victimes de cyber attaques, juste derrière les UAE et l'Arabie saoudite ; et au 24e rang dans le classement mondial. Le tableau ci-dessous montre le classement des 5 pays arabes les plus touchés par les cybers attaques.

Tableau N°11 : classement des 5 pays arabes les plus touchés

	Rang	
Pays	**Régional**	**Mondial**

Arabie saoudite	1er	17eme
UAE	2eme	18eme
Algérie	3eme	24eme
Egypte	4eme	32eme
Maroc	5eme	41eme

Source : https://www.alg24.net/cyberattaques-lalgerie-parmi-pays-plus-touches/. Consulté le 09/08/2018

II.2. Le dispositif légal national de la lutte contre la cybercriminalité

N'étant pas en reste de la dynamique mondiale concernant la lutte contre la cybercriminalité, l'Algérie s'est, dès la fin des années 90, engagée dans l'adaptation de son dispositif pénal national aux exigences de la lutte contre la criminalité informatique[1].

A. Le dispositif procédural de lutte avant la loi 09-04

Dans le code pénal algérien, l'introduction, en 2004, de dispositions inédites relatives à la criminalité liée aux TIC, a suscité l'attention du législateur algérien quant à la nécessité d'adopter des règles procédurales adéquates.

Or, les modifications apportées au code de procédure pénale, à la même année, par la loi n°04-14 du 10-11-2004 modifiant et complétant l'ordonnance n°66155 du 08-06-1966 portant code de procédure pénale, étaient loin d'apporter des solutions claires à tous les obstacles procéduraux que pose la criminalité informatique.

Après deux ans, une nouvelle loi est intervenu selon le code pénal Algérien le 20-11-2006 à travers la loi n°06-22 modifiant et complétant l'ordonnance n°66-155 du 08-06-1966 portants code de procédure pénale.

Celle-ci visait, notamment, la consécration de règles procédurales plus adaptées à certains types d'infractions nouvelles ou plus répandues, dont les atteintes aux systèmes de traitement automatisé de données(STAD).

B. Le dispositif procédural de lutte contre la cybercriminalité après la loi 09-04

L'estimation de la nouvelle orientation de la politique du gouvernement algérien en matière de lutte contre la criminalité liée aux TIC, s'est traduite par la loi n°09-04 du 05 août 2009*(voir annexe N°13)* portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication.

[1] www.cerist.dz. Consulté le 27/05/2018

Inspirée de la convention de Budapest sur la cybercriminalité, et du droit pénal comparé, cette loi prévoit des mesures procédurales répondant à trois impératifs majeurs pour le renforcement de la prévention et la lutte contre la cybercriminalité, à savoir :

- Le renforcement des prérogatives des organes d'investigations ;
- L'implication des opérateurs techniques ;
- Le renforcement de l'entraide judiciaire et de la coopération internationale.

C. Le projet actuel de loi relatif à la lutte contre la cybercriminalité

Lors d'une conférence de presse animée à l'issue de l'adoption des deux projets de loi portant code de procédure pénale et traitement des données personnelles à l'Assemblée populaire nationale (APN), Le ministre de la Justice a affirmé mercredi28/03/2018 à Alger, que son secteur préparait un projet de loi relatif à la lutte contre la cybercriminalité, mettant en avant la nécessité d'"adapter la législation algérienne aux développements survenus dans le monde".

Le ministre a mis l'accent sur l'importance de la coopération judiciaire internationale, lorsqu'il s'agit de l'utilisation des nouvelles technologies, qui doit être renforcée pour faire face au terrorisme et au crime organisé qui ne peuvent être combattus que dans le cadre de la coopération et des échanges d'informations, tant au niveau régional qu'international.[1]

II.3.Agents et organes de lutte contre la criminalité électronique

A. Organe National de Prévention et de Lutte contre les Infractions liées aux Technologies de l'Information et de la Communication(*ONPLITIC)*

La promulgation de la loi n°09-04 du 5 août 2009, article 13, portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication, l'organe national de prévention et de lutte contre les infractions liées aux technologies de l'information et de la communication a été mis en place , dans la perspective d'accompagner et protéger le citoyen algérien dans son entrée dans le cyber espace, dont beaucoup ne connaissent pas les dangers.[2]

L'organe est composé par des membres du gouvernement, des responsables des services de sécurité, et deux magistrats de la Cour suprême. Il regroupera aussi des officiers et agents de la police judiciaire émanant des services de renseignements militaires, des magistrats, des officiers de la Gendarmerie Nationale et de la Police nationale.

[1] www.cerist.dz. *O*p.cit.
[2] http://reporters.dz /index.php/rss-a-la-une/item/54151-organe-national-de-prevention-et-de-lutte-contre-les-infractions-liees-aux-tic-un-decret-nomme-les-representants-de-la-presidence-et-de-la-defense. Consulté le 09/08/2018

L'organe aura entre autres pour fonction de prévenir les cyber-attaques, d'assister les autorités judiciaires et les services de police judiciaire, d'assurer la surveillance des communications électroniques en cas d'infractions d'actes terroristes et subversifs ou d'atteinte à la sûreté de l'Etat.[1]

B. Centre de Prévention et de Lutte Contre la Criminalité Informatique et la Cybercriminalité (CPLCIC)

La gendarmerie nationale a mis en place une stratégie de protection, réduisant ainsi le champ de manœuvre des réseaux criminels et prévenir des attaques et les éventuels recrutements via ce monde virtuel. Pour cela, le CPLCIC s'engage dans la lutte contre les nouvelles formes de criminalité via le net.[2]

C. Ingénieurs et techniciens formés

Le mois d'Avril dernier le ministre de la Formation et de l'Enseignement professionnels, a annoncé, à partir de Tipasa, la formation de 24.000 ingénieurs et techniciens pour faire face à la criminalité électronique et protéger les réseaux et systèmes informatiques. "Partant du principe que la lutte contre la criminalité électronique et la protection des réseaux et systèmes informatiques passe par la formation de ressources humaines qualifiées.

Dans la perspective de faire face aux risques liés à la cybercriminalité, le ministère s'est lancé dans la formation d'une ressource hautement qualifié par la signature d'une convention en 2002 avec la société " Cisco ", laquelle a abouti à la création d'un centre pour la formation de "formateurs Cisco ", parallèlement à la création, à partir de 2006, de 36 académies à travers le pays, en application d'un programme " ambitieux et novateur " visant une formation et une mise à niveau conformément aux normes mondiales en vigueur.

L'Algérie compte, selon le ministre de la Formation et de l'enseignement professionnels, 700 formateurs Cisco , en matière d' " exploitation ", "exploration " et " sécurité " , au moment où la même société " Cisco " a certifié 21.000 diplômes d'ingénieurs et techniciens, estimant que cet " effectif humain hautement qualifié " aura une " contribution certaine dans la protection des réseaux et systèmes électroniques des entreprises et institutions , dont il a renforcé les rangs".

Conclusion

Partons du constat selon lequel les TIC se développent non seulement à un rythme infiniment plus rapide que les mentalités de la population en matière d'utilisation des TIC,

[1] http://www.nticweb.com /it/8398-un-organe-national-de-pr%C3%A9vention-et-de-lutte-contre-les-infractions-li%C3%A9es-aux-tic-mis-en-place.html. Consulté le 08/08/2018.
[2] Article rédigé par Mounira Amine Seka, le quotidien Soir d'Algérie, 2017, www.soird'algerie.dz consulté le 08/08/2018.

voir le manque de civisme et de confiance envers cette technologie. Malgré les investissements financiers continus et croissants dans ce domaine l'Algérie reste toujours parmi les pays les moins connectés à cause de la non fiabilité des débits de connections.

Le phénomène de cybercriminalité en Algérie est en phase embryonnaire car elle occupe une place moins importante par rapport aux infractions classiques fréquentes dans notre société. Cela n'empêche pas que l'Algérie reste un pays plus ciblé par les attaques informatiques, selon une étude déclaré par la société privée spécialisée dans la sécurité des systèmes d'information, kaspersky Lab l'Algérie est le 9e pays le plus menacé par le piratage et 60% des ordinateurs sont atteints de virus. Seulement, comme l'Algérie n'est pas encore véritablement passée au paiement électronique, elle ne représente pas une proie facile pour les traqueurs de fonds.

Section 2 : Interprétation et analyse des résultats de l'enquête

Introduction

Pour mieux analyser la propagation des TIC dans le secteur bancaire, Comprenant les banques de la wilaya de Tizi-Ouzou, ainsi la réalité de leurs aléas sur le système financier qui est déterminé sous le terme de « cybercriminalité »; objet de notre recherche; nous avons fait recours à une enquête sur le terrain par questionnaires *(voir annexe N°14)* et entretiens. Cette enquête a pour objectif de collecter le maximum d'information qui nous aidera à mieux cerner l'état des lieux en matière d'utilisation des TIC dans les banques ainsi le degré de leur implication dans la naissance des risques numériques. Pour ce faire, nous avons interrogés les banquiers des directions générales des banques de la wilaya de Tizi-Ouzou, ainsi les autorités responsables de lutte contre le crime informatique (direction de la sûreté de la wilaya).

Afin de mener à bien notre travail, nous avons suivi la démarche suivante :

- Le dépôt d'un questionnaire auprès des banques de notre échantillon ;

- La réalisation des entretiens avec les responsables des banques et de la sûreté de la wilaya, et la collecte des données à leur niveau.

La présente section sera scindée en trois points essentiels, le premier est une présentation du réseau bancaire de la wilaya de Tizi-Ouzou, le second point consistera en la présentation de la démarche méthodologique de notre enquête, suivie par l'analyse et l'interprétation des principaux résultats de la recherche.

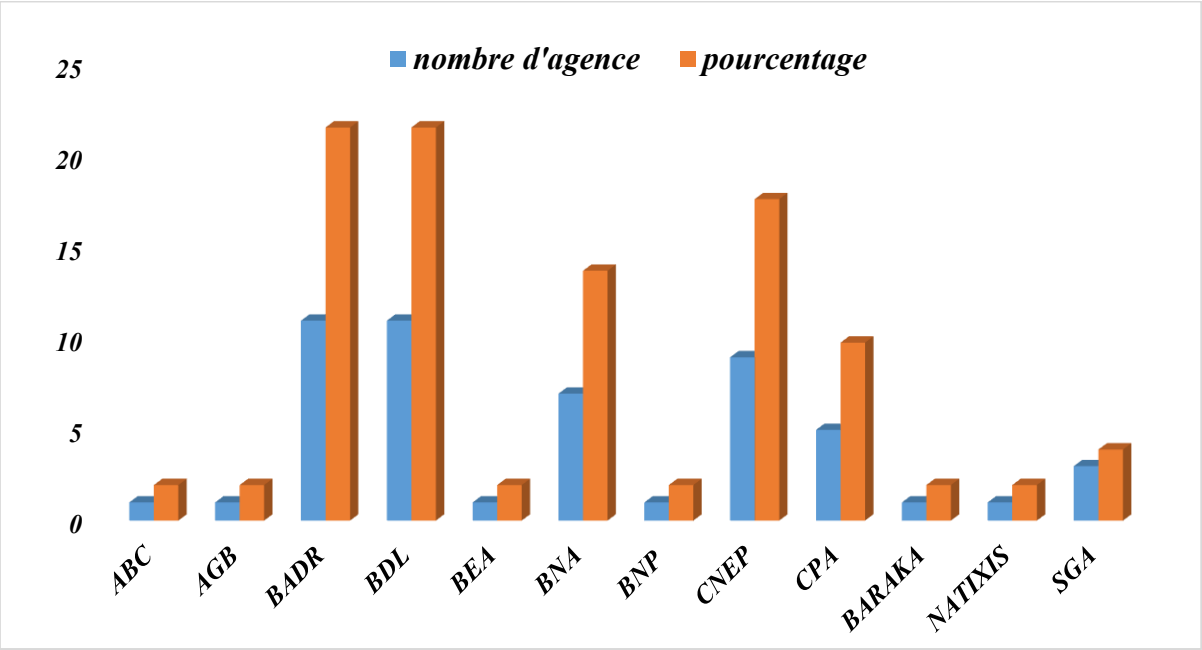
I/ Présentation du réseau bancaire de la wilaya de Tizi-Ouzou

Ce point sera consacré à la présentation du contexte actuel bancaire de la wilaya de Tizi-Ouzou. Actuellement le nombre d'agence des banques publiques et privés est comme suit :

Tableau n° 12 Banques publiques et privées	Nombre d'agences en 2018	Le taux de concentration en %
ABC	01	1.96
AGB	01	1.96
BADR	11	21.57
BDL	11	21.57
BEA	01	1.96
BNA	07	13.73
BNP Paribas	01	1.96
CNEP	09	17.65
CPA	05	9.80
EL Baraka	01	1.96
Natixis	01	1.96
Société Générale	02	3.92
Total	51	100

Source : établie par nos soins à partir des informations recueillies au niveau des banques de notre échantillon.

Graphe N°14 : Le nombre d'agences bancaire et leur pourcentage dans la wilaya de Tizi-Ouzou



Source : réalisé par nous-même à partir des données de tableau précédent.

Selon les données du tableau et de graphe ci-dessus, nous remarquons que la BADR et la BDL sont les banques les plus denses dans la wilaya de Tizi-Ouzou avec un taux de 21,57% chacune du total des agences implantées dans la wilaya, soit un réseau de Onze (11) agences réparties dans les communes de la wilaya. L'objectif visé par l'Etat est de promouvoir les activités agricoles, artisanales, agro-industrielles à travers la BADR, et des particuliers à travers la BDL dans les milieux urbains, ruraux et montagneux de la wilaya. La CNEP est classée en seconde position avec un réseau de neuf (9) agences réparties dans quelque daïra de la wilaya, soit 17, 30 % du total du réseau d'agences, la densité de la CNEP banque est très importante pour favoriser et développer les activités de crédits au logement et la mobilisation de l'épargne. Dans le secteur privé c'est la Société générale qui est en tête de liste avec un nombre de deux (2) banques.

II/Méthodologie de recherche

La méthodologie adoptée consiste à analyser les réponses recueillies par le questionnaire. Mais durant cette enquête nous avons rencontré quelques difficultés à savoir :

La première difficulté est l'obtention d'un rendez-vous pour un entretien. Les acteurs concernés sont inaccessibles et certainement très occupés et les agents compétents pour répondre à nos questions spécifiques sont difficiles à approcher.

La deuxième difficulté est forcément d'ordre stratégique ; les banques ne souhaitent pas divulguer certaines informations liées à leurs fonctionnement ce qui est compréhensible ; elles sont hésitantes à fournir des informations concernant leur stratégie adoptée et les

politiques suivies dans ce domaine pour des raisons confidentiels ou par crainte de la concurrence.

- **Les outils utilisés**

Dans le cadre de ce travail de recherche, nous avons distribué un questionnaire aux différentes banques de notre échantillon qui est constitué de douze(12) banques privées et étatiques de la wilaya de Tizi-Ouzou afin de constater et d'essayer de mieux comprendre le degré d'utilisation des nouvelles technologies ainsi leur impact négatif sur l'activité bancaire.

En outre, il fallait bien formuler nos questions pour en tirer le maximum d'informations exploitables et de les traiter de manière optimale.

- **L'environnement**

Notre objet de recherche est les banques et la direction de la sûreté de la wilaya de Tizi-Ouzou. L'échantillon de douze banques, privées et publiques, est représentatif car les différentes agences suivent la politique de l'agence mère**.**

III/ Interprétation et analyse des résultats d'enquête

Nous portons notre intérêt à ce stade sur les résultats de l'enquête ayant trait à l'analyse de degré de l'utilisation des TIC et celui de prolifération du phénomène de la cybercriminalité dans les banques de la wilaya de Tizi-Ouzou, et cela à travers le traitement et l'analyse des données des questionnaires recueillis.

En vue de vérifier l'hypothèse de notre recherche, nous tenterons de présenter les résultats de l'enquête par une analyse des réponses données par les responsables de la sûreté de la wilaya ainsi ceux des banques enquêtées tout en respectant les axes de notre questionnaire.

III.1.Analyse et interprétation des résultats recueillis au niveau des banques

D'après le tableau ci-dessous, le nombre de banques qui ont répondu au questionnaire est de neuf (09) banques sur un total de douze (12) banques. Comme le démontre la figure n°15, ces banques sont réparties équitablement entre banques privées et banques publiques, ce qui fait six (06) banques privées et six (6) banques publiques de notre échantillon d'étude.

Tableau N°13 : Echantillon de banque répondant au questionnaire

Nom Banques	Réponse
ABC	Non
AGB	Oui
BADR	Oui
BDL	Oui
BEA	Oui
BNA	Oui
BNP Paribas	Oui
CNEP	Non
CPA	Oui
EL Baraka	Oui
Natixis	Non
Société General	Oui
Total	9/12

Source : élaboré par nous même à partir des données collectées

Présentation des profils (catégorie de grade, poste occupé, niveau d'étude des répondants)

Le tableau suivant montre que 33.33% des responsables enquêtés sont des directeurs d'agence, avec 44.44% de l'échantillon qui forment la catégorie de maitrise assurant le statut de chef de service, et commerce extérieure, conseiller de la clientèle avec 11.11% chacune.

Guide d'entretien

	Effectifs	Pourcentage(%)
Chef de service	4	44,44
Commerce extérieure	1	11.11
Conseiller clientèle	1	11.11
Directeur d'agence	3	33.33
Total	9	100

Source : réalisé par nous-même à partir des données collectées.

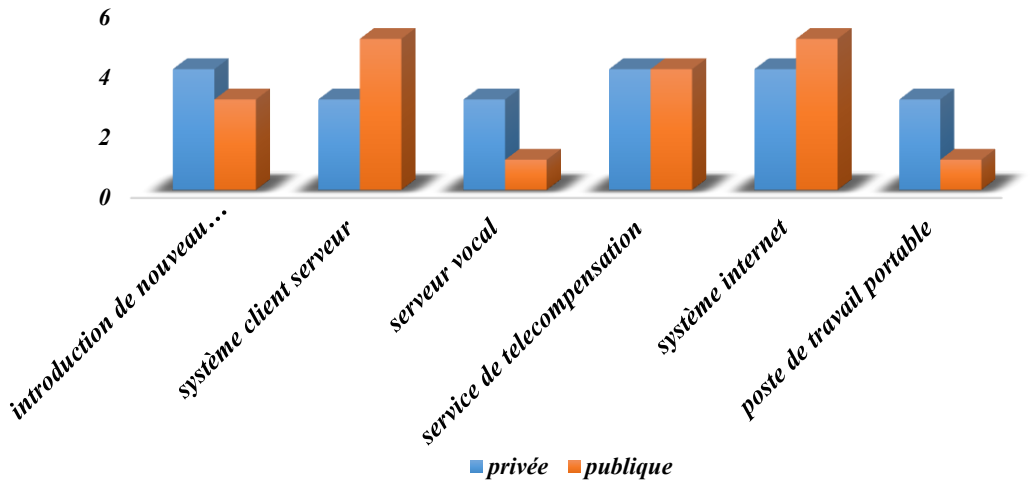
- **A. Les TIC des banques**

Les banques, confrontées à un environnement économique, et technologique en pleine mutation, ont subi des changements profonds dans leur fonctionnement. La plupart des banques de notre échantillon ont introduit de différents TIC pour répondre à ces changements. Les tableaux, graphes et figures ci-dessous nous montre le degré d'intégration des différents aspects des TIC dans leur système.

- **Les TIC que disposent les banques**

D'après le graphe n°16 les banques privées investissent plus en matière d'introduction de nouveaux équipements informatiques, la réalisation d'un serveur vocal et les poste de travail portables. En outre de TIC déjà décris, la BNPP investisse dans le multi canal et la BEA l'introduction dans le futur proche du SAP (*Système d'Automatisation de paiement*).

Graphe 16:les TIC que dispose les banques



Source : élaboré par nous même à partir des données collectées.

- **Impact d'introduction des TIC :** le tableau suivant montre l'impact des TIC sur le mode interne de travail

Tableau 14 : Impact sur le mode interne du travail

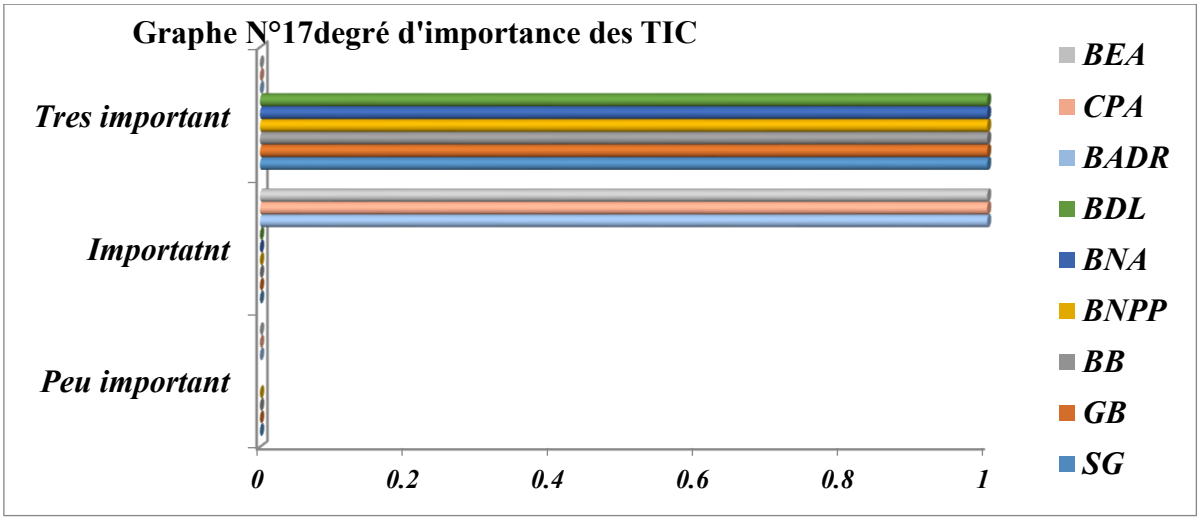
Impact sur le mode interne du travail	BNA	BEA	BDL	CPA	BADR	SG	GB	BB	BNPP
Rapidité et fiabilité de traitement des opérations	+	+	+	+	+	+	+	+	+
Amélioration de l'efficacité de la perception	+	+	+	+	+	+	+	+	+
Réduction de la contrainte de la présence physique derrière un bureau	+	-	+	+	+	+	+	+	+
Réduction du risque d'erreur	+	-	+	+	+	-	+	+	+
Suppression des taches en double	+	+	+	+	+	-	+	+	+

Source : élaboré par nous même à partir des données collectées.

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 perception, réduction de la contrainte de la présence physique derrière un bureau, puis suppression des taches en double et enfin dans la réduction du risque.

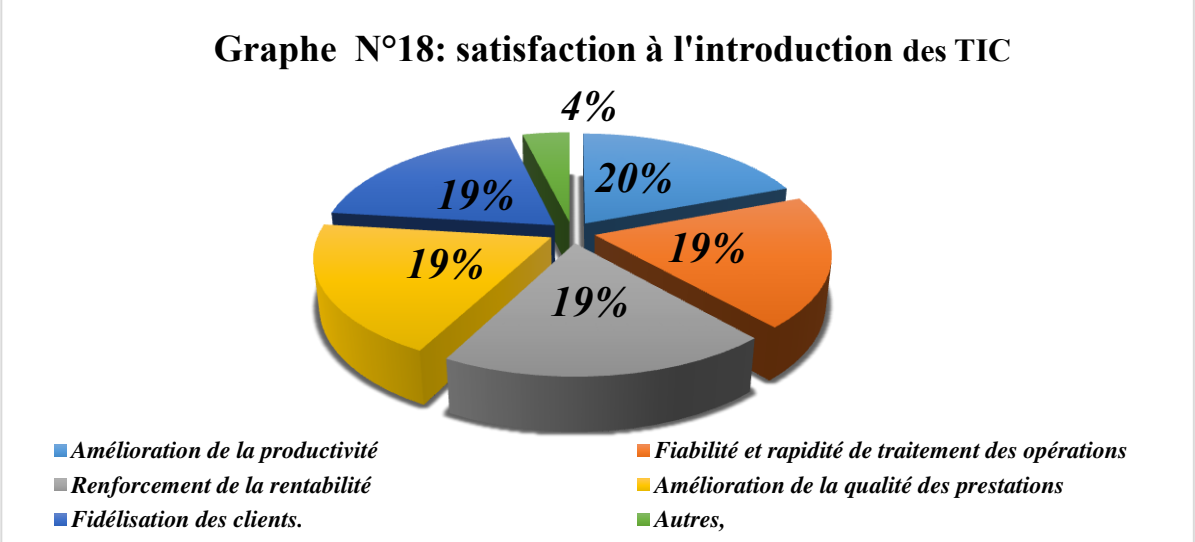
- **Impact sur la productivité**

L'introduction des nouvelles technologies dans les banques est important dans certaines banques et parfois très important aux autres. Comme il est indiqué dans (le graphe n°17). Les trois banques Etatiques (BEA, CPA, BADR) le considère important en tant qu'outil de travail dans l'amélioration de leur productivité vu la fiabilité et la rapidité à l'accès aux informations, comme il est très important chez la BDL et la BADR, ainsi dans l'ensemble des banques privées questionnées.



Source : élaboré par nous même à partir des données collectées.

- **Satisfaction d'introduction des TIC**

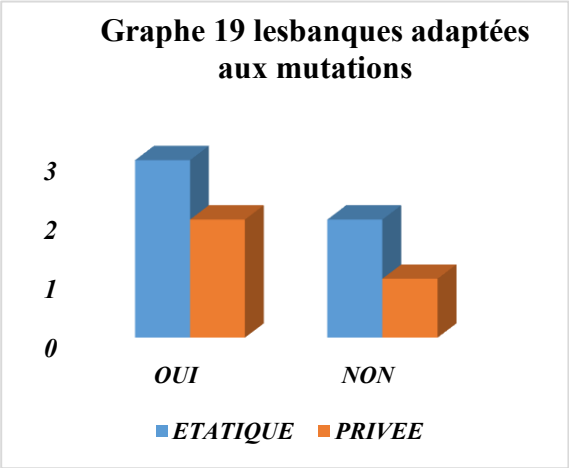


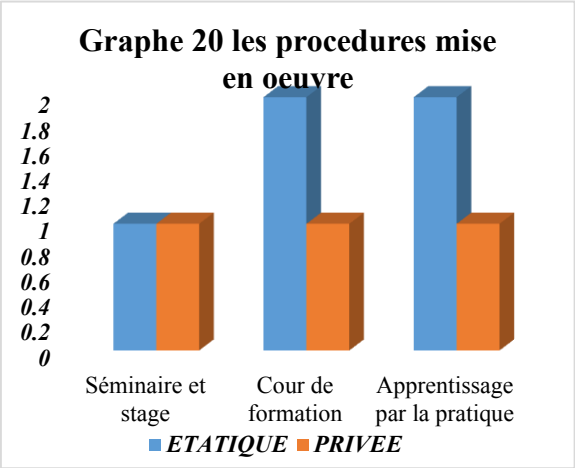
Source : élaboré par nous même à partir des données collectées.

Au sein des banques interrogées les satisfactions obtenues par les banques étatiques et privées par l'introduction des nouvelles technologies dans leurs activités sont reparties d'une façon équivalente dont **20%** pour la fidélisation des clients, et **19%**(pour l'amélioration de la productivité ainsi pour la fiabilité et rapidité de traitement des opérations et **19%** pour l'amélioration de la qualité des prestations et enfin renforcement de la rentabilité. (*Graphe N°18).*

- **Adaptation aux mutations des TIC**

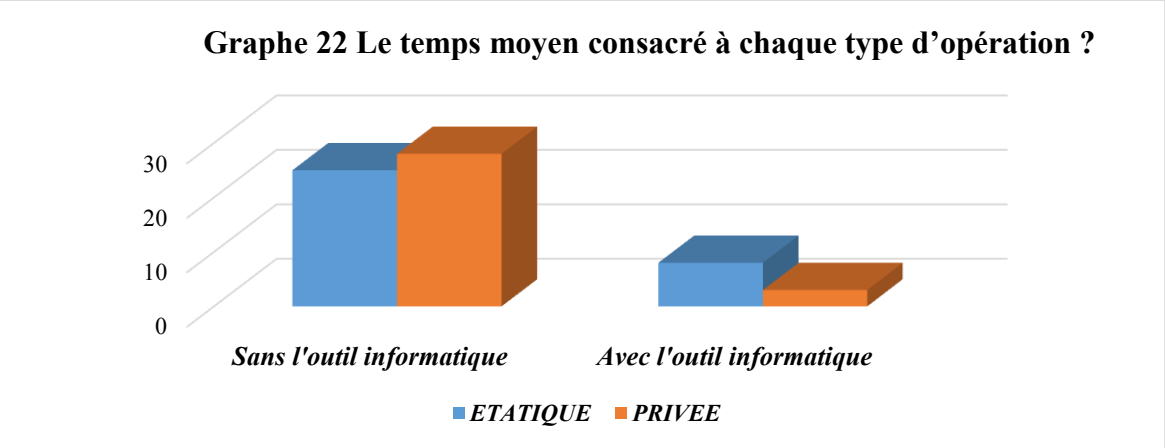
La pluralité des banques interrogées 5/9 sont adaptées facilement aux mutations technologiques (*Graphe n°19*) et ce, pour les raison suivante SG : obligation de changement, BNPP : équipe jeune et diplômée plus informatisée et pour la CPA, BDL et BNA : des formations bancaires ont été mise en œuvre auparavant. Par contre 3/9 des banques étatiques et privée restantes ont trouvé des difficultés par rapport aux mutations dont les procédures mise en œuvre pour adapter à ces mutations représentées dans le graphe N°20.





Source : élaboré par nous même à partir des données collectées.

- **Rôle des TIC**



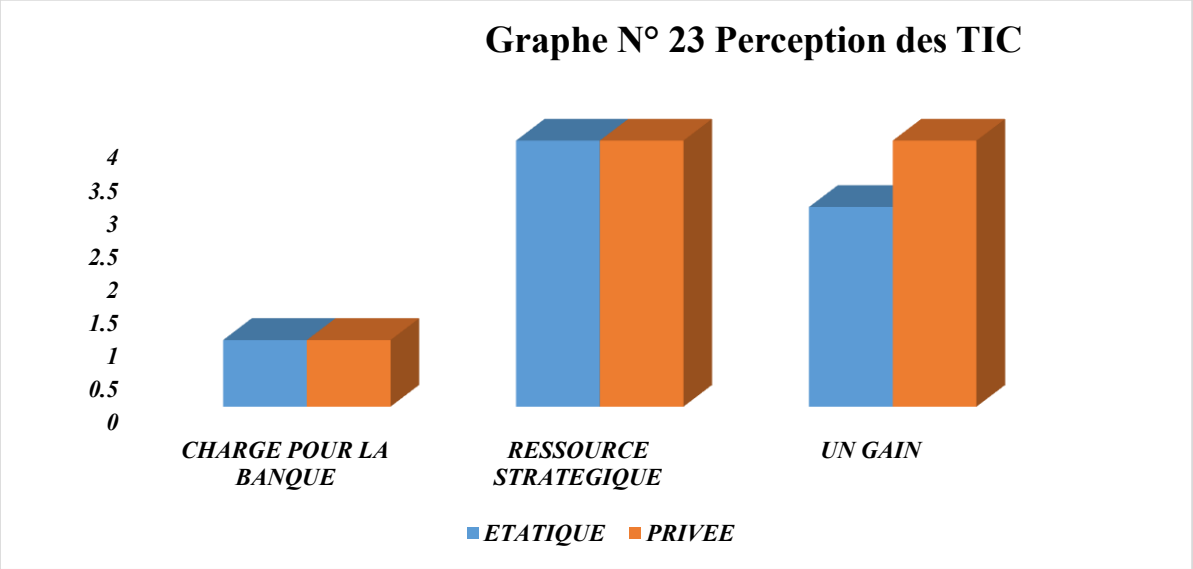
Source : élaboré par nous même à partir des données collectées.

Grâce aux technologies de l'information les banques peuvent effectuer plusieurs opérations par jours et le temps moyen pour le traitement est rapide et efficace comme il est démontré dans les graphes 21 et 22 précédents. Les banques étatiques enregistrent un nombre moyen d'opérations effectué sans l'outil informatique qui ne dépasse pas 500 opérations pendant environs 25 min, contrairement aux banques privées qui atteint presque les 2000 opérations pendant un temps de 28 min environ par jour. Alors que avec l'outil informatique l, les deux secteurs traitent presque le même nombre moyen d'opérations pour un écart de temps très important ; privé 3min tandis que le public 8 min. (*Graphe22*).

- **Importance des TIC**

La technologie joue un rôle très important au sein des banques étatiques et privés de ce fait la vision des banques au sujet des TIC a été déterminé comme étant une source de gain et une ressource stratégique pour les banques privées et Etatiques (*Graphe n°23*), et cela s'explique par l'investissement qui suit son installation dans l'entretien et la maintenance du matériel, comme dans les formations employés pour s'adapter au TIC .

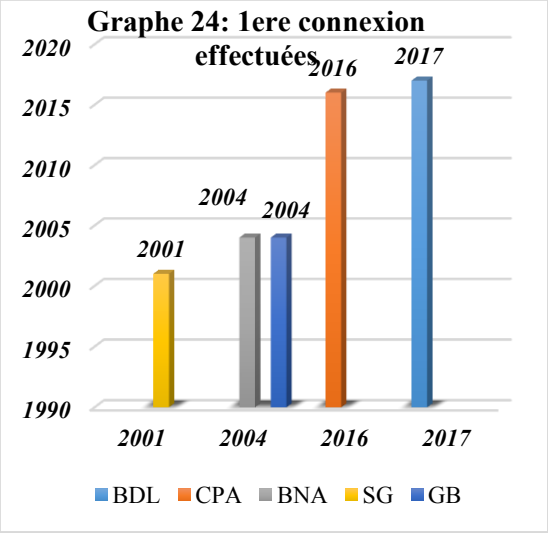
Au cours de notre enquête, aucune banque n'a donné son opinion personnelle concernant le rôle des TIC dans la banque. Mais en contrepartie elles ont cité quelques propositions concernant l'introduction d'autres nouvelles technologies. La BEA a proposé le E-Banking à grand échelle et fabriquer les GAB à l'intérieur de l'agence, de son côté le CPA c'était d'améliorer les SI actuel, et pour la BDL et la BADR c'est l'automate dans les réseaux agences. Les banques privées SG et BNPP prévoient le m banking.

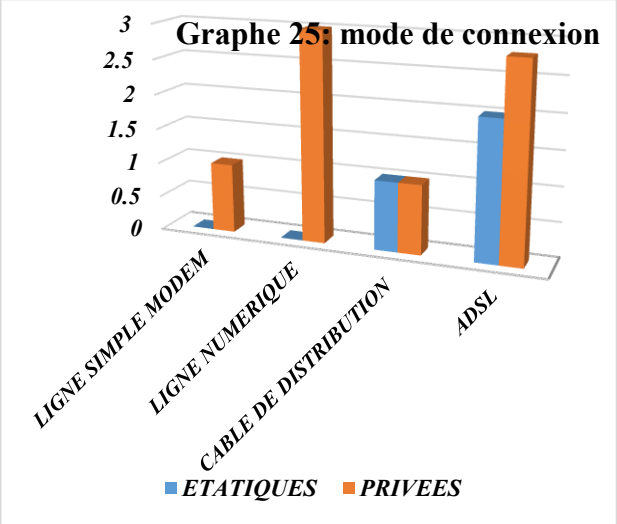


Source : élaboré par nous même à partir des données collectées.

- **La date d'introduction d'Internet (effectuer la 1ère connexion)**

Parmi les banques étatiques interrogées, la banque société général est la première à introduire l'internet en 2001 dont elle est connecté par une ligne téléphonique numérique et l'ADSL, viendra après la BNA qui est connecté par un câble de télédistribution, et Gulf Bank 2004 par une ligne numérique et CISCO, en final c'est le CPA et la BDL qui sont connectés en 2016-2017 avec l'ADSL et une ligne spécialisé(*graphe n°24 et 25*) d'âpres notre enquête la BEA n'est pas connecté à internet qui usent de l'intranet estimant que c'est pour assurer la sécurité des données de la banque.





Source : élaboré par nous même à partir des données collectées.

Les objectifs d'utilisation d'internet dans les banques interrogées sont représentés dans le tableau N°15 suivant : **Tableau n°15 : objectifs d'utilisation d'internet**

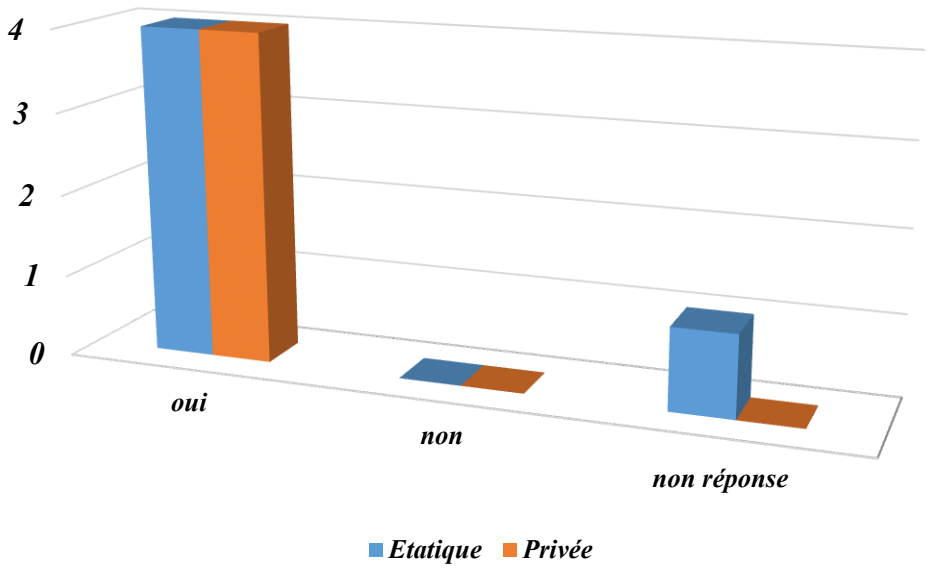
Les objectifs	BNA	BDL	BEA	BADR	CPA	SG	GB	BB	BNPP
Pour télécharger des fichiers (documents, rapport, études,…)	-	-	-	-	-	+	-	+	+
Pour télécharger des logiciels (gratuit ou pas)	-	-	-	-	-	+	-	-	-
Pour rechercher des informations	-	-	-	-	+	+	+	-	+
Consultation de courrier électronique	+	+	-	-	+	+	+	+	+
Echange de données avec les coopérants (ou liens avec vos agences)	+	+	-	+	+	+	+	+	+
Echange de fichiers avec les clients	-	-	-	-	-	+	+	+	+
La présentation de la banque	-	-	-	+	+	+	+	-	+
Diminuer les couts	-	-	-	-	-	+	-	-	+

Source : élaboré par nous même à partir des données collectées.

- **L'existence d'un site WEB**

Les sites web regroupe un ensemble de page web reliées entre elles et situées sur un même serveur, les sites de référence en banque et finance, c'est des véritables sites de portail, où on trouve les information sur la bourse, les marchés financiers, et les informations économiques et financières,[1]la disposition d'un site web par les banques enquêtées est une manière de renforcer leur présence sur internet, ainsi le graphe N°27 montre que l'ensemble des banques étatiques et privées enquêtées qui activent à la wilaya de Tizi-Ouzou ont un sites web, par contre une banque n'as pas donnée de réponse à cette question (*CPA*).

Graphe 27: existance d'un site web

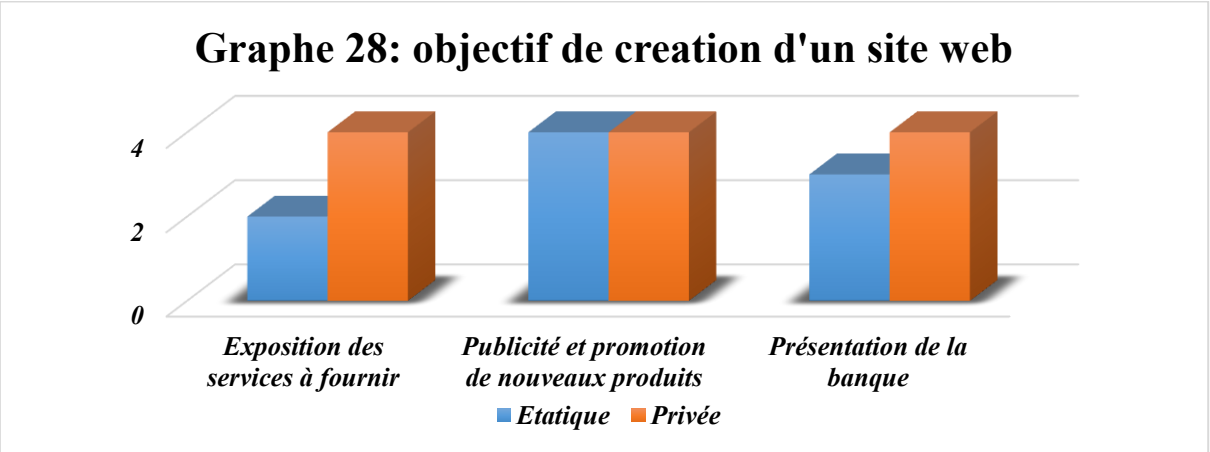


Source : élaboré par nous même à partir des données collectées.

- **Les objectifs de la création des sites Internet**

Les objectifs de création d'un site comme nous venons de le citer au-dessus sont multiple à savoir la présentation de la banque, la publicité des produits, l'exposition des services Etc. Durant notre enquête la pluparts des banques privées sont motivées à atteindre le maximum des objectifs via l'hébergement d'un site y compris ceux que nous venons de citer (graphe 28), contrairement aux banques étatiques qui se focalisent sur quelques-uns et ignorent quelques autres.

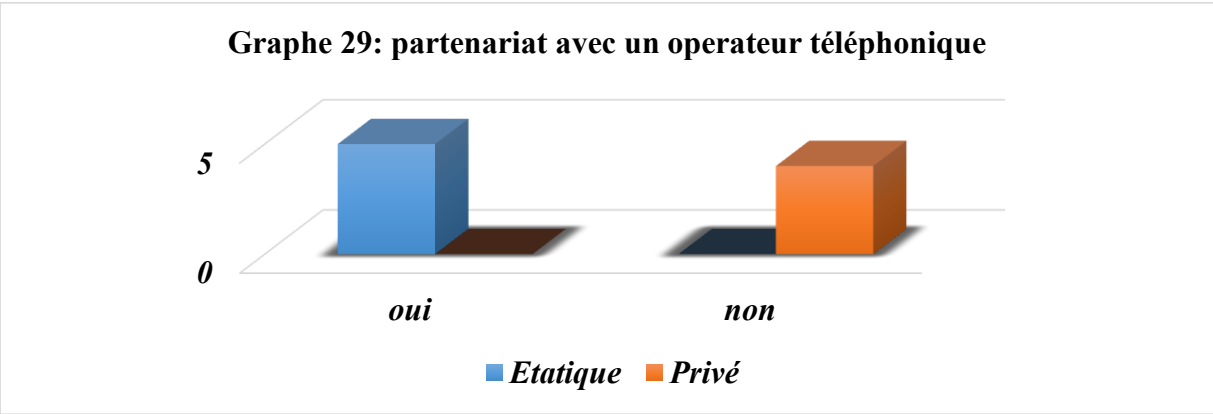
[1] Julie .G. « *internet guide des meilleurs sites pour la gestion et le management* » édition 2000, P76.



Source : élaboré par nous même à partir des données collectées

- **Partenariat avec un opérateur téléphonique ou Algérie Télécom ?**

Nous remarquons que seulement cinq banques sur neuf (BEA, BADR, BNA, CPA, BDL) 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 (BEA) où le partenariat s'est fait avec l'opérateur SWIFT Télécom. Les banques privées n'ont pas de partenariat avec Algérie télécom sauf Gulf Bank qui est en partenariat avec Mobilis et ce juste pour ces employés.



Source : élaboré par nous même à partir des données collectées

B. Moyens de paiement (monétique et automatisation) :

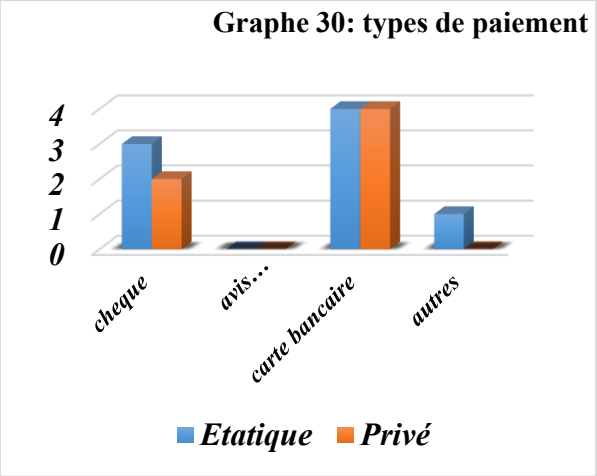
L'étude des différents moyens de paiement automatisés réside à clarifier les points suivants.

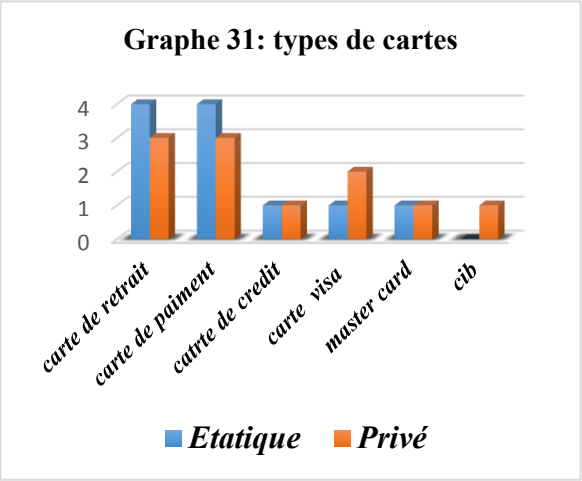
- **Le moyen de paiement le plus automatisé**

D'après les banques interrogées, il s'est avéré que la carte de paiement est le moyen le plus automatisé dans les banques Etatiques et privées comme il est indiqué dans le graphe n°30 car elle offre aux clients un paiement virtuel, c'est-à-dire via internet et elle permet aussi des retraits d'espèces aux distributeurs de billets, suivi par le chèque utilisé beaucoup plus

dans les banques Etatiques , il existe aussi certaines banques qui utilisent d'autre moyens comme le CPA qui utilise l'ordre de virement .

- **Type de carte utilisée**



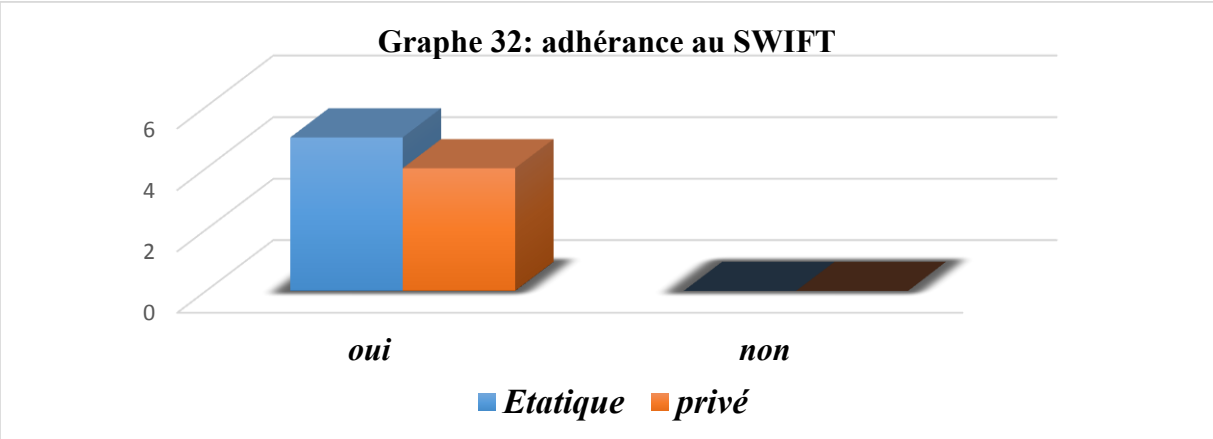


Source : élaboré par nous même à partir des données collectées

Nous remarquons que les cartes de paiement et de retrait sont les plus utilisées chez les banques Etatiques et privés (*Graphe n°31*). Certaines banques utilisent aussi la carte Visa et Master CARD et la carte interbancaire le cas des banques (*société General, Gulf Bank, Baraka bank.BDL*) et leur degré d'utilisation est presque le même.

- **Adhérence au réseau SWIFT**

L'ensemble des banques de notre échantillon sont membre du réseau SWIFT (graphe n°32). La date d'adhérence à ce réseau diffère d'une banque à une autre, BDL en 2001 suivi par la SG EN 2005, BNA et BEA en 2008. L'utilité de cette adhérence réside dans la sécurisation des transactions à l'étranger.



Source : élaboré par nous même à partir des données collectées.

- **Disposition d'un (DAB/GAB)**

A partir de notre enquête, nous déduisons que le développement des DAB au niveau des banques publiques est plus élevé par rapport au banques privés eà l'extension de société générale comme il est indiqué dans le tableau n °16 et le graphe 33 ci-dessous :

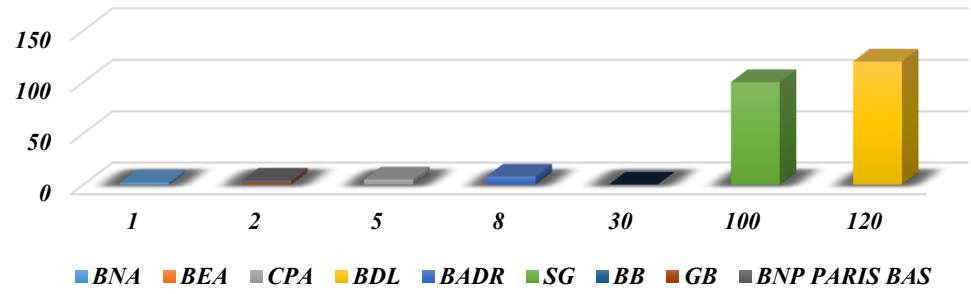
Tableau n°16

	BNA	BEA	CPA	BDL	BADR	SG	BB	GB	BNPP
Nombre d'agence	07	01	05	11	11	02	01	02	01
Nombre de DAB	2	-	5	120	08	100	-	2	1

Source : élaboré par nos même à partir des données collectées.

Comme nous voyons dans le tableau n° 16 la BEA et El baraka Bank ne dispose que des GAB, dont nous trouvons 100 GAB à la BEA et 30 GAB à Baraka Bank.

Graphe 33:Nombre de DAB



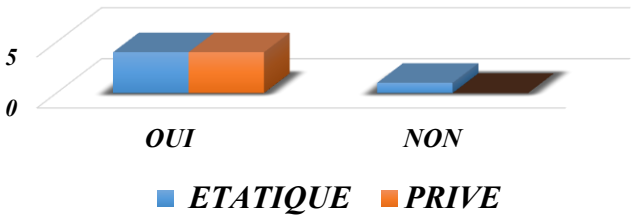
Source : élaboré par nous même à partir des données collectées

- **C. système informatique**

La production de la banque est de traiter l'information, le stocker automatiquement dans des banques de données, d'où la nécessité d'adapter une stratégie de développement du système informatique**.**

- **Adaptation d'une stratégie de développement du système informatique**

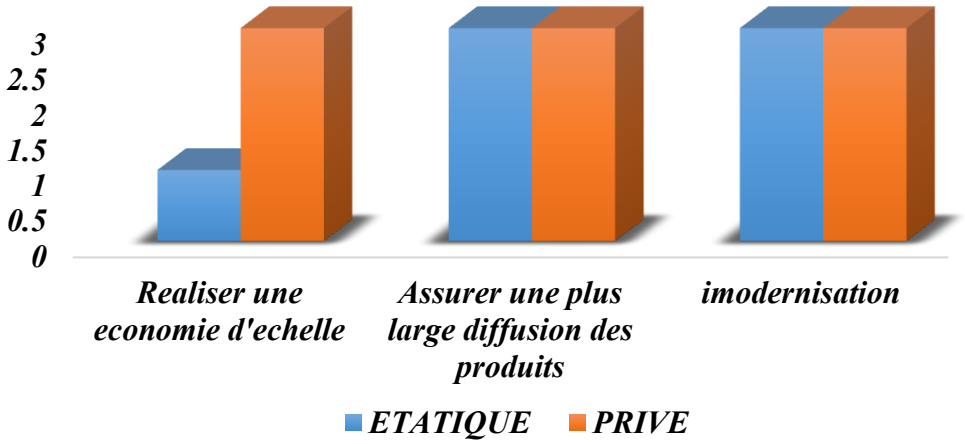
Graphe34: le developpement du systeme d'information dans les banques



Source : élaboré par nous même à partir des données collectées

D'après le graphe n°34, le SI est développé à 99%, c'est-à-dire que presque toutes les banques (Etatiques et privées) ont investi dans le développement de celui-ci, sauf la BEA qui n'a pas adapté une stratégie à développer son SI. Selon les banques interrogées, la stratégie de développement du SI a été effectuée sous quelques critères déterminés selon leur choix (graphe n°35). La réalisation d'économie d'échelle est un critère aussi important dans la stratégie du développent du SI au sein des banques privées ce qui est délaisser par les banques Etatiques sauf la BNA qui le prend en considération.

Graphe 35: stratégie de developpement du SI



Source : élaboré par nous même à partir des données collectées

- **Qualification du processus d'informatisation de la banque (y compris les agences)**

Les banques ont connu alors un processus d'informatisation à plus de 90% graduel à vitesse rapide (la totalité des banques privées) et entre70% à 90% (pour la banque étatique BDL),et entre 50%et 70% graduel à vitesse plutôt moyenne (*voir graphes n36 et 37*).

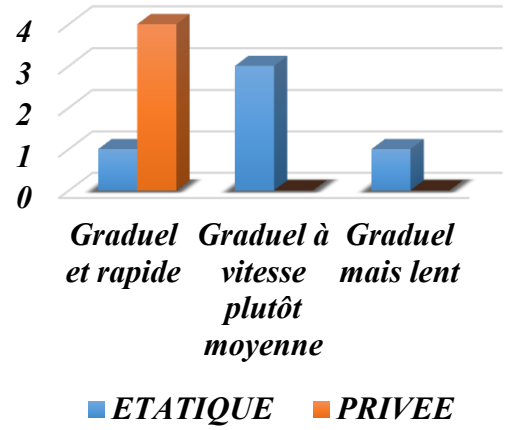
Les banques sont toujours prêtes à introduire de nouvelles technologies pour améliorer leur quotidien. Donc, chaque banque consacre un budget à l'informatisation (équipement et logiciel), mais pendant notre enquête nul n'a pu répondre à cette question puisque lors des entretiens que nous avons eus avec les responsables, ces derniers nous ont expliqué que certaines informations sont centralisées et qu'elles ne peuvent être divulguées.

Par ailleurs, sur un total de réponses de deux (02) banques sur neuf (09), le budget annuel destiné à l'informatisation du total du budget en pourcentage de la banque se répartit comme suit :

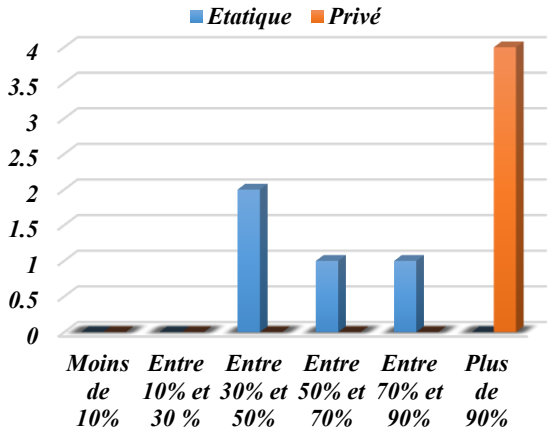
- Société Générale Algérie: 25% de son budget total dans l'informatisation ;
- BDL: 20% de son budget total.

- **Le taux d'informatisation des banques et des agences**

Graphe 36: mode d'informatisation



Graphe 37: taux d'informatisation



Source : élaboré par nous même à partir des données collectées

- **Le contrôle de la performance du système informatique**

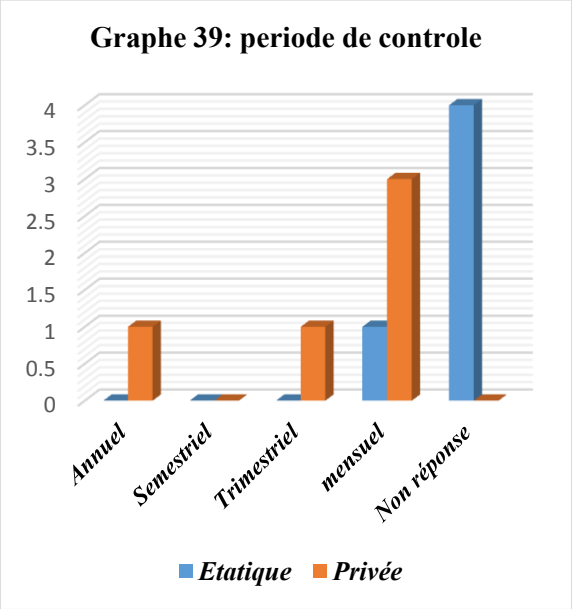
L'augmentation des risques technologiques et informatiques due au développement de la micro-informatique et son utilisation pousse les banques à contrôler la performance de leurs systèmes. D'après les résultats de l'enquête (*voir graphe n°38*), les banques privées procèdent au (3 banques interrogées sur un total de 4) contrôle de la performance de leurs systèmes, tandis que la plupart des banques Etatiques non pas répondus à cette question à l'exception de la BDL.

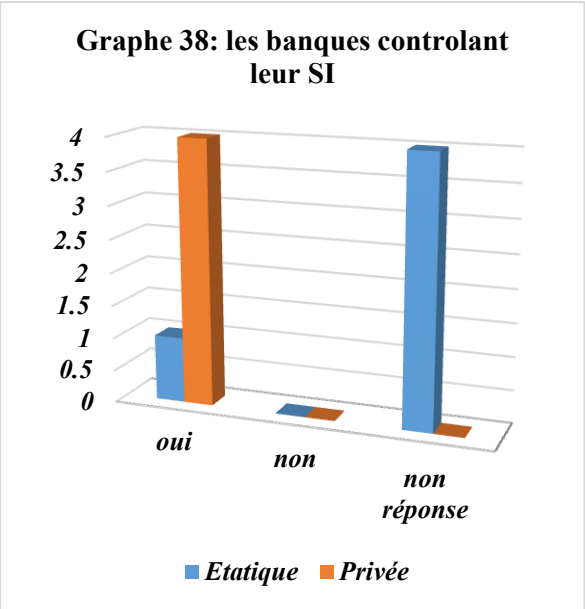
Ce contrôle se déroule soit mensuellement, trimestriellement, semestriellement ou annuellement (*voir graphe n°39*), dans notre cas la plupart des banques Etatique et privées, le contrôle s'effectue mensuellement ou trimestriellement. Il existe une seule banque qui affirme que le contrôle se fait annuellement en plus du contrôle mensuel et trimestriel selon le besoin.

La manière pour se faire diffère d'une banque à une autre :

- BDL : la mise en place des cellules de contrôle des données ;
- SG : suivant le retour des agents sur leurs défaillances et leurs erreurs ;
- GB : par le biais de l'équipe Help desk ;
- BNP P : questionnaires avec les collaborateurs et clients, certification, département de qualité.

- **La période de déroulement du contrôle**





Source : élaboré par nous même à partir des données collectées

- **D. Les risques numériques et la sécurité informatique**

Afin de pouvoir mesurer le risque, le surveiller, le gérer et le réduire ce contrôle suppose de nouveaux outils informatiques et de personnel capable de le concevoir et de l'appliquer. Grâce à l'utilisation d'intranet, la banque dispose de nouveaux moyens, à titre d'exemple les logiciels et antivirus performants. En plus, les banques utilisent un nouveau moyen pour la détection de risque ou de menace par la mise en place d'un système d'alerte.

Dans le cadre de notre recherche et en vue d'affirmer ou non notre hypothèse « qu'en est-il du cas des banques algérienne en matière des TIC et de la (cybercriminalité) », en se basant sur la question : « disposez-vous d'un système d'alerte en cas d'effraction ou de menace à caractère numérique ? », les résultats de l'enquête apparaissent dans le graphe n°40.

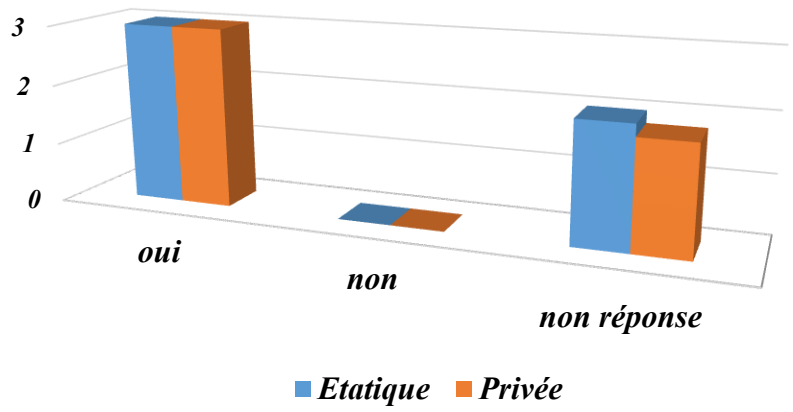
- **Système d'alerte en cas d'effraction ou de menace à caractère numérique**

nous remarquons, d'après la figure n°40, que 6/9 des banques interrogées affirment disposer au sein de leur banque d'un système d'alerte ce qui nous amène à dire qu'ils ont été confrontés à des risques et des menaces ; par contre 3/9 des banques interrogées n'ont pas répondus à cette question.

Il existe plusieurs systèmes et ils diffèrent d'une banque à une autre, c'est-à-dire chacune utilise un système :

- CPA : système d'alarme relié à la sûreté de la wilaya ;
- BDL : alarme et anti intrusion.

Graphe 40: disposition d'un systeme d'alerte



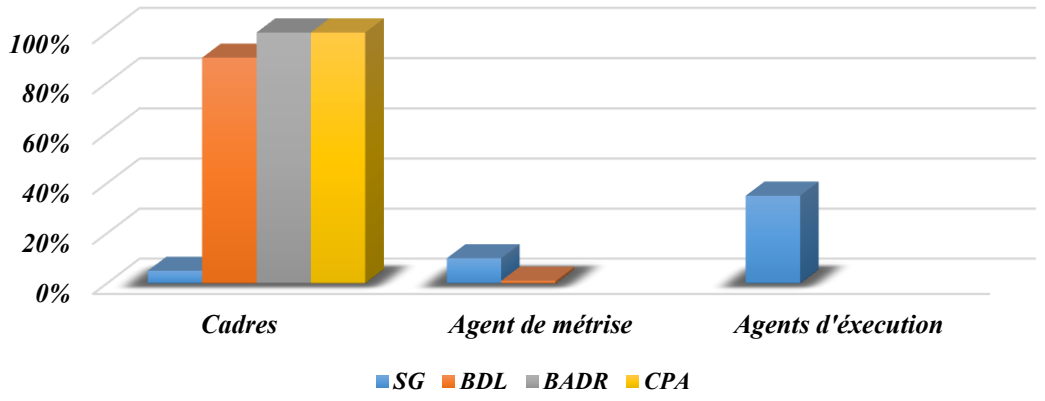
Source : élaboré par nous même à partir des données collectées

- **Nombre d'informaticiens auxquels la banque fait appel**

Les banques pour faire face aux menaces et aux risques informatiques encourus doivent se doter d'un personnel informaticien qualifié et compétent. L'informaticien contribue à faire évoluer en permanence les systèmes informatiques de la banque en fonction des objectifs stratégiques ainsi que des évolutions technologiques et réglementaires. Il doit faire preuve de vigilance quant à la gestion des risques liée à l'utilisation de l'informatique. Le chargé de qualité aide à l'amélioration des procédés internes de l'entreprise.

Selon notre enquête, nous constatons que 4/9 des banques interrogées n'ont pas répondus à notre question concernant le nombre d'informaticien recrutés. Le reste est représenté sur le graphe 41 suivante :

Graphe 41: statut d'informaticiens recrutés



Source : élaboré par nous même à partir des données collectées

- Avec le CPA : au niveau régional 11 agents et 2 informaticiens ;
- BDL : une cellule informatique par région.

- **La sécurisation des réseaux**

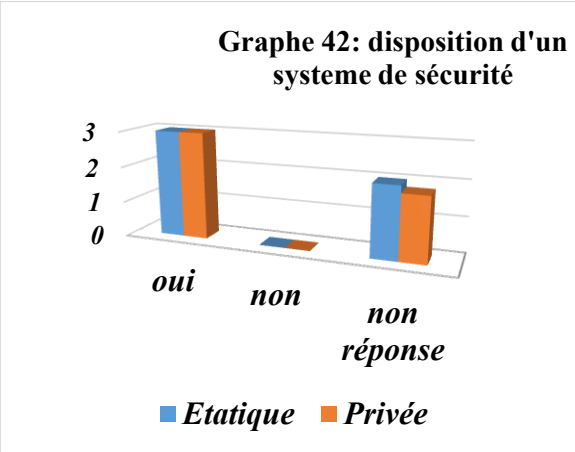
Il existe deux natures de la sécurité du réseau informatique centralisé, et la nature de la sécurité réseau décentralisée.

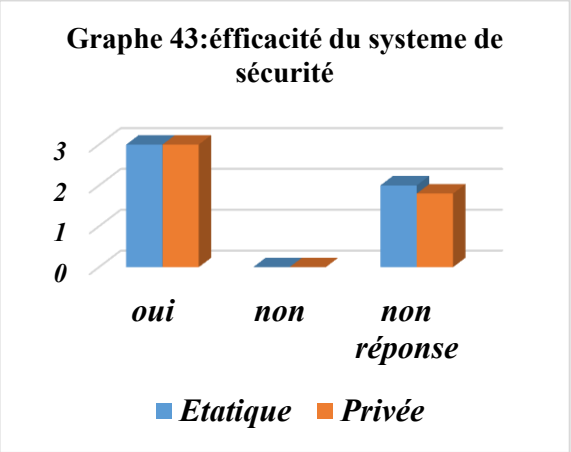
La majorité des banques interrogées (graphe n°42 et 43) affirment que la disposition d'une sécurité du Système d'Information est l'affaire de tous et dans tous les domaines. Elle exige une démarche organisationnelle allant de l'analyses des risques jusqu'à la mise en place de moyens et de procédures afin de garantir : la confidentialité des informations, l'intégrité de l'information, la disponibilité de l'information et la protection contre les virus.

La majorité des banques sécurisent leur réseau en s'appuyant à des dispositifs de sécurité, soit avec des logiciels adaptés à des menaces comme les virus, soit par un service spécialement perçu pour ça. Pour se faire le :

- CPA : sauvegarde les informations sur DAT et les transfère vers le site central ;
- BDL : met en place un antivirus compatible (agrément) ;
- SG : système de sécurité centralisé avec antivirus ;
- GB : met en place des logiciels, antivirus, et surveillance ;
- BNPP : antivirus, mot de passe.

- **Efficacité du système de sécurité**





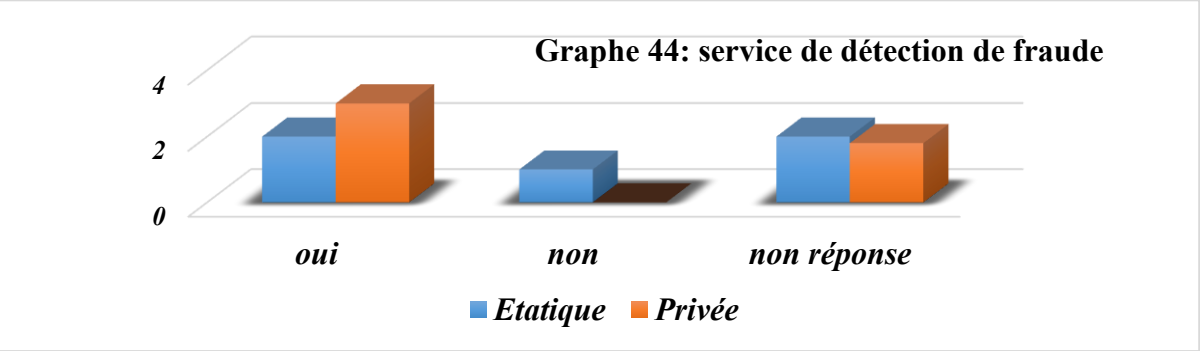
Source : élaboré par nous même à partir des données collectées

- **Les infractions liées aux TIC**

Durant notre enquête, la plupart des banques que ce soit Etatiques ou privées n'ont pas confirmé ni le nombre d'infractions liées aux TIC ni le degré d'atteintes par les différentes intrusions (mesures confidentielles). Malgré le nombre minimal de réponses que nous avons eu nous avons pu établir les interprétations dans les graphes qui suivent.

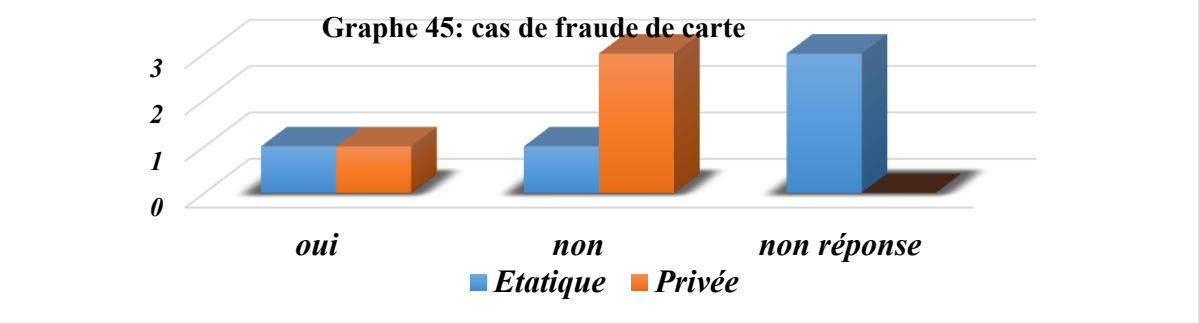
Certaines banques comme le CPA nous a donné une estimation de 1% de nombre d'infractions liées aux TIC auxquels a fait face, la SG confirme que le temps moyen de traitement des infractions est immédiat à la SATIM, de même pour GB, elle les traite très rapidement pour éviter les perturbations.

- **Service de détection et de traitement de fraude :** Ce qui concerne l'existence d'un service qui permet de détecter la fraude, 5/9 des banques interrogées ont répondus « oui » pour la possession de tel service (graphe n°44). Les 3 banques privées de notre échantillon, de leur côté détiennent ce service et ont était victime de fraude de carte et d'usurpation d'identité la BNPP (voir graphe n°45). En revanche les banques Etatiques comme le CPA ne possèdent ce service dont elle était victime de fraude de carte et d'usurpation d'identité. (*Graphe n°45*)



- **Source :** élaboré par nous même à partir des données collectées

- **Cas de fraudes de cartes bancaires ou des cas d'usurpation de numéros de cartes bancaires**

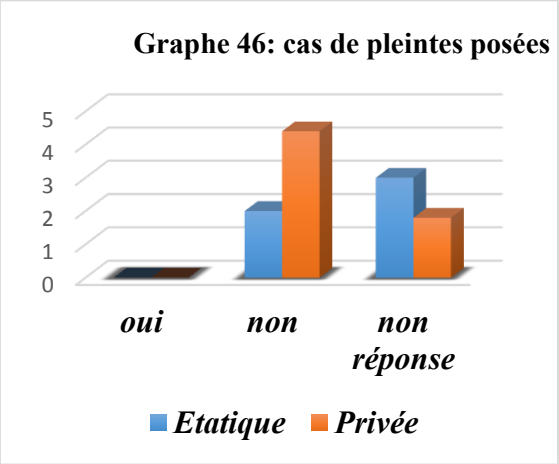


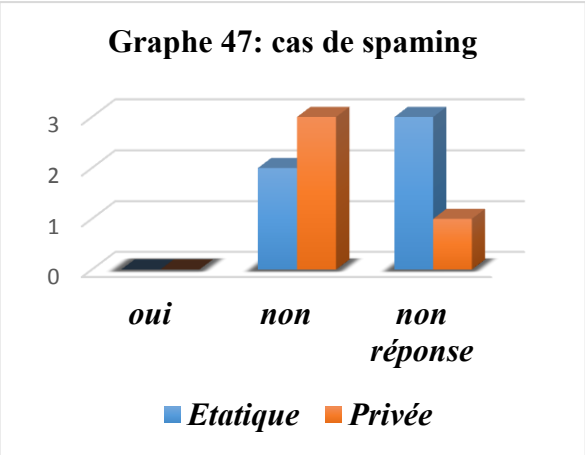
- **Source :** élaboré par nous même à partir des données collectées

- **Intrusion «spamming » ou infection par virus« Malware »**

L'ensemble des banques Etatiques et privées CPA, BDL,SG, GB BNPP n'ont pas étaient victime d'intrusion dites spamming ni leurs clients (*graphe n °46 et 47*). Au contraire des banques Etatiques, les banques privées détiennent un service qui permet aux particuliers de dénoncer des spam.la SG : service MESSAGI GB : application développées en interne, et la BNPP : l'agence et suivies centraux.

- **Nombres des plaintes reçues de la part de la clientèle ayant été victime de SPAM**



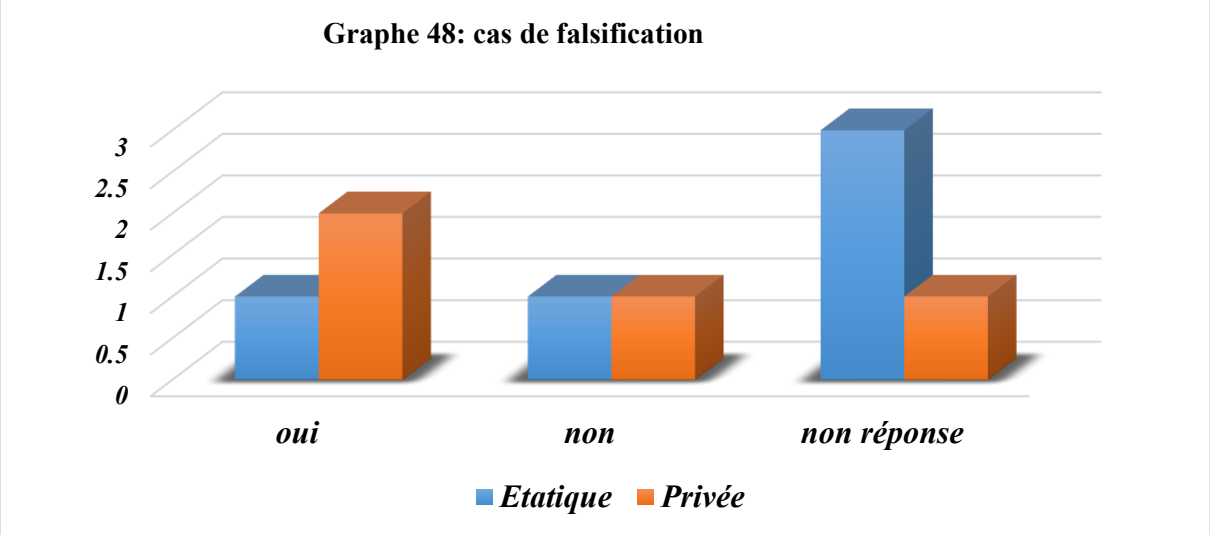


- **Source :** élaboré par nous même à partir des données collectées

- **Cas de falsification de chèques**

Sur l'échantillon interrogé, 3 banques ont répondu oui au cas de falsification de chèque.

SG : 2 cas /an ; BNPP : très faible ; CPA : =2%. (*Graphe n°48*).



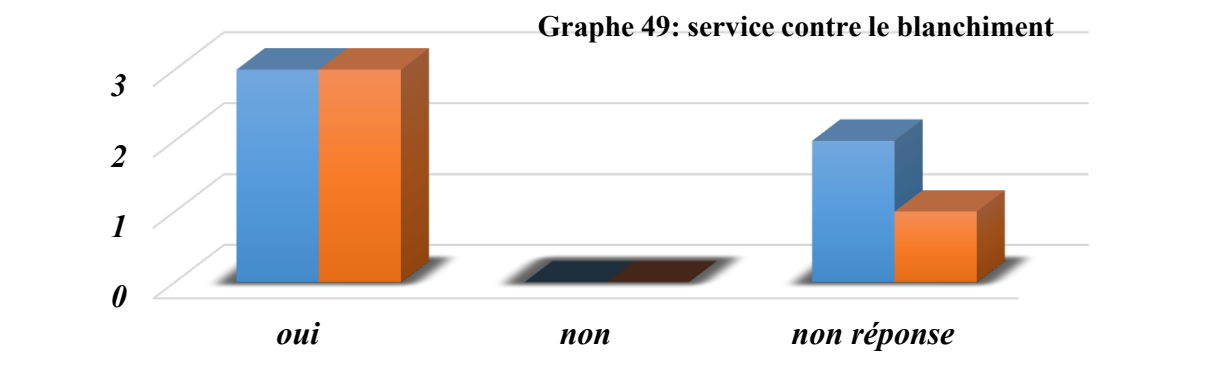
- **Source :** élaboré par nous même à partir des données collectées

- **Dispositif de lutter contre le blanchiment d'argent**

Sur les neufs banques interrogées, six banques ont répondu « OUI » à la disposition d'outils de lutte contre le blanchiment d'argent. Selon les réponses des banques les dispositifs sont :

- BDL : cellule anti blanchiment ;
- GB : logiciel de détection d'opérations suspectées et vigilance permanente ;

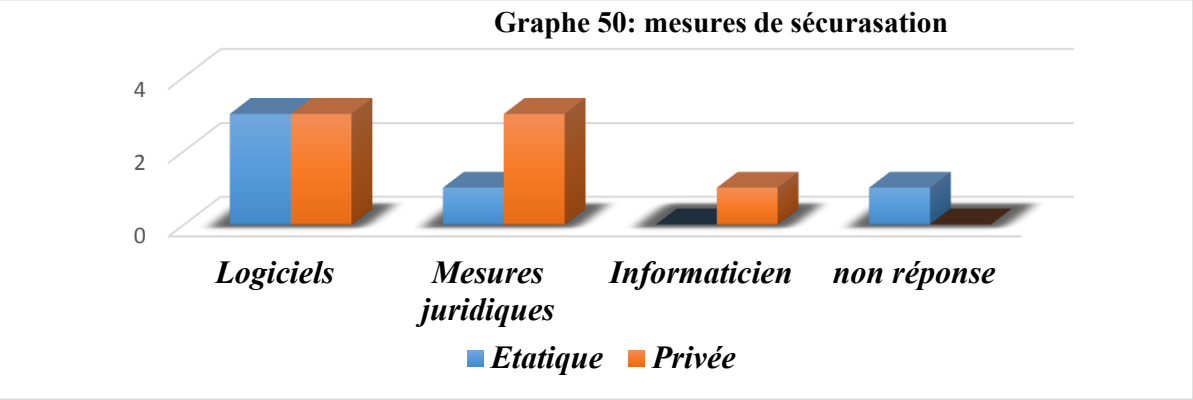
- SG : suivi au quotidien au niveau des points de ventes plus un système qui détecte les montants de versements dépassants les seuils autorisés.



Source : élaboré par nous même à partir des données collectée

- **Mesures de sécurisation des données et matériel**

Sur l'ensemble de 9 banques interrogées, les six banques (SG, GB, BNPN, CPA, BDL, BADR) disposent des outils pour protéger et sécuriser leurs données et matériels. (*Graphe n °50*)



Source : élaboré par nous même à partir des données collectées

III.2.Les résultats de l'entretien fait au niveau de la sureté de la wilaya de Tizi-Ouzou

La police judiciaire joue un rôle très important dans la lutte et la prévention contre les infractions liées aux TIC (la cybercriminalité). Dans ce principe chaque direction de sureté de wilaya possède une brigade de lutte contre la cybercriminalité relevant de la police judiciaire.

Au cours de notre entretien, le chef de la brigade nous a proclamé les informations suivantes :

- **Les affaires qu'ils traitent**
  - Piratage individuel ou professionnel ;
  - Atteinte au système d'information SI ;

- Escroquerie par internet ;
- Cyber terrorisme ;
- Atteintes aux personnes (diffamation ; diffusion de photos ;diffusion de l'ordre publique……..) ;
- Vente de marchandises prohibées.

- **Quelques statistiques**
  - En 2017: 47 affaires traitées au niveau de la wilaya ;
  - En 2018: 33 affaires traitées ;
  - La plus part des affaires non résolues sont sorties contre X ;
  - Le personnel qui active au sein de la brigade reçoit à chaque fois des formations de perfectionnement au niveau national (CERIST) et au niveau international ;
  - Le chef de la brigade nous a confirmé qu'ils n'ont pas reçues des peintes dans le secteur bancaire et financier car les banques qui activent sur la wilaya de Tizi-Ouzou sont reliées à leur direction générale. Ces dernières relèvent des fonctions de la brigade relevant de la police judiciaire de la direction générale de la sureté nationale.

Conclusion

La cybercriminalité dans les banques algériennes, et en Algérie en général n'est pas en extension vu le retard de l'introduction des technologies de l'information et du développement insuffisant de la monétique d'une part, et du manque de la culture d'utilisation des TIC chez la population d'une autre part, néanmoins le phénomène est brusque et couteux, il pourrait faire perdre aux banques des sommes gigantesques à travers le piratage, les fraudes liés aux cartes bancaires, aux distributeurs automatiques, au falsification de chèque, détournement et blanchiment d'argent.

Lors de notre enquête, le chef du service du commerce extérieur de la banque d'Algérie, nous a confirmé que le nombre de cyber menaces enregistrées dans le secteur bancaire et financier est vraiment faible vu le retard que connais notre pays en matière d'introduction des TIC dans les banques, de même pour la mentalité et la culture de la société algérienne.

Conclusion

En partant de l'idée qui détermine que l'introduction des nouvelles technologies dans le secteur bancaire, a un impact négatif sur l'activité bancaire bien connu sous le terme de « cybercriminalité » comprenant toute infraction liée aux fraudes et attaques informatiques.

A cette égard nous déduisons que l'Algérie est très loin d'être affectée par ce phénomène illicite, vu son retard dans l'introduction de ces nouvelles technologies dans son activité et cela s'explique par la diversification des mentalités des quotidiens et de civisme qui usent de se connecter au réseau informatique.

Notre enquête vise dans un premier lieu de délimiter l'usage des TIC dans les banques publiques et privées et leur impact négatif sur l'activité bancaire bien précisément celles de wilaya de Tizi-Ouzou, et dans un second lieu nous avons introduit le rôle de la brigade de la sureté de wilaya de Tizi-Ouzou qui est spécialisée dans la lutte contre la cybercriminalité.

À partir de notre enquête et les réponses obtenues nous avons conclu que toutes les banques enquêtées utilisent des TIC dans leurs activités. Par ailleurs, le degré d'utilisation des TIC au sein des banques privées est très élevé permettant ainsi de rendre le travail du personnel aisé, car elles investissent plus en matière d'introduction des nouvelles technologies par rapport au banques publiques , nous déduisons aussi que les banques qu'elles soient privées ou publiques ont sécurisées leur système d'information d'où aucune fraude bancaire n'a été détecté comme il nous a confirmé le chef de la brigade de sureté de wilaya et que les affaires traités n'ont aucune relation avec les banques sauf les atteintes aux personnes et l'escroquerie par internet (ex piratage de facebook)et vente de marchandises prohibées.

Enfin, la sécurité des systèmes informatiques permet de réduire les risques et d'assurer la pérennité des banques.

Les vagues d'innovations qui se sont succédé durant les dernières décennies dans le domaine des technologies de l'information et de la communication ont profondément modifié la nature des services bancaires et financiers.

Ces technologies, entendues comme un large ensemble regroupant 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 télécommunications ouverts, ont renouvelé la relation entre les banques et leurs clients ainsi que les prestations financières et les métiers bancaires. Elles ont créé des opportunités stratégiques et commerciales.[1]

Un des avantages les plus évidents de l'Internet par exemple réside dans la réduction substantielle des coûts d'infrastructures et de transaction. De même, l'offre bancaire en ligne peut être adaptée au profil de la clientèle et à ses attentes. Elle permet d'atteindre de nouveaux segments de clientèle, en particulier dans les activités de courtage.

Cette nouvelle donne génère également des risques nouveaux qui doivent être soigneusement considérés. La question relève tout d'abord d'une réflexion d'ensemble sur la stabilité financière[2]. Il faut notamment garder à l'esprit que la banque électronique transcende les frontières géographiques ou sectorielles d'où elle semble également privilégiée par les cybercriminels.

La notion de cybercriminalité constitue l'une des formes de criminalité transnationale qui connaît le développement le plus rapide dans les pays du monde entier. La croissance rapide d'Internet et de l'informatique s'est accompagnée d'un développement économique et social, mais la dépendance accrue à Internet a aussi multiplié les risques et les vulnérabilités et a ouvert de nouvelles possibilités d'activités criminelles[3]. L'amplification de l'ensemble de ces risques (risques stratégiques, risques financiers, risques opérationnels…….), met les banques et les établissements financiers devant un risque probablement systémique.

La cybercriminalité est un phénomène qui s'affranchit des frontières. En conséquence, les services chargés de l'application de la loi doivent surmonter les défis des enquêtes transfrontalières, les différences entre les systèmes juridiques et la disparité des capacités[4].

[1] Danielle MONSIMIER, « *banques et nouvelles technologies* », revue horizon bancaire, N° 316, 02/2003
[2] Danielle MONSIMIER, *O*p.cit , P2.
[3] Secrétariat général d'INTERPOL - 200, quai Charles de Gaulle - 69006 Lyon - France - www.interpol.int
[4] www.interpol.int consulté le 05/09/2018.

Dans le cadre de notre travail de recherche, nous avons entamé une étude sur les TIC et les infractions liées à leurs utilisations au niveau d'un certain nombre de banques de la Willaya de Tizi-Ouzou (ville). De ce fait, pour répondre aux objectifs que nous sommes tracés, il a fallu suivre une démarche méthodologique. A ce titre, nous avons opté pour une enquête par questionnaire réalisée auprès d'un échantillon de banques. Cela, nous a permis malgré les difficultés rencontrées citées auparavant, de dégager les résultats suivants :

- Malgré les efforts fulgurants des autorités algériennes pour innover d'avantage dans le domaine des TIC, l'introduction de ces dernières au niveau des banques interrogées, qu'elles soient publiques ou privés, est très moyenne. En établissant un état des lieux et comparativement avec ce qui a été affirmé dans le premier chapitre, nous avons constaté que les TIC ne sont diffusées que d'une manière relativement moyenne dans les structures des banques, mais les dirigeants sont conscients du retard ;
- Internet n'est pas vraiment utilisé au maximum. Les banques n'exploitent pas encore ce canal et ne proposent que des services très limités. Ce canal tant important n'est pas pris dans le cadre des stratégies des banques. Celles ayant répondu semblent être de simples utilisatrices de ce canal alors qu'elles peuvent en être de véritables actrices.

Dans ce contexte, l'Algérie a multiplié ces dernieres années les initiatives tendant à favoriser l'accès aux technologies en tant qu'outils modernes de communication et d'échanges. Mais si l'usage de l'Internet comme technologie de l'information et de la communication se généralise de plus en plus en Algérie, son implication dans le développement économique reste très limitée. Ceci est sans doute dû, en grande partie à l'absence d'une politique de formation et de recherche sur les moyens et les méthodes à adopter pour l'intégration de cette technologie dans les différents secteurs de l'activité économique.

- Les moyens de paiement sont en phase de développement encore, donc en retard. Sur ce niveau, les banques interrogées semblent avoir recours d'une manière massive aux supports de papier bien que les technologies informatiques et télé communicationnelles permettent cette automatisation.
- Une utilisation du potentiel informatique limitée dans les banques questionnées. En étudiant le volet « informatique » des TIC au niveau de l'échantillon, nous avons pu spécifier la sous- utilisation des moyens informatiques et leur manque au niveau des agences, la faible exploitation du logiciel bancaire utilisé et surtout le manque flagrant d'informaticiens.
- Le secteur privé est en avance par rapport au secteur public en matière d'introduction et d'utilisation des TIC mais cela, ne nous permet pas de dire que ce secteur est exposé au

risque de cybercriminalité car les deux secteurs sont sous contrôle de la banque centrale d'Algérie.

- L'infiltration du phénomène de cybercriminalité dans les banques de notre échantillon est faible vu le retard de l'introduction des technologies de l'information et du développement insuffisant de la monétique, mais un Système d'alerte en cas d'effraction ou de menace à caractère numérique est mis en place, et la sécurisation des réseaux est prise en charge. La SATIM en plus de son rôle principal dans l'automatisation des transactions interbancaires et de la monétique, veille à la sécurité des moyens de paiements.
- La cybercriminalité n'est pas en expansion en Algérie vu le retard dont est victime en matière des TIC, cela n'empêche les autorités de penser à la prévention en allouant les dispositifs nécessaires au cyber sécurité par :
  - La création d'un office national de lutte contre les infractions liées aux TIC ;
  - Un cadre juridique par la loi 09-04 du 14 Chaàbane correspondant au05/08/2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication, et l'article du CPA (Code Pénal Algérien), « article 95 Bis07, atteintes liées au STAD » ;
  - Création de brigades de lutte contre la cybercriminalité dans les organismes de sûreté et gendarmerie nationale;
  - Le rôle des institutions réglementées :
    - ARPT (Autorité de régulation de la poste et des télécommunications), TDA (télé et diffusion algérienne) : radio et diffusion numérique ;
    - ARPT : accès aux réseaux large bande ;
    - CERIST (Centre de recherche et d'information scientifique) : fournisseur d'accès aux services Internet ou ISP, contenu numérique en arabe ;
    - MPTIC (ministère de la poste et des technologies de l'information et de la communication) : logiciel à code service ouvert, et le cyber sécurité.

Bibliographie

Ouvrages

1. AZZOUZI Ali, « La cybercriminalité au Maroc », édition Ali El Azzouzi, 2010, Casablanca- Maroc.
2. BARNES, S, J and Corbitt,B(2003), « mobile banking, concept and potential »internationnal journal of mobile communication ,vol.1N°3.
3. CARBONNER (J), « sociologie juridique », éd A Colin(1992), ed.PUF, collthemis, Paris, 1978 refondue coll. Quadrige, 1994 et 2004.
4. CHAPIRON, B « évaluation du système d'information pour optimisation des forces de vente », mars 2009.
5. DOMINIQUE Rambure « les systèmes de paiement », éd ECONOMICA. Paris, 2005.
6. D-PLIHON « la monnaie et ses mécanismes », édition la découverte Paris, 2000,2001.
7. DUFLOT. F« les infections Informatiques Bénéfiques », Juriscom, 2004, Paris, France.
8. Emily FLITTEER, «hackers switch to new digital currency after Liberty Reserve», Reuters, 9 août 2013.
9. FILIOL. F« Les virus informatique : théorie, pratique et applications », Ed. Springer, 2004.
10. Frédéric VISNOVSK, « les attentes de l'ACPR sur le risque informatique », « Cyber-sécurité &fraude : un risque majeur pour l'industrie financière »,Paris, le Février 2018.
11. Frédéric VISNOVSKY, « Quel rôle pour les superviseurs bancaires face à la cyber criminalité », Paris, 27mars 2015.
12. GASSIN(R) , « le droit pénal de l'informatique »,D S ,1986,Charon
13. GEMIGNANI, "Computer Crime: The Law in '80, Indiana Law Review", Vol. 13, 1980.
14. GOUVAERE Virginie (2002), « l'évolution de travail avec les NTIC », institut national, de recherche et de sécurité, Lorraine.
15. GUELEC. Det RALLE P(2003), « les nouvelles théories de croissance »,5eme édition, la découverte, Paris.
16. Jean-Luc SARRAZIN : BTS banque « techniques bancaire des marchés des particuliers », 3^{e} édition, Canada (Québec), 2013.
17. LIPSEY R.G.C bekar et K carlo (1998A), « what requiries explantation ?in help men », general perpuse technologies and economic grouth,1998.
18. M. CHAWKI, Essai sur la notion de cybercriminalité, IEHEI, 2006.
19. Nathalie COUTINET « définir les tic pour mieux comprendre l'économie », éd HAL (archives-ouvertes) Paris, décembre 2007.
20. PASCAL Thoniel « usage de l'authentification dans le domaine bancaire » édition technique de l'ingénieur, Paris, 2010.
21. ROWE. F, "Des banques et des réseaux : productivité et avantages concurrentiels", Ed Economica, 1994, Paris.
22. Solange GHERNAOUTI-HELIE « La cybercriminalité : Le visible et l'invisible », collection le savoir suisse, Edition 2009.
23. WATIN AUGOUAR (M), préface du livre « cybercriminalité défi mondial »VII.
24. Y.COLVERT, dictionnaire des banques et assurances, Paris 1988.

Revues, Articles, rapports et Documents divers

1. **A**.LUCAS : le droit de l'informatique, (paris, puf)1987 n°413.
2. article rédigé par Mounira Amine Seka, le quotidien Soir d'Algérie, 2017.
3. Article sur les enjeux de la cybercriminalité, paru en juillet 2009.ELAZZOUZI Ali.
4. BlackMarket ou Darknet : Les DarkNets sont distincts des autres réseaux car le partage y est anonyme (c'est-à-dire que les adresses IP ne sont pas partagées publiquement).
5. Bulletin 32 cyber,pdf www,crtf.dz.
6. Commission Européenne –affaire intérieures-la cybercriminalité-avril 2012.
7. D.WALL : crime and the internet (N, Routledge) 2001.
8. Directive 2013/36/UE du Parlement européen et du Conseil européen du 26 juin 2013 concernant l'accès à l'activité et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, dite en anglais « CRD IV ».
9. Edouard FERNANDEZ BOLLO-, Autorité de contrôle prudentiel et de résolution (ACPR). pdf.
10. ENFRERLIN Clément, un focus sur la cybercriminalité, 2011.
11. FIA-NET « La fraude à la carte bancaire : le livre blanc 2008 »
12. François PAGET « Fraude financière et opérations bancaires en ligne : menaces et contre-mesures
13. Groupe de travail sur les « monnaies virtuelles », du Ministère des finances et des comptes publics, juin 2014.
14. KASPERSKY Eugene, « cybercriminalité, une guerre perdue ?documentation française, article n°6 sécurité global, défis de la cybercriminalité, hiver 2008-2009, France.
15. Lamri DOUDI, département d'informatique, université de Sétif « place de l'Algérie dans le monde des TIC ».4 novembre 2017.
16. LEVY ,Haking, offences, australien institute of criminology, 2005.McAfee® Avert® Labs.
17. Nadia Chettab, « Economie, TIC et bonne gouvernance en Algérie », papier imprimé, université, Badj Mokhtar Annaba,.
18. Office québecois.de la langue française, le grand dictionnaire terminologique. Québec retrieved marche 10/2009.
19. Patrick BISCIARI, Nouvelle Economie, workingpapers. document séries, PDF.
20. Rapport de l'ONDRP, 2011.
21. Rapport de l'UIT (2015-2016-2017) « mesurer la société de l'information »
22. Rapport de l'UIT, « Guide sur la cyber-sécurité pour les pays en développement
23. Rapport de l'UIT, « comprendre la cybercriminalité guide pour les PED », 2009.
24. Rapport de l'UIT. rapport sur le développement des télécommunications /TIC dans le monde, 2006.
25. Rapport de la CNUCED, 2014
26. Rapport du CSIS (center for strategic and international studies) sponsoriées par Mcafee.
27. Rapport IUT global cybersécurité Agenda /high –level expert group, global strategic. report,2008.
28. Revue banque, « les banques face au défis de la cybercriminalité, article rédigé par CHRISTINE LEJOUX 20/04/2016.
29. Revue de « Banque de France », Focus- les dangers liés au développement des monnaies virtuelles : l'exemple du « bitcoin », n° 10-5 décembre 2013.
30. SIEBER,Councit of Europe organised crime,report 2004.

Thèses et mémoires

1. Abdelkader RACHEDI (2003) « TIC structure et comportement de l'homme dans l'entreprise, thèse de doctorat : univ de Abou Baker BELAID, Tlemcen.
2. BELATTAF Sylia, « la cybercriminalité : l'Algérie est elle suffisamment outillée ?le cas des banques +algériennes. » mémoire de master –univ Abderrahmane Mira de Bejaia 2014-2015.
3. BOOS Romain « lutte contre la cybercriminalité au regard de l'action de l'Etat » thèse de doctorat .univ de Lorraine, 2016.
4. BOUCHENOUA Karima, BELAIDENE LYDIA « impact des TIC sur la performance bancaire cas des banques de la ville de : univ Abderrahmane Mira, 2015/2016.
5. BOULENOUAR Nassima Ouarda « les nouveaux supports de communication TIC : Facteurs de différentiation dans l'activité bancaire », mémoire de magister, univ d'Oran ,2014.
6. 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.
7. LEBERT M.F « de l'imprimerie à l'internet » thèse paris,ed 00h00 (1999).

Webographie

1. http:// www.ssri.dz la-cyber-sécurité-état-des-lieux-en-Algérie/; 2014.
2. http://www.banque-info.com/lexique-bancaire/d/distributeur-automatique-de-billets--dab
3. http://www.itpro.fr/a/cheques-electroniques/
4. http://www.cairn.info/zen.php?ID_ARTICLE=EMR_129_0110 >
5. http://blog.wikimemoires.com/2011/04/definition-du-paiement-electronique-e-paiement/
6. http://experts-univers.com/inconvenients-avantages-des-ntic.html
7. www.definitiondelacybercriminalité.com
8. http://www.zdnet.fr/actualites/le-groupe-petrolier-aramco-cible-d-unecyberattaque-l-acte-d-activistes-39775459.htm
9. http://www.lenetexpert.fr/lufthansa-victime-dune-cyberattaque-le-net-expert-informatique/
10. http://www.lenetexpert.fr/la-chaine-tv5-monde-victime-dun-piratage-de-grande-ampleur-par desindividus-se-reclamant-du-groupe-etat-islamique-le-net-expert-informatique
11. http://collection.nlc-bnc.ca/
12. http://www.justice.gov/>.
13. https://www.google.fr/#q=new+hacker%27s+dictionary+pdf
14. https://www.securiteinfo.com/attaques/hacking/dos.shtml
15. .https://www.mag-securs.com/communiques/id/33116/la-cybercriminalite-coute-tres-cher-a-l-economie-mondiale.aspx
16. https://www.clusif.asso.fr
17. **https://www.pcsansvirus.com/pages/emsisoft-anti-malware/attention-aux-phishing-dis-hameconnage-et-vos-donnees-personnelles.html.**
18. http://static.fianet.com/__docs/livre_blanc_juin-2008.pdf
19. http://www.reuters.com/article/2013/08/09/net-us-cybercrime-digital-currency-idUSBRE9780GM2013080.

20. http://www.canafe-fintrac.gc.ca/intro-fra.asp

21. http://www.isiq.ca/entreprise/publications/articles/articles_pdf/zerospam_fiche-dessous_hameconnage.08.pdf

22. http://blogs.orangebusiness.com/securite/
23. http://www.olf.gouv.qc.ca/
24. http://fr.wikipedia.org/wiki/Intégrité_des_données
25. www.mitre.org/publication/all/ten-strategie-off-a-world-class-cybersécurité-operation-center;
26. https://www.algerie24.dz
27. www.mptic.dz
28. www.SATIM.dz
29. http://www.radioalgerie.dz/news/fr/article/20180221/134543.html
30. : https://www.alg24.net/cyberattaques-lalgerie-parmi-pays-plus-touches/
31. www.cerist.dz
32. http://reporters.dz/index.php/rss-a-la-une/item/54151-organe-national-de-prevention-et-de-lutte-contre-les-infractions-liees-aux-tic-un-decret-nomme-les-representants-de-la-presidence-et-de-la-defense.
33. http://www.nticweb.com/it/8398-un-organe-national-de-pr%C3%A9vention-et-de-lutte-contre-les-infractions-li%C3%A9es-aux-tic-mis-en-place.html.
34. http:/manifest.univ-ouargla.dz
35. www.latribune.fr
36. www.sgg.dz.

Résumé

À l'arrivée des nouvelles technologies de l'information et de communication (NTIC), ont imposées un nouvel espace d'échange où circulent des flux d'informations numériques, avec le libre accès, dont lequel s'effectuent tous types de transactions et prestations électroniques.

L'utilisation massive de ces NTIC a donné lieu à l'apparition des criminalités informatiques ce qu'on appelle la cybercriminalité. Elle désigne toutes formes d'attaques réalisée au moyen de réseau informatique ou de système d'information, la menace que fait peser la cybercriminalité suscite une attention élevée de toutes les entreprises et institutions financières.

Quelle serai les dispositifs mise en place pour sécuriser leur système d'informations ?

Quel est la réaction des banques face à ce phénomène ? Et qu'en est-il de cas des banques Algériennes ?

Mots clés: NTIC, espace d'échange d'informations, criminalités informatiques, cybercriminalité, système d'information, institutions financières, banques.

Summary

With the advent of the new information and communication technologies (NICTs), a new exchange area has been created where digital information flows circulate, with free access, of which all types of transactions are carried out; electronic services.

The massive use of these NICTs has given rise to the emergence of computer crimes called cybercrime. It refers to all forms of attacks carried out via computer network or information system, the threat posed by cybercrime is attracting high attention from all companies and financial institutions.

What will be the devices set up to secure their information system?

What is the reaction of banks to this phenomenon? And what about the case of Algerian banks?

Key words: NICT, information exchange, computer crime, cybercrime, information system, financial institutions, banks.

ANNEXE N° 1 : autres définitions des TIC

Le **tableau n°1, 2,** résume les différentes définitions et inscriptions des TIC selon différentes parties : Etats-Unis, Union européenne et France, Selon ONU et OCDE ainsi que certains auteurs :

Tableau n°1 : **Définition des TIC selon Etats-Unis, Union Européenne et la France……**

Pays	**Définitions**
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 informatique 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 des services associés aux ordinateurs ; les industries d'équipements de communication et des services recensant les offreurs qui fournissent des infrastructures matérielles et immatérielles permettant la connexion entre ordinateurs et serveurs.
Union européenne et France (1998)	Le secteur TIC apparait sous la forme d'une liste d'activité 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.
Selon **ONU** et **OCDE** (1998)	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.

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

Tableau n° : 2

Casino, G (Septembre **1999**). NTIC : de quoi parlet-on ? Etude TICO : Technologie de l'information et de la communication dans les organisations.	En résumé, nous dirons donc des NTIC qu'elles sont des technologies de traitement des processus intellectuels faisant appel à l'unification de différentes technologies basées sur l'électronique disponibles et accessibles via des infrastructures de réseau, soit au plan local (entreprise) soit au plan mondial.

Source : www.anact.fr, publié le 10 Février 2006. Edition ANACT : Agence Nationale pour l'Amélioration des Conditions de Travail.

ANNEXE N°2

Les onze indicateurs associés à l'IDI relatifs à l'accès aux TIC :

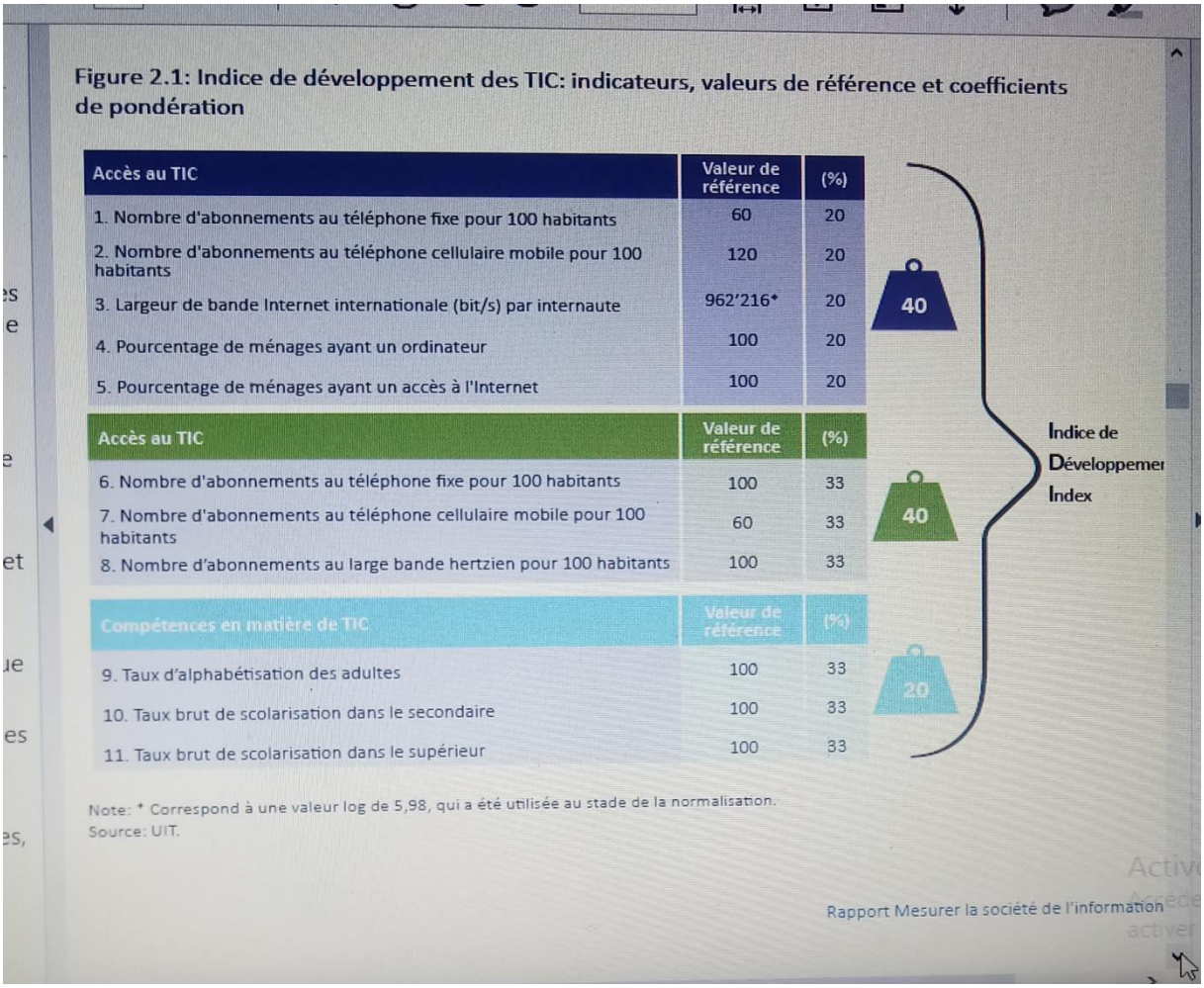


Figure 2.1: Indice de développement des TIC: indicateurs, valeurs de référence et coefficients de pondération

Accès au TIC	Valeur de référence	(%)
1. Nombre d'abonnements au téléphone fixe pour 100 habitants	60	20
2. Nombre d'abonnements au téléphone cellulaire mobile pour 100 habitants	120	20
3. Largeur de bande Internet internationale (bit/s) par internaute	962'216*	20
4. Pourcentage de ménages ayant un ordinateur	100	20
5. Pourcentage de ménages ayant un accès à l'Internet	100	20
Accès au TIC	**Valeur de référence**	**(%)**
6. Nombre d'abonnements au téléphone fixe pour 100 habitants	100	33
7. Nombre d'abonnements au téléphone cellulaire mobile pour 100 habitants	60	33
8. Nombre d'abonnements au large bande hertzien pour 100 habitants	100	33
Compétences en matière de TIC	**Valeur de référence**	**(%)**
9. Taux d'alphabétisation des adultes	100	33
10. Taux brut de scolarisation dans le secondaire	100	33
11. Taux brut de scolarisation dans le supérieur	100	33

40

40

20

Indice de Développemer Index

Note: * Correspond à une valeur log de 5,98, qui a été utilisée au stade de la normalisation.
Source: UIT.

Rapport Mesurer la société de l'information

ANNEXE N° 3

Tableau n° 3 : les prestations de service bancaire 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)	-Information sur les produits bancaires -Cours des devises -Cotations boursières	- Internet -Téléphone
Accès aux informations individualisées	-Relevé de compte, encours carte bancaire -Consultations des comptes	-GAB/DAB -Internet
Simulation	-Simulation de prêt -Simulation de portefeuille titre -Suivi de budget personnel	-Internet -PC+logiciel money
Action sur le processus transactionnel		
Opérations de base	-Virement bancaire -Remise de chèque	-GAB/DAB -Internet -Automate vocal
Opérations évoluées	-Ordre d'achat ou de vente de titres -Octroi d'un prêt	-Internet -Service bancaires téléphoniques
Communication interpersonnelle à distance		
Communication en temps réel	-Opposition carte bancaire -Situation d'urgence à l'étranger	-Centre d'appel téléphonique
Communication en temps différé	-Réclamation	-Internet (messagerie électronique) -Téléphone

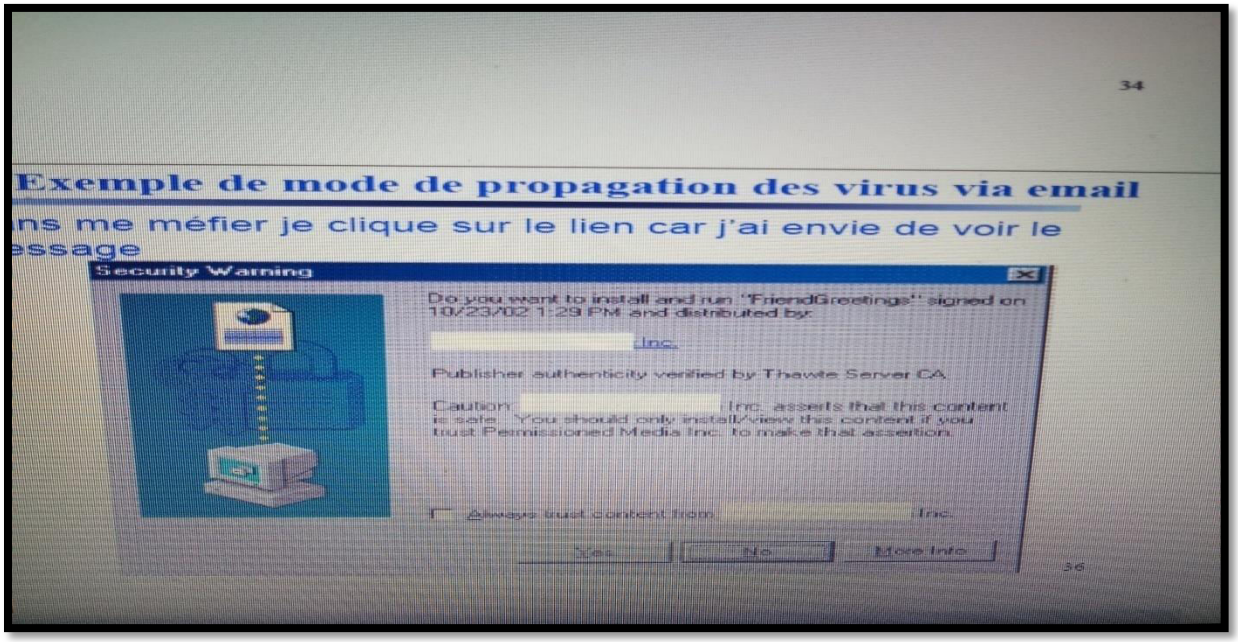
Source : Horizon bancaire, « l'accès directe au système d'information par le client final via les medias électroniques », Sylvie GERBAIX.

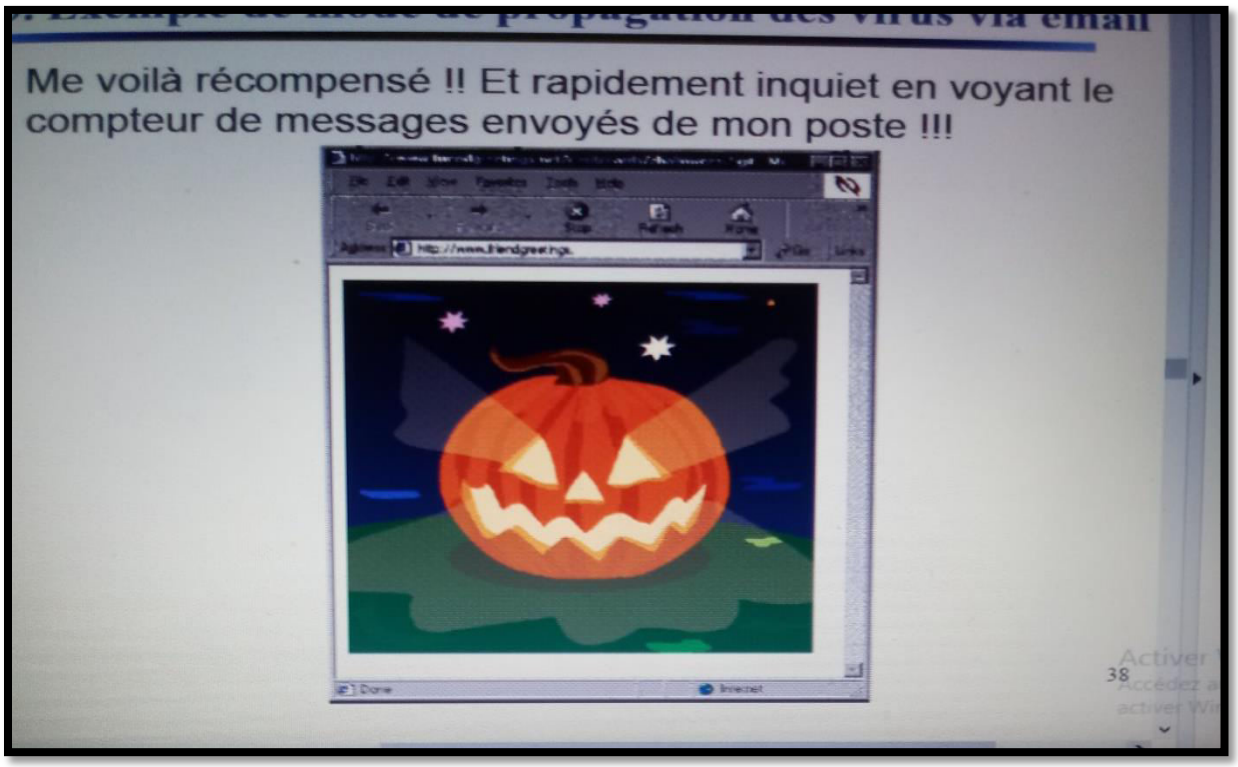
ANNEXE N° 4

Les principales techniques du piratage bancaire.

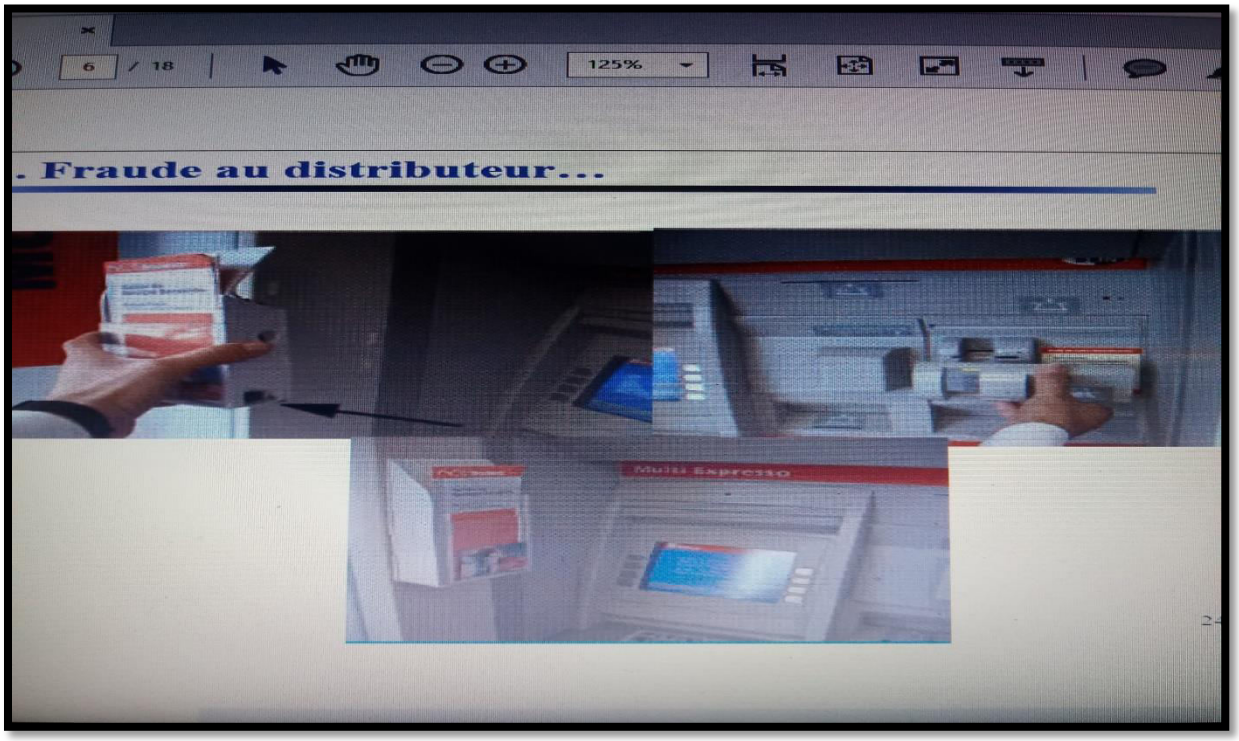
Source : https://www.clusif.asso.fr

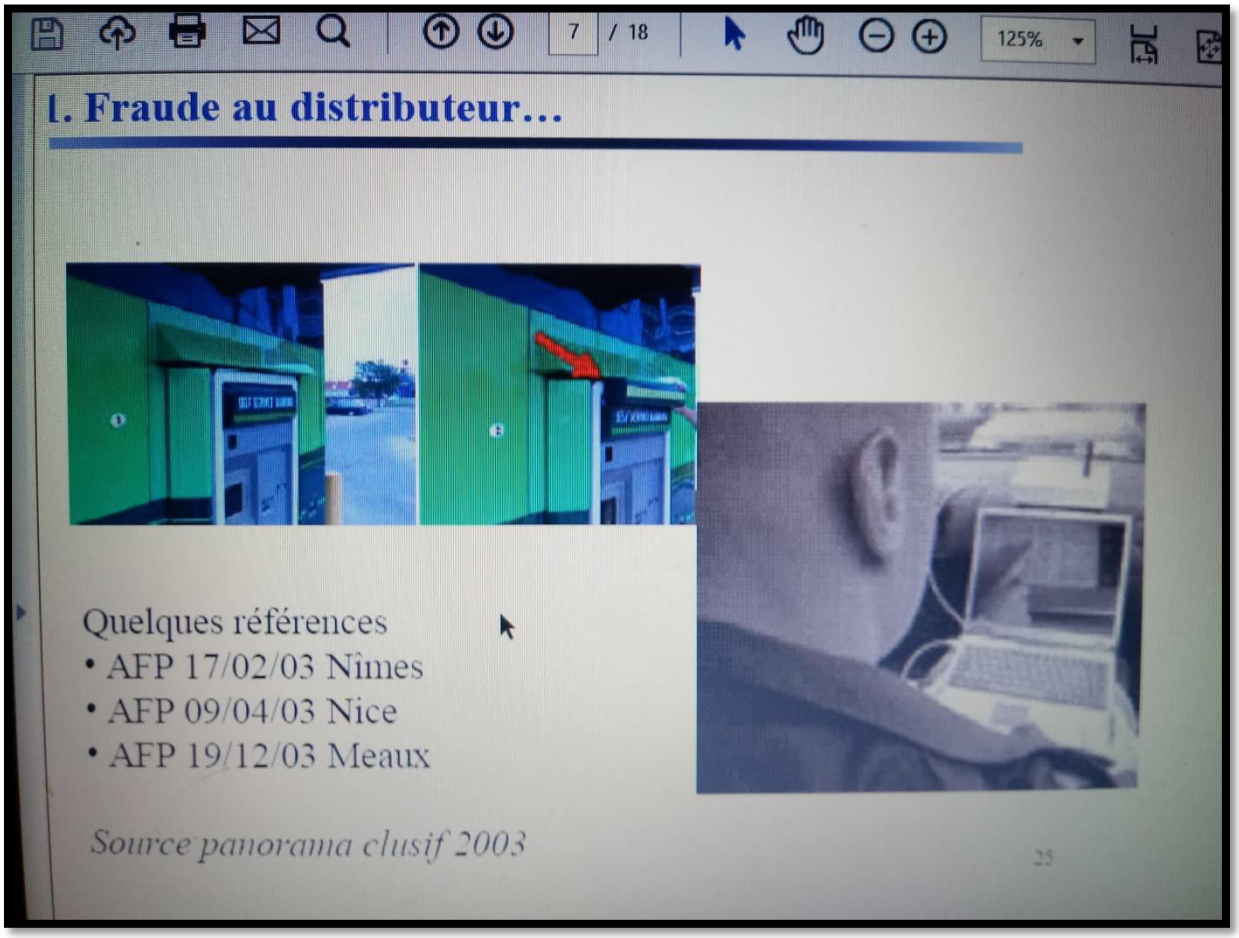
ANNEX N°5 : phishing par e-mail



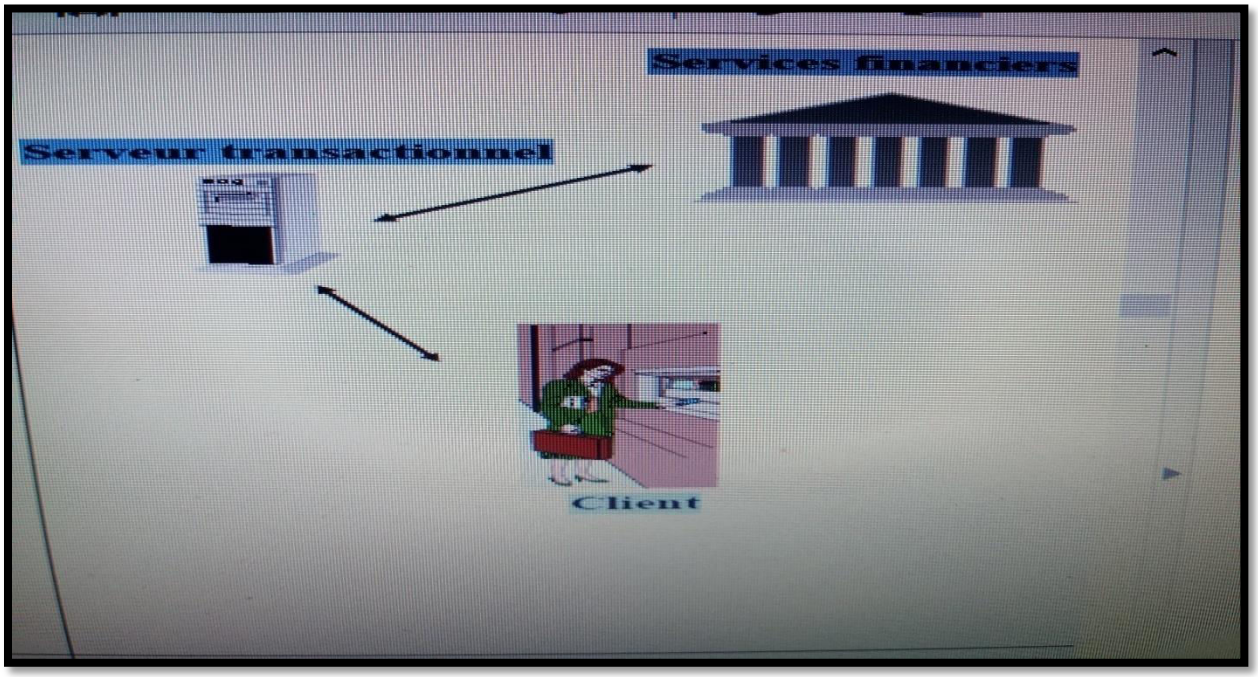


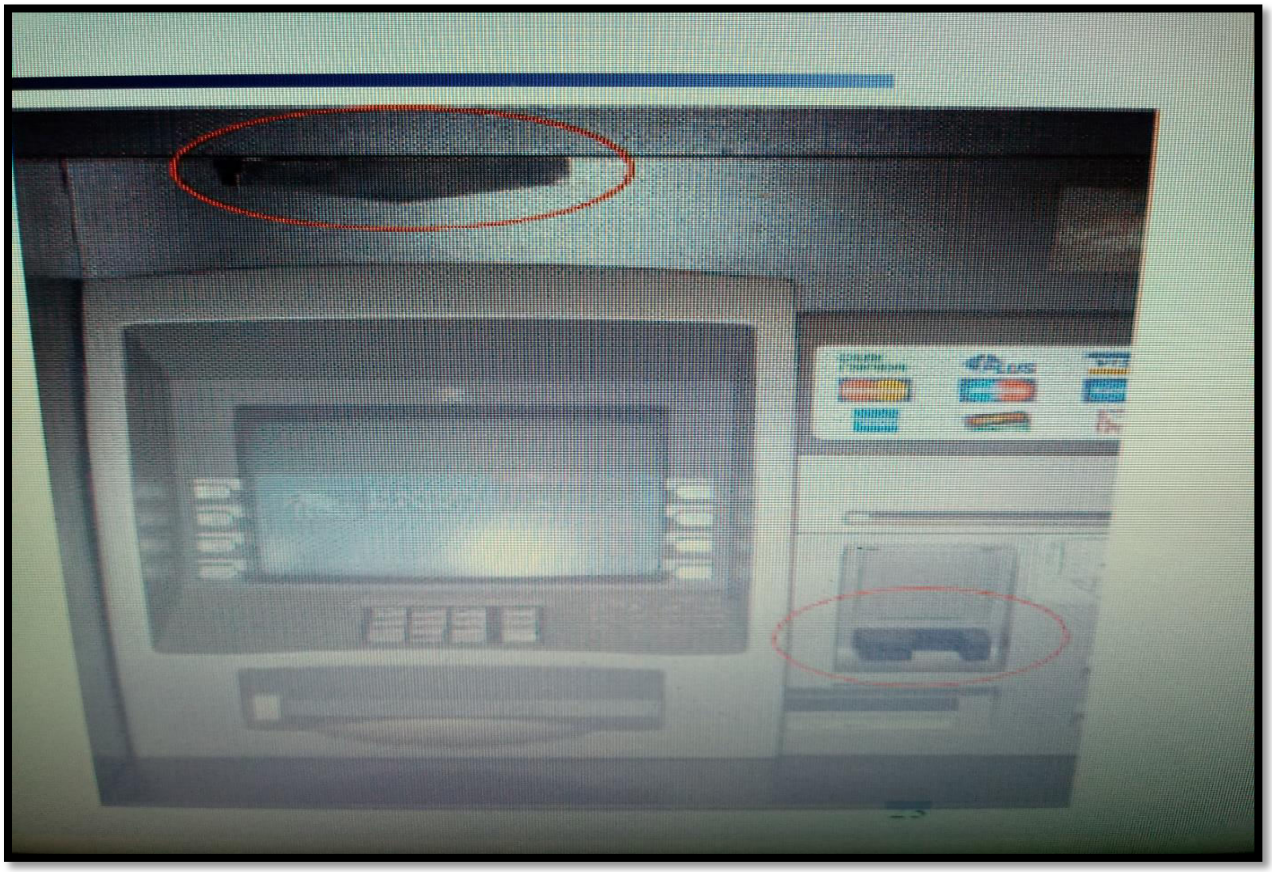
ANNEXE N° 6 : la fraude aux distributeurs



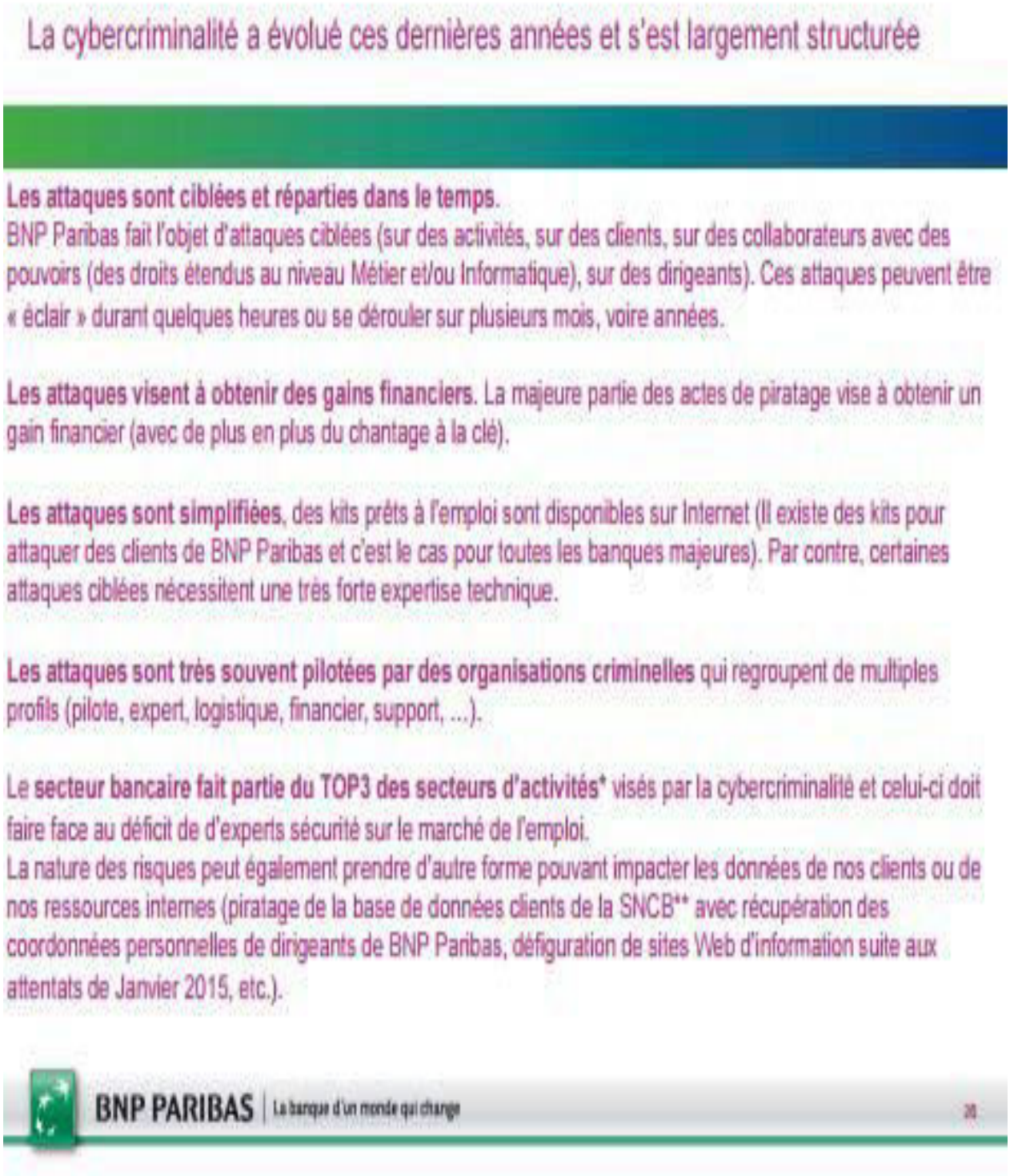


ANNEXE N° 7 : la fraude à la carte bancaire





ANNEXE N° 8 : La structure de la cybercriminalité selon le BNP PARIBAS



ANNEXE N° 09 : activités de veille de la banque

Encadré 1

Équipes de détection et équipes de réaction

Face à la cyber-menace, la détection des attaques et la capacité à réagir rapidement sont essentielles. Ces actions de sécurité informatique se sont progressivement structurées depuis la naissance d'Internet et l'apparition des premiers « virus » informatiques au début des années 1990. Aujourd'hui, les administrations et les grandes entreprises du monde entier s'organisent en interne et conjuguent aussi leurs efforts en partageant de l'information sur les nouvelles menaces identifiées. Les principaux établissements du secteur financier en France participent à ces réseaux d'échanges et disposent d'équipes capables d'intervenir. Ce type d'activité est également réalisé par des prestataires spécialisés. Il existe deux types d'équipes :

– les centres opérationnels de sécurité (COS) (*security operating centers* – SOC) sont chargés de la veille sécuritaire sur les platesformes logicielles et matérielles. Ils ont la responsabilité de la détection des attaques et de toute anomalie pouvant conduire à reconnaître une action malveillante sur le système d'information. Pour une meilleure efficacité, ils comportent parfois en leur sein une équipe chargée de tester la sécurité (équipe dite d'« attaque ») et une équipe chargée de détecter au plus tôt les attaques (équipe dite de « défense »). Leur rôle est désormais crucial pour permettre une intervention rapide et contrer les attaques ;

– les équipes de réponse aux incidents de sécurité informatique, plus connues sous leur acronyme anglais CSIRT (*computer security incident response teams*), sont, quant à elles, chargées d'intervenir en cas d'incident. Les CSIRT exploitent donc les alertes produites par les COS, ainsi que d'autres alertes reçues par d'autres canaux pouvant signaler des anomalies. Ils peuvent se faire reconnaître par des réseaux internationaux comme le FIRST (Forum for Incident Response and Security Teams), le CERT (Computer Emergency Response Teams) ou le TF-CSIRT en Europe, afin de développer les capacités d'échange d'informations. Le CSIRT a la charge de l'analyse des alertes et la mise en oeuvre d'une réponse appropriée. Au niveau national, l'ANSSI pilote le CERT-FR qui opère pour les administrations françaises et accompagne l'action du CERT des grandes entreprises (cf. encadré 2 ci-contre).

ANNEXE N° 10

Encadré 2

Loi de programmation militaire et rôle de l'ANSSI

En France, la loi de programmation militaire du 18 décembre 2013 reprend les orientations du *Livre blanc sur la défense et la sécurité nationale* parues la même année. Afin de prendre en compte les risques pour la nation des cyber-attaques, elle détaille les dispositions relatives à la protection des infrastructures vitales contre la cyber-menace. Cette loi s'applique aux « opérateurs d'importance vitale » (OIV), qu'ils soient privés ou publics, et qui sont désignés pour chaque secteur d'activité d'importance vitale (SIV) par arrêté du ministre coordonnateur (ministre de l'Économie et des Finances pour le secteur financier). Elle oblige notamment les OIV à mettre en œuvre des mesures de sécurité, à déclarer immédiatement tout incident affectant le système d'information et à se soumettre à des audits de leurs systèmes à la demande du Premier ministre (pas de périodicité explicitement imposée) par l'ANSSI ou autre service de l'État.

L'autorité nationale chargée de la défense des systèmes d'information est l'ANSSI, qui est placée sous l'autorité du Premier ministre. Ses missions ont été détaillées dans un décret du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale (décret n° 2015-351). Ce décret inclut notamment des précisions sur les règles de sécurité à appliquer, les modalités de mise en place de systèmes de détection des attaques au sein des OIV, la collecte des incidents de cybercriminalité et enfin les modalités de contrôle de la bonne application de ces règles. Elle prépare la stratégie nationale pour la sécurité numérique, mise à jour en octobre 2015.

ANNEXE N° 11 : PRESENTATION DE LA SATIM

SATIM, Société d'Automatisation des Transactions Interbancaires et de Monétique, est :

- Une filiale de 08 Banques Algériennes : (BADR, BDL, BEA, BNA, CPA, CNEP, CNMA, ALBARAKA), créée en 1995 à l'initiative de la communauté bancaire.
- L'opérateur monétique interbancaire en Algérie, pour les cartes domestiques et dans un futur proche, internationales.
- L'un des instruments techniques d'accompagnement du programme de développement et de modernisation des banques et particulièrement de promotion des moyens de paiement par carte.
- SATIM réuni 17 adhérents dans son réseau monétique interbancaire : 16 Banques dont 07 banques publiques et 09 banques privées ainsi que Algérie Poste.

LES MISSIONS DE LA SATIM

LES principales missions de SATIM sont :

- Œuvre au développement et à l'utilisation des moyens de paiement électronique.
- Met en place et gère la plate-forme technique et organisationnelle assurant une interopérabilité totale entre tous les acteurs du Réseau Monétique en Algérie.
- Participe à la mise en place des règles interbancaires de gestion des produits monétiques interbancaires en étant une force de proposition.
- Accompagne la banque dans la mise en place et le développement des produits monétiques.
- Personnalise les chèques et les cartes de paiement et de retrait d'espèces.
- Met en œuvre l'ensemble des actions qui régissent le fonctionnement du système monétique dans ses diverses composantes :
    - maîtrise des technologies,
    - automatisation des procédures,
    - rapidité des transactions,
    - économies des flux financiers, etc...

ACTIVITES DE LA SATIM

Les activités de la Société d'Automatisation des Transactions Interbancaires et de Monétique SATIM se situent essentiellement sur trois (03) axes :

Chèque : Depuis sa création, SATIM assure la prestation de personnalisation pour la majorité des établissements bancaires.

Le retrait par carte interbancaire CIB :(voir annexe) : En 1997, SATIM a lancé le retrait d'espèces à partir des DAB (Distributeurs Automatiques de Billets de banque) en mettant en place le Réseau Monétique Interbancaire (RMI).

Dans ce cadre, SATIM assure les fonctions de connexion et de gestion des DAB/GAB, la personnalisation des cartes de retrait interbancaires « pour les banques", la mise en place des switch pour les membres ayant leur propres système d'autorisation.

Plusieurs banques participent au Réseau Monétique Interbancaire de retrait d'espèces dont sept banques actionnaires de la SATIM (BNA, BDL, CPA, BADR, BEA, CNEP-Banque, CNMA) ainsi que d'autres institutions, on citera entre autre (Algérie – Poste, Société Générale Algérie, BNP Paribas El Djazair, Housing bank, AGB, Natixis, Fransa-Banque, HSBC, ABC, ARAB Bank et AL SALAM Banque) .

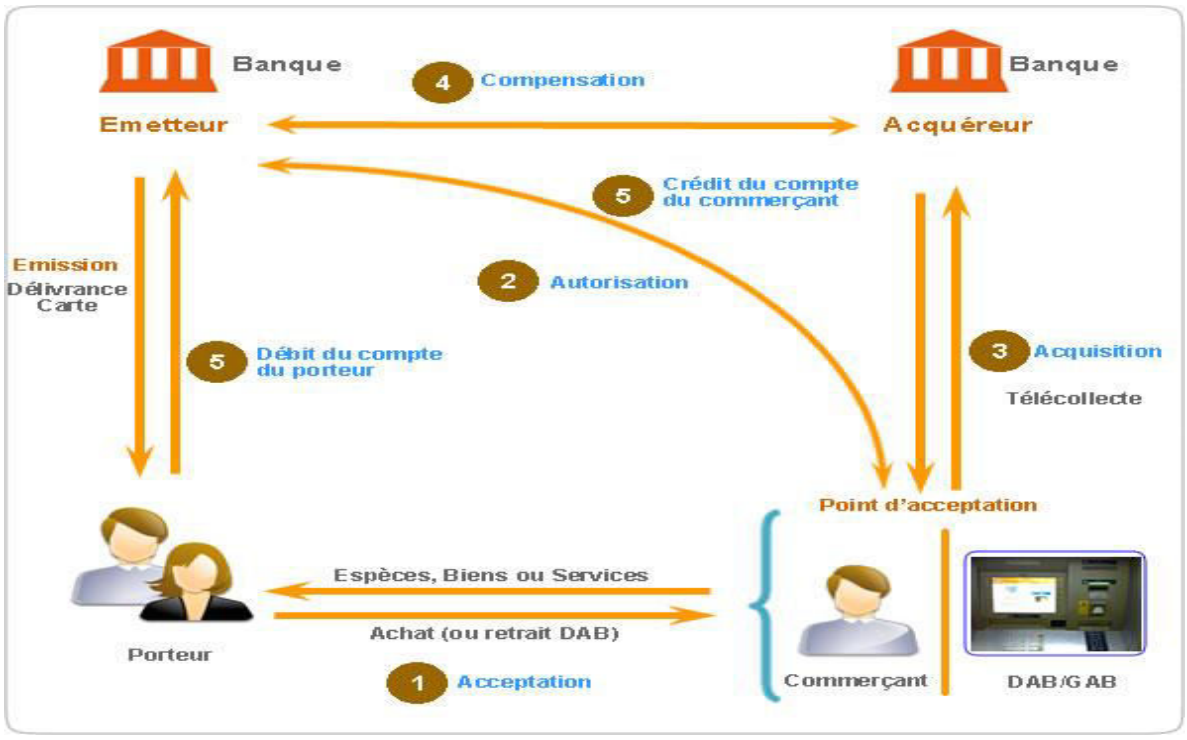
Aujourd'hui les porteurs de différentes institutions financières peuvent effectuer des retraits d'espèces à travers 1250 Distributeurs Automatiques de Billets installés sur le territoire national.

Le paiement par carte interbancaire CIB : Le paiement par carte interbancaire s'inscrit dans le cadre du projet de modernisation du système de paiement de masse et constitue l'un des maillons important pour le développement du secteur bancaire.

Ce projet d'envergure nationale répond aux standards internationaux en la matière.

En plus de retrait, le client titulaire d'une carte domestique Interbancaire CIB peut régler ses achats de biens et de services, avec sa carte auprès des commerçants affiliés au Réseau Monétique Interbancaire et dotés d'un TPE.

ANNEXE N° 12 : Processus d'une transaction monétique



La carte classic,offrant des services de paiement et de retrait interbancaire.
Elle est proposée à la clientèle selon les critères arrêtés par chaque banque.

La carte gold, proposée également à la clientèle selon les critères arrêtés; Outre le paiement et le retrait d'espèces,cette carte offre des fonctionnalités supplémentaires et des plafonds de retrait et de paiement plus important

ANNEXE N°13

La loi 09-04 du 05/08/2009

ANNEXE N° 14

Le questionnaire de notre enquête

QUESTIONNAIRE

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 télé compensation
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 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			

3) 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 :…… ……..					

….…..					

4) Est-ce que vous vous êtes facilement adaptés aux mutations technologiques de votre banque ?

OUI : NON :

5) 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

6) 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)

7) Souhaitez-vous introduire d'autres nouvelles technologies au sein de votre banque ?

OUI : NON :

8) A quelle date votre banque a-t-elle introduit Internet (effectuer sa connexion) ?

9) 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 : ……
……

9) Avez-vous un quelconque partenariat avec un opérateur téléphonique ou Algérie Télécom?

OUI : NON :

Lequel :

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 ?

6) Êtes-vous membre du réseau SWIFT ?

OUI : NON :

Si OUI, depuis quand ?

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

(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 :

(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**3.4.5**

b- Exposition des services à fournir**3.4**

c- Publicité et promotion de nouveaux produits **1.3.4.5**

d- Autres : ……

……

……

7) 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)

8) Est-ce que vous contrôlez la performance de votre système informatique ?

OUI : NON :

9) 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 :

2) Disposez-vous d'un système d'alerte en cas d'effraction ou de menace à caractère numérique ?

OUI : NON :

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 :

4) Quel est le pourcentage que représente le personnel informaticien de votre banque :du total de votre effectif **:**

5) Le système de sécurité employé permet il d'assurer une surveillance efficace et permanente des risques encourus ?

OUI : NON :

Si OUI, comment ?

……

……

……

6) Existe-il un service de détection et de traitement de fraude ?

OUI : NON :

7) Votre système aurait il été victime d'une intrusion «spamming » ou infection par virus« Malware »?

OUI……NON :

8) Y' a-t-il un dispositif qui permet de lutter contre le blanchiment d'argent ?

OUI : NON……

9) Avez-vous déjà reçu des plaintes de la part de vos clientèle ayant été victime de SPAM ?

OUI…….. NON :

10) Existe-il un service interne qui permet aux particuliers de dénoncer des spam ?

OUI : NON :

11) 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 :

12) Avez-vous fait face à des fraudes de cartes bancaires ou des cas d'usurpation de numéros de cartes bancaires ?

OUI : NON :

13) Avez-vous rencontré des cas de falsification de chèques ?

OUI : NON :

14) 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 :

ANNEXE 15 : les motivations des cybers delinquants

Listes des tableaux, schémas, figures, graphes et annexes

LISTE DE TABLEAUX

Chapitre 3

Section1

N°	Titre	Page
01	Nombre d'abonnés à la 3G et 4G	**105**
02	Indicateur des infrastructures passives	**106**
03	Nombre d'abonnés à internet	**107**
04	Nombre d'abonnés par débits	**108**
05	Nombre de site web et service en ligne en 2015	**109**
06	Nombre d'opérateur et prestation du segment Telecom	**110**
07	Indicateur des infrastructures postales (2010-2017)	**111**
08	Nombre de guichet	**112**
09	Nombre de compte CCP	**112**
10	Nombre de CIB et GAB (2010-2017)	**113**
11	Classement des 5 pays arabes les plus touchés	**118**

Section2

N°	Titre	Page
12	Banques publiques et privées de wilaya de Tizi-Ouzou en 2017	**122**
13	Echantillon des banques répondant au questionnaire	**125**
14	Impact d'introduction des TIC sur le mode interne de travail	**126**
15	Objectifs d'utilisation d'internet	**130**
16	Disposition des GAB et DAB	**134**

LISTE DES FIGURES

CHAPITRE1 :

N°	Titre	Page
01	Elément de définition des TIC	**21**

CHAPITRE 2 :

N°	Titre	Page
01	Exemple de blanchiment d'argent via une mule	**78**
02	Réexpédition de marchandises douteuses par une mule	**79**
03	Propagation vers un risque systémique	**82**
04	Les 3 démentions de la sécurité	**86**
05	LES 4 grandes activités de la sécurité opérationnelle	**98**

CHAPITRE 3

N°	Titre	Page
01	Le contexte bancaire actuel en Algérie	**115**

LISTE DES SCHEMAS

CHAPITRE 1 :

N°	Titre	Page
01	Schéma d'offre bancaire	**29**
02	Classification des modes de prestation de services bancaires selon le déplacement des clients	**31**
03	Définir la cybercriminalité	**42**
04	Décortication de la cybercriminalité	**45**
05	Typologie des cas de cybercriminalité	**53**
06	Infraction de cybercriminalité touchant le système financier	**54**

CHAPITRE 2

N°	Titre	Page
01	Une escroquerie type de cybercriminalité bancaire et financière	**63**
02	Blanchiment de bitcoin	**74**
03	Circuit de la monnaie virtuelle au cœur de la cybercriminalité	**75**
04	Evolution de risque de réputation	**81**

LISTE DES GRAPHES

CHAPITRE 1

N°	Titre	Page
01	Contribution des TIC a la croissance économique	**24**
02	Evolution mondial des principales TIC 2000-2015	**26**
03	Ménages ayant accès à internet selon le niveau de développement	**27**
04	Les cibles de programmes connect 2020	**28**

CHAPITRE 2

N°	Titre	Page
01	Face à l'absence de fiabilité de perfect money, les cybercriminels se tournent vers d'autres outils	**72**

CHAPITRE 3

N°	Titre	Page
01	Evolution du nombre d'abonnés à la téléphonie fixe	**103**
02	Evolution du nombre d'abonnés résidentiels et professionnels.	**104**
03	Taux de pénétration	**104**
04	Evolution du nombre d'abonnés à la téléphonie mobile par type de paiement	**105**
05	la répartition des parts de marchés entre les opérateurs	**106**
06	Largeur de bande Internet international en Mbits	**107**
07	Répartition d'abonnés Internet par type de technologie pour 2017	**108**

08	Répartition des abonnements internet par débit	**109**
09	Représentation des infrastructures postales	**111**
10	Nombre de guichets aménagés pour les personnes à besoins spécifiques	**112**
11	Evolution de porteur de carte monétique et le nombre de transactions le GAB	**113**
12	Evolution de la cybercriminalité entre 2014 et 2017	**117**
13	La place de la cybercriminalité en Algérie	**117**
14	Le nombre d'agences bancaire et leur pourcentage dans la wilaya de Tizi-Ouzou	**123**
15	Statut des banques	**125**
16	Les TIC que disposent les banques	**126**
17	Degré d'importance des TIC	**127**
18	La satisfaction à l'introduction des TIC	**127**
19	Les banques adaptées aux mutations des TIC	**128**
20	Les procédures mises en œuvre	**128**
21	Le nombre moyen d'opération effectué avec et sans outil informatique	**128**
22	Le temps moyen consacré à chaque type d'opération	**128**
23	Perception des TIC	**129**
24	La première connexion effectuée	**130**
25	Mode de connexion	**130**
27	Existence d'un site web	**131**
28	Objectifs de création de site internet	**132**
29	Partenariat avec un opérateur Téléphonique	**132**
30	Types de paiement	**133**
31	Les types de cartes	**133**
32	L'adhérence au réseau Swift	**133**
33	Nombre de DAB	**134**
34	Développement d'un SI	**134**
35	Stratégie de développement du SI	**135**
36	Mode d'informatisation	**136**
37	Le taux d'informatisation des banques	**136**
38	Contrôle de la performance du SI	**137**
39	La période de déroulement de contrôle	**137**
40	Disposition d'un Système d'alerte	**138**
41	Statut d'informaticiens recrutés	**138**
42	Disposition d'un système de sécurité	**139**
43	L'efficacité de système de sécurité	**139**
44	Service de détection de fraude	**140**
45	Cas de fraude de carte bancaire	**140**
46	Cas de peinte reçu	**141**
47	Cas de spamming	**141**

48	Cas de falsification de cheque	**141**
49	Dispositif de lutte contre blanchiment d'argent	**142**
50	Mesure de sécurisation 142	**142**

Liste des annexes

N°	**Titre**	**Page**
N°1	Autres définitions des TIC	160
N°2	Les onze indicateurs associés à IDI relatif à l'accès au TIC	161
N°3	Les prestations de services à distance	162
N°4	Les principales techniques de piratage bancaire	163
N°5	Fishing par email	164
N°6	La fraude aux distributeurs	165
N°7	Fraude à la carte	166
N°8	La structure de la cybercriminalité selon BNP Paribas	167
N°9	Activités de veille de la banque : Encadré 1equipe de détection et équipe de réaction	168
N°10	Encadré 2 : loi de programmation et le rôle du ANSSI	169
N°11	Présentation de la SATIM	170
N°12	Processus d'une transaction monétique	171
N°13	La loi 09/04/ du 5/08/2009	172
N°14	Model de questionnaire de notre enquête	179
N°15	Les motivations des cybers délinquants	180

Table des matières

Sommaire……I

Abréviations…….....III

Glossaire……V

Introduction générale……12

Chapitre 1 :l'émergence des NTIC et la naissance de la cybercriminalité……18

Introduction…….18

Section 1 : L'émergence des NTIC....……..……..20

I. Définitions et terminologies……20

I.1 évolution de la terminologie ……..20

I.2 définition des TIC……...22

I.3 les TIC une troisième révolution ?.....23

II. Etat des lieux des TIC……...25

- Indice de développement des NTIC(IDI)……..25

II.1 Au niveau mondial……26

II.2 Dans les pays arabe……...28

II.3 En Afrique…….....29

II.4 TIC et banque……29

III. Avantages et risques des NTIC……...38

Conclusion……...39

Section 2 : la naissance de la cybercriminalité…….……...40

I/ Définition et terminologie……..40

I.1 évolution de la terminologie……...……40

I.2 définition appropriée à la cybercriminalité……42

I.3 la distinction de la cybercriminalité et les criminalités apparentées……..…47

I.4 la cybercriminalité une 3 ème grande menace ?.....51

II/ Typologies de la cybercriminalité……52

II.1 typologies des cas de la cybercriminalité……..52

II.2 infraction de cybercriminalité touchant le système économique et financier……...54

II.3les techniques de la cybercriminalité…….57

III/ Impact de la cybercriminalité……58

Conclusion……..59

Conclusion du chapitre……...60

Chapitre2 : La banque face aux aléas de la cybercriminalité……62
Introduction……62
Section 1 : Les failles de sécurité dans le secteur bancaire et financier……63
I/ La cybercriminalité bancaire et financière……..63
I.1 la cybercriminalité bancaire……...65
I.2 la cybercriminalité financière……....69
II/La cybercriminalité est un risque pour la banque……..80
II.1 un risque cyber qui renforce la nécessaire attention……81
II.2 un risque potentiellement systémique……...82
Conclusion……...84
Section 2 : Activité de veille pour lutter contre la cybercriminalité……..85
I/La sécurité du système d'information……85
I.1 faire de la sécurité, c'est être « fermé » dans un environnement complètement ouvert.86
I.2 les dispositifs légaux internationaux de lutte contre la cybercriminalité…….....90
II/ Dispositifs et activités de veille adaptés par les banques……...92
II.1 l'adaptation des banques au risque des cyberattaque……....92
II.2 la notion de cybersécurité……96
Conclusion……...99
Conclusion du chapitre……100
Chapitre 3 : La cybercriminalité en Algérie……...102
Introduction……...102
Section 1 :L'Algérie face au phénomène de la cybercriminalité……..103
I/ Etat des lieux des TIC en Algérie……103
I.1 indicateur de développement de la société informatique……103
I.2 indicateurs des infrastructures et services postaux en Algérie……110
I.3 la place des TIC dans les banques Algériennes……114
II/ Etat des lieux de la cybercriminalité en Algérie……...117
II.1 l'évolution de la cybercriminalité en Algérie……117
II.2 le dispositif légal national de lutte contre la cybercriminalité……118
II.3 agents et organes de lutte contre la criminalité informatique……120
Conclusion……121
Section 2 : Interprétation et analyse des résultats de l'enquête……...122
Introduction……..122
I/Présentation de réseau bancaire de la wilaya de Tizi-Ouzou……122

II/ méthodologie de la recherche……123
III/ l'interprétation et analyse des analyse des résultats d'enquête……124
III.1 analyse et interprétation de résultats recueillis au niveau des banques……124
III.2 les résultats de l'entretien réalisé au niveau de la sûreté de la wilaya……..142
Conclusion……143
Conclusion du chapitre……144
Conclusion générale……..146
Bibliographie…….....150
Liste des tableaux, schémas, figures et graphes……155
Annexe …….....160
Table des matières……181