Introduction générale

Depuis les années 70, le progrès des technologies de l'information et de la communication (TIC), notamment des réseaux, a conduit à des avancées au niveau du secteur bancaire déclenchant de ce fait deux révolutions informatiques.

Dans un premier temps, la banque a subi la révolution des grands systèmes de traitement interne de gros volume d'opérations ainsi que celle des supports logistiques de communication au sein de la profession grâce au développement des réseaux interbancaires.

Après dix ans, une deuxième révolution s'est déclenchée grâce à la propagation de ces technologies qui sont parvenues à toucher toutes les agences par la mise en place des terminaux décentralisés.

Cette généralisation ainsi que celle de l'informatique ne s'est certainement pas arrêtée à ce stade-là, en effet, aujourd'hui, l'utilisation d'Internet et ses dérivés s'est enracinée dans notre quotidien rendant la société de plus en plus connectée dont l'outil commun est désormais les Ordinateurs, tablettes et Smartphones. L'adaptation de ces outils a provoqué la mutation du secteur bancaire. Devenues multicanales, les banques sont désormais capables d'interagir avec sa clientèle via différents canaux de contact utilisables simultanément, notamment, les systèmes de paiement en ligne, les sites Web bancaires les terminaux, les guichets automatiques ainsi que les applications mobiles.

Néanmoins, la multicanalité s'avère assujettie à plusieurs menaces du fait que les utilisateurs de ces technologies sont plus susceptibles de laisser des traces que ce soit des informations sur leur compte et carte bancaire, leur numéro, leur mail et bien plus encore. Ces menaces ont suivi ces utilisateurs avec multiples mécanismes tels que le Phishing, l'enregistrement des clés, les logiciels malveillants et les logiciels espions conduisant ainsi à la prolifération des attaques cybernétiques devenus, de nos jours, plutôt courantes sur la toile.

Ces actes cybercriminels ne concernent pas uniquement les institutions financières, mais d'après les rapports publiés tel que celui de l'entreprise allemande de cybersécurité NTT Security, celles-ci restent désormais la première cible des cyberattaques. Effectivement, d'après les dernières statistiques de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (Melani), ces attaques ont carrément doublé durant l'année 2014 et ont subi une

augmentation remarquable en 2016 pour enregistrer en Suisse une centaine de tentatives cybercriminelles visant les solution d'e-banking chaque jour.

Pouvant être similaires aux crimes économiques et financiers, ces attaques se traduisent généralement soit par une perte financière, par l'atteinte de l'image et de la réputation de l'établissement victime ou même par un risque pénal pour non-conformité légale et réglementaire… Ces conséquences peuvent s'avérer catastrophiques, réellement, la cybercriminalité coûte annuellement à l'économie mondiale aux alentours de 600 milliards de dollars, l'équivalent de 0,8% du PIB mondial, enregistrant une hausse continue expliquée par la facilité d'accès à ce type de crime. Ceci sans prendre en considération des dégâts engendrés par l'atteinte de l'image de l'institution financière, touchant ainsi à la confiance des clients ; le socle de toute opération financière.

Face à de tel chiffres, il n'est probablement pas surprenant de savoir que le secteur bancaire est également le secteur le plus soucieux an matière de cyber sécurité. Affirmant la prise de conscience de ce par les institutions financières, Tanguy de Coatpont, directeur général de Kaspersky Lab France révéla que ces derniers ont « travaillé dur pour sécuriser davantage les transactions financières en ligne ». Néanmoins, leurs efforts ne peuvent aboutir « que si les utilisateurs appliquent quelques bonnes pratiques simples : ne jamais cliquer sur des liens ou des pièces jointes envoyés par des inconnus, faire attention aux fichiers inhabituels, ne pas utiliser des bornes Wi-Fi publiques pour effectuer des paiements en ligne ou encore s'assurer de l'authenticité d'un site Web en vérifiant par exemple le format de l'URL ».

Cependant, il faut noter que, quel que soit la qualité et le volume du travail, isolée, une banque ne peut en aucun cas faire face à ce phénomène. Lutter contre la cybercriminalité implique tout un cadre juridique visant à renforcer les règlementations en terme de protection des données et d'analyse de risques et encore, la coopération et la coordination que ce soit entre les entités ou les pays reste primordial pour parvenir à un bon système de lutte contre la cybercriminalité.

Les pays s'avèrent donc responsables de veiller sur la sécurité cybernétique que ce soit par l'adoption d'une législation appropriée ou par la mise en place d'une stratégie nationale efficace pour lutter contre l'utilisation criminelles de ces nouvelles technologies tout en misant sur le renforcement de la sécurité informatique du pays. C'est bien à quoi œuvre la Tunisie aujourd'hui.

Etant en tête des pays de l'Afrique du Nord, la 89ème mondiale en matière de connectivité mobile et 73ème en termes d'infrastructures devançant ainsi la Russie, la Tunisie s'est tournée vers la digitalisation. Effectivement, parmi les préoccupations du gouvernement

d’union nationale figure le projet de la numérisation de l’administration Tunisienne ; une stratégie qui devrait être adoptée par tous les ministères et les institutions publiques.

Afin de suivre le courant du développement technologique continu, « la Tunisie œuvre d'arrache-pied à renfoncer ses capacités de cyberdéfense via l'instauration d'une stratégie nationale en la matière », a souligné Kamel Akrout, conseiller principal pour la sécurité nationale.

Pour ce qui est du secteur financier, les banques Tunisiennes s’avèrent bien ouillés en matière de TIC du fait que leur majorité bénéficient d’une bonne connectivité, possèdent des sites web et des applications mobiles.

D’après conseiller principal pour la sécurité nationale, 82% de la totalité des crimes dans le monde sont des crimes cybernétiques dont 12% sont liés directement à l'espionnage des données financières et gouvernementales.

"Face à cette situation, la Tunisie est appelée à prendre les mesures nécessaires pour bien protéger son espace cybernétique" a signalé M. Akrout. Effectivement, parmi les principales lacunes de la Tunisie en matière de protection cybernétique l’absence d’un cadre juridique spécifique à la cybercriminalité. Néanmoins, il existe bien un projet de loi traitant ce sujet n’ayant pas encore vu le jour pour à cause de la non stabilité des pouvoirs publics.

La motivation de ce travail réside dans le manque énorme d’informations et de chiffres concernant la cybercriminalité au niveau du secteur bancaire tunisien. De ce fait, une étude quantitative sur l’exposition ainsi que sur les moyens utilisés pour lutter contre ce phénomène pourrait être intéressante afin d'avoir une idée claire sur l’état sécuritaires des banques tunisiennes.

Ainsi, ce mémoire tentera de répondre à la question suivante :

Est-ce que les banques tunisiennes sont bien outillées contre le phénomène de la cybercriminalité ?

Pour ce faire, ce travail s’articulera autour de trois chapitres.

Le premier chapitre étant scindé en deux, se penchera dans un premier lieu sur la définition des technologies de l’information et de la communication tout en évoquant leurs caractéristiques, avantages et inconvénients ainsi que leur introduction dans le monde en général et au niveau du secteur bancaire en particulier. Ensuite nous allons procéder à la démystification du phénomène de « Cybercriminalité » en portant une attention particulière à sa présence au niveau du secteur bancaire.

Le second chapitre, sera consacré en totalité à la lutte contre la cybercriminalité. D'abord, au niveau de la première section, nous allons exposer différents moyens de lutte contre la cybercriminalité à savoir les moyens techniques, légaux, humains et organisationnels. Dans un deuxième temps, nous allons présenter un moyen de suivi de la performance en sécurisation cybernétique notamment la notation en cyber-sécurité.

Le dernier chapitre sera consacré à une étude centré sur le cas tunisien. Dans un premier temps, nous allons présenter un bref aperçu sur l'introduction des TIC en Tunisie et au niveau du secteur bancaire ainsi que sur les attaques cybernétiques contre ces institutions pour enfin présenter les différents moyens utilisés pour lutter contre ce phénomène. Au niveau de la deuxième section, nous allons nous pencher sur l'étude de la réalité des banques Tunisiennes en terme d'équipement en TIC, d'exposition au risque cybernétique et de degré protection contre un tel phénomène et ce par l'analyse d'un questionnaire élaboré pour ce faire.

Chapitre 1 : Les TIC et la cybercriminalité

Introduction :

TIC et NTIC sont des acronymes pour respectivement les Technologies de l'Information et de la Communication et les Nouvelles Technologies de l'Information et de la Communication qui rassemblent les télécommunications, les multimédias, Internet, l'informatique et l'audiovisuel dont l'évolution s'est déroulée sur quatre phases. Du milieu des années soixante jusqu'à la fin des années soixante-dix, les nouvelles technologies de l'information et de la communication ont vécu la première phase de leur évolution celle de « l'information centralisée » avec l'élaboration des systèmes d'orientation assistés par ordinateurs notamment les réseaux. D'ailleurs, durant cette phase, avec le développement des réseaux interbancaires le secteur bancaire a connu sa première révolution informatique. Du début des années quatre-vingt jusqu'au milieu des années quatre-vingt-dix vient la deuxième phase, celle des « micro-ordinateurs » qui facilitent la conception et la diffusion des programmes et rendent l'utilisation interactive plus économique. La troisième phase s'est déclenchée à la fin des années quatre-vingt-dix avec l'utilisation d'« Internet » permettant l'accès instantané aux sites depuis différents lieux. La dernière phase a vu le jour avec le « numérique », qui fusionne toutes les technologies à caractère analogique (ordinateur, télévision radio ect.) dans un ensemble numérique intégré (Cunningham et Fröschl, 1999) permettant aux individus d'accéder à Internet par leurs téléphones mobiles.

Les NTIC ont intégré petit à petits les secteurs les plus stratégiques des pays ; la santé, la gestion de l'énergie, l'éducation, les services de communication, le transport, le secteur bancaire, le commerce etc.

Toutefois, cette rapide évolution s'avère assujettie à de multiples menaces pouvant être ainsi problématique aussi bien pour les personnes physiques que morales. Effectivement, de nouveaux délits et infractions sont nés et se sont développés avec le progrès de ces technologies, communément connus sous le terme de « Cybercriminalité ». Ce phénomène tellement attrayant, a déjà tenté des milliers de cyber délinquants, causant des désastres au niveau de tous les secteurs, notamment, le secteur bancaire.

Au niveau de ce premier chapitre, nous trouvons indispensable de l'entamer par une première section où nous essayerons de définir les TIC, d'évoquer leurs caractéristiques, avantages et limites et de faire un tour d'horizon sur ces technologies dans le monde en général et au niveau du secteur bancaire en particulier afin de mieux assimiler les répercussions et les transformations dues à leur introduction. Au niveau de la deuxième section, nous allons tenter de démystifier le phénomène de « Cybercriminalité » qui s'est manifesté avec l'évolution des TIC en mettant l'accent sur la cybercriminalité au sein du secteur bancaire.

Section 1 : Les Technologies de l'information et de la communication (TIC)

Les notions de technologies de l'information et de la communication (TIC) et de nouvelles technologies de l'information et de la communication (NTIC) regroupent les techniques et outils informatiques, d'Internet et de télécommunications utilisées dans le traitement et la transmission des informations (Abtoy, 2004). Par extension, ces notions concernent également le secteur d'activité économique de technologies de l'information et de la communication.

Les NTIC désignent les TIC qui viennent d'être inventées, le concept des nouvelles technologies est apparu suite à l'évolution des technologies réseaux, à l'initiative de plusieurs ingénieurs réseaux qui ont jugé primordial de différencier entre ces technologies et les anciennes. Toutefois, une NTIC devient ancienne lorsqu'elle disparait du marché.

1. Définition des TIC :

Vu l'hétérogénéité et la complexité des TIC, la littérature n'a pas pu, jusqu'à Juillet 1998, parvenir à un consensus sur leur définition. Le comité de la Politique de l'Information, de l'Informatique et des Communications (PIIC) de l'Organisation de coopération et de développement économiques (OCDE) en collaboration avec la Commission statistique de l'Organisation des Nations unies (ONU) et l'Eurostat (Eurostat est une direction générale de la Commission européenne chargée de l'information statistique à l'échelle communautaire), ont tenté de définir le secteur des TIC comme étant les secteurs manufacturiers et des services qui facilitent la transmission, le stockage et le traitement de l'information par des moyens électroniques[1].

Ces réflexions se sont orientés vers la proposition d'une définition internationale du secteur des Technologies de l'Information et de la Communication qui a servi par la suite de point de départ à des rectifications dans les nomenclatures au niveau national et international.

[1] Plus précisément : Concernant les secteurs manufacturiers : les produits d'une industrie considérée doivent être destinés à remplir la fonction de traitement de l'information et de la communication incluant la transmission et l'affichage, utiliser l'informatique pour détecter, mesurer et/ou enregistrer un phénomène physique ou pour contrôler un processus physique. Concernant les services : les produits d'une industrie considérée doivent être capables d'assurer la fonction de traitement de l'information et de la communication par un moyen électronique (OCDE 2000)

En effet, plusieurs auteurs, organismes et Etats ont proposé des définitions des TIC dont les plus importantes sont les suivantes :

D'après une convention internationale de l'OCDE, le secteur des TIC inclue les secteurs producteurs et distributeurs de TIC (fabrication et commerce de gros de matériel informatique, électronique et automatismes industriels…) ainsi que les secteurs des services directement liées aux TIC (Services informatiques, télécommunications, location …). En revanche, elle exclue les industries créant de l'information appelées aussi les industries de contenu[2] (Dryden, 2003).

Selon les Etats- Unis: D'après la nomenclature Standard Industrial Classification (SIC) de 1987 publiée par l'Office of Management and Budget, les « industries des technologies de l'information » incluent d'une part, les industries « matérielles » comprenant les offreurs (grossistes et détaillants) d'instruments électroniques de mesure et d'équipements informatiques et d'autre part, les logiciels et les industries de services englobant les industries de logiciels « prêts à l'usage » et des services liés aux ordinateurs : les fournisseurs des infrastructures immatérielles et matérielles procurant la base de connexion entre ordinateur et serveur.

Selon l'union européenne et France : Le secteur TIC est défini par une liste d'activités se référant à la nomenclature européenne adoptée à la suite des travaux de l'OCDE. Cette définition englobe trois filières : les télécommunications qui comprennent les réseaux et donc Internet, : l'informatique avec la fabrication des ordinateurs et des logiciels et enfin l'électronique.

Selon HERBERT SIMON (prix Nobel des sciences économiques 1998) Les TIC contribuent à rendre: « Toute information accessible aux hommes, sous forme verbale ou symbolique, également sous forme lisible par ordinateur; les livres et mémoires seront stockés dans les mémoires électroniques… », il les a définis comme étant: « L'ensemble des technologies d'informatique et de télécommunication, elles sont les résultats d'une convergence entre technologies. Elles permettent l'échange des informations ainsi que leurs traitements. Elles offrent aussi de nouveaux moyens et méthodes de communication ».

Selon Benoit Chapron (2006) Les TIC sont définis comme étant une « expression aux contours assez flous, apparue avec le développement des réseaux de communication, désignant

[2] Secteur industriel qui couvre trois activités principales à savoir, la création de produits et services basés sur le contenu de l'information, le conditionnement et le développement de ces produits et services et leur distribution. Il regroupe ainsi les secteurs de l'édition électronique, imprimée et audiovisuelle.

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-spécialiste. Au confluent de l'informatique, des réseaux de télécommunication et de l'audiovisuel ; les TIC s'adressent au plus grand nombre »

Selon Charpentier: « Les (TIC) sont un ensemble de technologies utilisées pour traiter, modifier et échanger de l'information, plus spécifiquement des données numérisées. La naissance de ces TIC est due notamment à la convergence de trois activités. Au sens strict, les TIC sont composées du:

- Domaine des télécommunications qui comprend lui-même les services et les équipements.
- Domaine de l'informatique qui comprend le matériel, les services et les logiciels.
- Domaine de l'audiovisuel qui comprend principalement la production et les services audiovisuels ainsi que l'électronique grand public. »

Selon Amabile et Gadille, 2003 les NTIC constituent un ensemble de technologies associées à l'utilisation d'Internet et de ses protocoles, ainsi que les réseaux locaux permettant la connexion des stations de travail ou des micro-ordinateurs.

2. Caractéristiques des TIC :

Les technologies d'information et de communication disposent de plusieurs caractéristiques :

- **Omniprésence :** Ces technologies sont utilisées au niveau de la majorité des secteurs (finance, éducation, santé …).
- **Amélioration :** Ces technologies sont en constante évolution, en effet, elles ne cessent de se développer et de se perfectionner facilitant le quotidien de ses utilisateurs tout en minimisant les coûts, permettant ainsi une maximisation d'output.
- **Source d'innovation :** A part leur développement propres, les TIC permettent la création de nouveaux moyens, produits et processus et ce à un rythme de plus en plus accéléré.

- **Rapidité :** Ces technologies facilitent les tâches ce qui rend leur exécution plus rapide.
- **Miniaturisation :** Ces technologies se soucient de la création de produits informatiques, ou électroniques et de leurs dispositifs ainsi que des supports d'information à des échelles de plus en plus petites.
- **Multicanalité :** les TIC adoptent trois canaux. En premier le lieu, le canal textuel, puis, le canal image et enfin le canal son étant moins répandu.

Les technologies de l'information et de la communication sont omniprésentes du fait qu'elles ont touché tous les secteurs de l'économie auxquels le monde bancaire fait partie. Réellement, ce dernier appartient aux premiers secteurs utilisateurs du commerce électronique effectuant des transactions commerciales et des services à travers le réseau Internet. En effet, les banques en lignes offrant des produits et services diversifiés et variés sont de plus en plus présentes.

Ces technologies affectent aussi l'organisation du travail et la productivité, vu qu'elles constituent une mine d'informations pour les professionnels les aidant à mieux connaitre leur clientèle et que le traitement des données est effectué dans moins de temps et avec plus d'efficacité et de précision, ce qui rend le service plus rentable et plus adapté aux besoins du consommateur qui devient plus exigeant et connaisseur.

3. TIC au niveau du secteur bancaire : moyens de paiement électronique

La nature des prestations bancaires et financières a été profondément touchée grâce à l'introduction d'Internet, l'évolution continue et les innovations qui se sont succédées des technologies d'information et de communication. Notamment, elle a pris son élan dans le développement des services de banque à distance d'où l'émergence des banques sans guichet, généralement appelée banques en ligne ou encore « e-bank », introduisant de nouveaux types de services tel que l'octroi de crédits, l'achat de titres, la carte bancaire et les distributeurs et guichets automatiques bancaires.

Outre les services de banque à distance, la banque a tiré profil de l'essor d' Internet et des technologies de l'information au niveau des télécommunications et des moyens de paiements :

3.1 Les nouveaux outils de télécommunication

Les bons rapports entre les milieux financiers, bancaires financiers et les télécommunications ont débutés avec l'invention du télégraphe.

Etant primordiales dans la gestion des relations avec les clients et les autres institutions, les télécommunications ont fortement contribué à l'expansion des milieux financiers en apportant des moyens plus performant parmi lesquels on peut citer la banque par fil et la banque par écran.

- La banque par fil : elle regroupe le téléphone : un service permanent permettant une consultation limitée par serveur vocal et le fax : réservé aux abonnés souhaitant recevoir leurs relevés des comptes détaillés de toutes les transactions effectuées.

- La banque par écran : elle regroupe l'Internet, l'Intranet, l'Extranet et les EDI (Échange de Données Informatisé).

L'Internet : c'est un réseau informatique composé de réseaux internationaux, nationaux, régionaux accessible par tout le monde qui permet de connecter les banques entre elles afin de transmettre de nombreuses informations : de la voix pour le téléphone, des images pour la télévision, des textes pour les sites Web, du courrier pour les emails etc...

L'Intranet bancaire : L'Intranet bancaire est un réseau interne qui relie tous les ordinateurs d'une même banque quel que soit leurs emplacement, situés au niveau du siège ou dans des bureaux distants (le réseau d'agences). Ce réseau dédié contient l'ensemble des informations bureautiques, des applications et de télécommunication au service de l'activité interne de la banque. De ce fait, il est invisible pour toute personne étrangère.

L'Extranet : C'est une fraction de l'intranet bancaire étendue aux personnes, institutions et clients agréés pour que ces derniers puissent accéder, après authentification, d'une manière sécurisée à des informations précises.

L'EDI (Échange de Données Informatisé): l'EDI est un outil réservé à l'échange électronique consistant à transférer automatiquement les informations en connectant le programme de gestion d'une entreprise à celui d'une autre par une ligne spécialisée.

L'EDI est utilisé d'une manière intensive dans le monde bancaire vu qu'il est souvent considéré comme un vecteur important de service client du fait qu'il réduit les coûts de fonctionnement, optimise l'organisation et améliore l'activité et ce en automatisant quelques opérations telles que les virements des salaires et les prélèvements.

3.2 Les instruments de paiement : La carte bancaire

La carte bancaire, est un moyen de paiement qui a fait son apparition à la fin des trente glorieuses et dont le développement s'est étendu sur une vingtaine d'années afin de parvenir à tous les réseaux bancaires et tous les particuliers. Il fallait attendre les années quatre-vingt pour passer de la carte à piste magnétique à la carte à puce et commence à faire des retraits dans des distributeurs automatiques et à régler les paiements chez les commerçants avec une meilleure sécurisation. Cette carte est délivrée par un établissement de crédit à son titulaire accompagnée d'un code secret.

On distingue différentes technologies de système de paiement ainsi qu'une variété de cartes.

- Les technologies de système de paiement sont matérialisées soit par des appareils installés au niveau des agences permettant le retrait automatique d'espèces ou par des appareils électroniques chez les commerçants permettant le paiement par carte. Il s'agit des DAB, GAB et TPE qui sont décrit dans ce qui suit :

  - ✓ Guichets automatiques de billets (GAB) : Ce sont des automates aménagés au niveau des agences qui permettent au client détenteurs d'une carte bancaire, à l'aide de leurs codes confidentiels, d'effectuer eux même leurs opérations bancaires et ce 24 H sur 24. Ces appareils automatiques permettent à la clientèle de l'établissement propriétaire, notamment, de réaliser plusieurs opérations tel que la consultation de

solde, la demande de RIB ou de chéquiers, la remise de chèques, le virement de compte à compte au sein de la banque et enfin le versement et retrait d'espèces.

- ✓ Distributeurs automatiques de billets (DAB) : Ce sont des automates permettant aux titulaires de cartes de retirer des espèces de leurs comptes à l'aide d'un code confidentiel individuel
  Les GAB fonctionnent aussi en tant que des distributeurs de billets (DAB) pour les clients titulaires de cartes acceptées par l'appareil.

- ✓ Terminal de Paiement Electronique (TPE) : C'est un appareil électronique fourni par la banque à une catégorie de clients tels que les prestataires de services et les commerçants leur permettant d'accepter les transactions de paiement de leur clientèle via des cartes de paiement bancaires.
  Ce moyen de paiement moderne assure une grande sécurité, un gain de temps et une utilisation facile.

❖ En ce qui concerne **les cartes bancaires**, ce moyen de paiement, sous forme de carte en plastique, est délivré par un établissement de crédit. Il en existe plusieurs types, qu'il ne faut pas confondre.
Les cartes les plus connues sont la carte de retrait, la carte de paiement, la carte de débit et la carte de crédit. Il en existe cependant d'autres comme la carte prépayée, la e-carte etc.

- ✓ La carte de retrait : C'est une carte permettant exclusivement d'effectuer des retraits d'espèces dans les distributeurs automatiques de billets, parfois même dans les seuls distributeurs du réseau bancaire de la banque émettrice. Elle permet également de consulter le compte, d'effectuer des dépôts, de commander des chéquiers.

- ✓ La carte de débit : c'est une carte de paiement qui remplit les fonctions de la carte de retrait et permet, en plus, d'effectuer des achats directement chez des commerçants ou à distance dont les montants des transactions sont prélevés sur le compte du porteur dans moins de 48h. Ces cartes sont communément appelées « carte à débit immédiat » ou parfois encore « carte à autorisation systématique ».

- ✓ La carte de crédit : C'est une carte permettant d'effectuer les opérations réalisables avec une carte de paiement, mais dont l'utilisation est adossée à un crédit renouvelable; les montants sont débités de façon différée sur le compte du porteur. Egalement, ce sont les cartes de crédit renouvelable ainsi que les cartes de crédit à la consommation.

- ✓ La carte prépayée C'est une carte exclusivement réservée aux particuliers permettant de disposer d'une somme d'argent limitée préalablement alimentée. Elle peut être déclinée sous forme de « carte cadeaux » ou encore de « carte rechargeable ».

- ✓ La e-carte**:** C'est une carte virtuelle qui sert à sécuriser les transactions réalisées sur Internet. Ainsi, le client obtient un numéro de carte éphémère pour chaque transaction réalisée pour que le numéro « réel » de la carte bancaire ne transite pas sur Internet.

De nouvelles solutions de paiements ont été développées par des banques afin de faciliter et simplifier encore plus les procédures d'achat et d'encaissement. Notamment, BNP Paribas, conjointement avec la Société Générale et La Banque Postale ont instauré plusieurs solutions de paiement innovantes tel que Paylib[3], Mobo[4] et le paiement sans contact[5].

3.3 Le m-Banking

Le mobile Banking est un service fourni par une banque ou une autre institution financière permettant à ses clients d'effectuer des opérations bancaires à distance à partir d'un appareil mobile tel qu'une tablette ou un smartphone. Il s'agit d'une application fournie par l'institution financière afin de rendre les services bancaires mobiles, notamment les transactions financières et les échanges communicationnels, toujours disponibles réduisant ainsi la visite des clients éligibles à ce type de service d'où un moindre coût de traitement des transactions.

[3] Paylib ; un portefeuille numérique en ligne s'adressant aux entreprises qui vendent sur Internet assurant mobilité
[4] Mobo ; une application mobile transformant le smartphone ou la tablette en terminal de paiement et ce, à l'aide d'un lecteur de carte connecté à un 'Pin Pad'
[5] Le paiement sans contact ; un instrument de paiement facilitant les petits achats au quotidien grâce à la technologie communication à courte portée (NFC : Near Field Communication) avec laquelle le terminal de paiement et la carte ou le mobile doivent être équipé.

Les services bancaires mobiles permettent aux clients de gérer leurs finances personnelles à distance. En effet, elles peuvent inclure la consultation de comptes bancaires, les paiements de factures électroniques, les transferts et les virements dans la limite du montant choisi par l'institution ainsi que le conseil en contactant les banquiers par e-mail ou SMS. Certaines applications permettent également le téléchargement et l'impression des copies de relevés.

4. Etat des lieux des TIC dans le monde

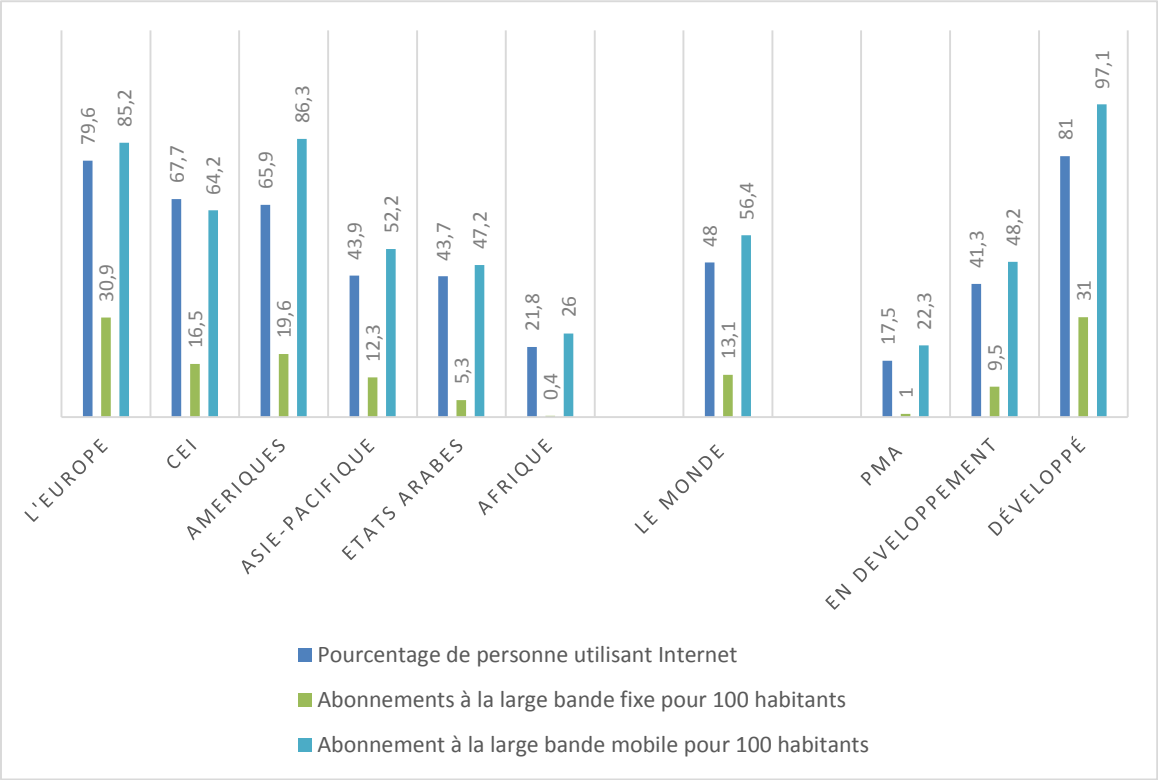
Les dernières données de l'UIT (Union Internationale des Télécommunications) concernant le développement des TIC indiquent que l'utilisation et la connectivité de ces technologies suivent une croissance soutenue, cette croissance est plus accélérée pour le sous-indice d'utilisation. En effet, selon le rapport « Mesurer la société de l'information de 2017 » fournit par l'UIT, le sous-indice d'utilisation a augmenté en moyenne de 0,37 point, contre 0,13 point dans le sous-indice d'accès, et ce grâce à l'adoption haussière de la large bande mobile dans le monde ce qui a permis à un nombre ascendant de personnes, en particulier des pays en développement, à rejoindre la société de l'information et accéder à Internet et son utilisation.

Dans notre travail, nous allons nous concentrer sur l'utilisation des TIC qui peut être visualisé par trois indices :

- ✓ Le pourcentage des personnes utilisant Internet
- ✓ Le nombre d'abonnements à la large bande fixe pour 100 habitants; correspond au nombre d'abonnements à la large bande fixe (filaire) pour l'accès à Internet public divisé par la population et multiplié par 100.
- ✓ Le nombre d'abonnements à la large bande mobile actifs pour 100 habitants ; désigne la totalité des abonnements à la large bande mobile ordinaire augmentée par les abonnements à la large bande mobile dédié permettant l'accès à l'Internet public.

Le réseau large bande est un réseau capable de transmettre des signaux à un débit élevé dont la définition diffère d'un pays à un autre et ce dépendamment de la capacité de transmission à partir de laquelle le réseau peut être caractérisé comme large bande.

Figure 1: Utilisation des TIC dans le monde



Source: ITU World Telecommunication /ICT Indicators database

Des fractures numériques importantes subsistent encore, malgré l'essor des TIC, au niveau de quelques pays et régions. Cette disparité d'utilisation et d'accès à Internet est nettement remarquable entre les pays développés et ceux en voie de développement notamment les pays les moins avancés. En effet, en Europe et dans la région Amériques ainsi que dans la CEI (Communauté des États Indépendants), le nombre d'abonnement à la large bande mobile pour 100 habitants dépassent de loin celui constaté au niveau des autres régions et correspondent même au triple du nombre enregistré en Afrique et ce avec un débit de connexion probablement plus élevé.

On constate des disparités comparables entre les taux d'utilisation d'Internet. Réellement, à peu près la moitié de la population du monde utilisent Internet mais avec d'une manière disproportionnée. La proportion des utilisateurs d'Internet est deux fois plus élevée dans les pays développés que celle dans les pays en développement et est de 17% uniquement dans les PMA. Au niveau des Amériques, les individus utilisent plus ou moins trois fois plus Internet que les personnes vivant en Afrique. Quant à l'Asie-Pacifique et les Etats Arabes, ils ont quasiment le même taux d'utilisation.

En ce qui concerne la large bande fixe, on constate un nombre d'abonnements très bas par rapport à la large bande mobile qui atteint en 2017 deux abonnements par 500 personnes en Afrique. L'Europe enregistre le plus grand nombre d'abonnements étant de 30 par 100 habitants suivie par la région d'Amériques avec 19 abonnements et la CEI avec 16 abonnement par 100 habitants.

Des progrès notables ont également été accomplis en vue de réduire ces fractures numériques tant au niveau d'utilisation d'Internet qu'au niveau du nombre d'abonnements à la large bande fixe et mobile.

- L'accès à Internet

Tableau 1: Les nombres des individus qui utilisent l'Internet

		2010	2011	2012	2013	2014	2015	2016	2017
Pourcentage d'individus utilisant Internet	Développé	66,5	67,7	72,0	73,8	75,6	77,4	79,6	81,0
	En développement	20,6	23,4	26,3	29,0	32,4	36,1	39,0	41,3
	Monde	28,9	31,3	34,3	36,9	39,9	43,2	45,9	48,0
Croissance du pourcentage	Développé	-	2%	6%	3%	3%	2%	3%	2%
	En développement	-	13%	12%	11%	12%	11%	8%	6%
	Monde	-	8%	10%	7%	8%	8%	6%	5%

Source: ITU World Telecommunication /ICT Indicators database

Le progrès au niveau de la croissance des utilisateurs d'Internet au niveau des pays en voie de développement est désormais discret. Néanmoins, il enregistre un taux toujours positif et supérieur à celui des pays développés et ceci tout au long des sept ans d'où un pourcentage d'utilisateurs d'Internet qui double durant cette période pour passer de 20.6% à 41.3% dans les pays en développement.

❖ **Etat des lieux des TIC au niveau du secteur bancaire :**

Dans le monde bancaire, les NTIC touchent principalement les moyens de paiement traversant une évolution permanente qui semble s'accélérer. Si la liquidité reste prépondérante dans plusieurs pays dans le monde, principalement pour les petites transactions du quotidien, les paiements électroniques sont de plus en plus utilisés (rapport mondial sur les paiements réalisés par le cabinet Capgemini et le groupe bancaire BNP Paribas édition 2017).

Effectivement, ce nouveau mode de paiement a vu sa part s'amplifier en 2014-2015 pour enregistrer la plus grande croissance de la décennie avec 11.2% alimentée particulièrement par l'Asie émergente (Chine, Hon Kong, Inde et autres marchés Asiatiques) avec un taux de croissance de 43,4% et ce grâce aux portefeuilles et paiements mobiles générant la multiplication d'utilisation des cartes bancaires. Les marchés en développement ont, de même, contribués à 32,1% du volume mondial des paiements numériques, cette année-là, et ont enregistré un taux de croissance colossal de 21,6% contre une contribution des marchés matures à hauteur de 67,9% avec un taux de croissance de 6,8%.

Cependant, il est à noter qu'au cours de la dernière décennie, le nombre de cartes de crédit à diminué en dépit des cartes de débit. En effet, alors que la part de marché des cartes de débit est passée à 70,5% du total des transactions par carte en 2015 étant de 202 milliards contre 69,9% en 2014, la part de marché des cartes de crédit est passée de 30,1% en 2014 à 29,5% en 2015 pour atteindre un total de 85 milliards. Ceci peut être expliqué principalement par la publication du Bâle III vers la fin de 2010 fixant de nouvelles normes plus contraignantes via des exigences supplémentaires en fonds propres qui assignent des pondérations en capital basées sur la nature et le montant de l'exposition gonflant ainsi le risque lié à ces cartes. Effectivement, un milliard d'unités monétaire de prêts-cartes ou d'engagements de crédit inutilisés à des milliers de consommateurs est traité, selon Bâle III, de la même façon qu'une exposition d'un milliard d'unités monétaire à une seule contrepartie.

Quant aux paiements sans contact, ils sont en train de devenir la « nouvelle normalité » en Europe, particulièrement, en France où la circulation des cartes Visa sans contact a doublé, passant de 20,3 millions en 2014 à 40 millions en 2015 et le Royaume-Uni dominant les marchés sans contact avec un nombre de cartes sans contact en circulation qui atteignent les 106,9 millions en 2015.

Parallèlement à l'accroissement de la part des transactions non monétaires dirigée principalement par les cartes bancaires et les transferts électroniques, le chèque et les espèces ont vu leur part se dégrader sensiblement à l'échelle mondiale.

Effectivement, le volume de chèques a continué de baisser pour enregistrer un taux de croissance de -13.4% en 2014 avec un volume de 2,5 milliards de chèques et un montant de 1.200 milliards d'euros. Ce n'est pas peu certes, mais bien moins qu'en 2009 où le volume était de 3,5 milliards de chèques. De nos jours, il ne représente pas plus que 5% des paiements alors qu'en 1992 et 1975 il représentait respectivement 51% et 75%. D'après le rapport mondial sur

les paiements, il existe des pays qui envisagent même de retirer progressivement les chèques du marché dans un proche avenir, notamment, le Royaume-Uni et l'Australie.

En gros, l'étude du cabinet Capgemini et le groupe bancaire BNP assure l'apparition d'un environnement des paiements plus moderne grâce aux innovations multiples de la finance, les fintechs, de nouvelles attentes de la clientèle et le changement progressif du cadre réglementaire visant entre autres à encourager l'émergence de nouveaux acteurs et la concurrence au niveau du paiement.

5. Les avantages et risques des TIC

5.1 Les avantages des TIC

Au niveau du secteur bancaire, les nouvelles technologies de l'information et de la communication comprennent l'évolution du matériel ainsi que les logiciels liant les clients et la banque, d'une part et la banque et ses services de gestion, d'autre part et bien sûr leur mise à jour pour être toujours à la page et garantir un niveau de sécurité acceptable touchant, de ce fait, non seulement les produits et services bancaires mais le fonctionnement des banques et leur organisation aussi. Afin d'expliciter encore plus les avantages d'une meilleure intégration de ces nouvelles technologies nous allons fournir une liste qui n'est certes pas exhaustive mais qui rassemble les plus intéressants pour le secteur bancaire :

- **Amélioration de l'efficacité et de la productivité des établissements bancaires :**

Les transactions qui, jadis, se réalisaient uniquement au niveau des agences sont devenu, avec l'intégration des NTIC, accessibles via plusieurs canaux, tels que le téléphone ou l'Internet, à travers les plateformes en ligne des banques. L'utilisation de ces technologies a permis aux banques de réduire l'effectif et améliorer la productivité et l'efficacité du personnel par des formations professionnelles. En effet, il existe principalement deux raisons à la multiplication les canaux de désintermédiation : mieux connaitre leur clientèle et les servir plus efficacement.

L'automatisation du système bancaire a facilité la mise en œuvre des produits et services financiers, entre autres les ordres de vente et d'achats des titres financiers et le virement bancaire et a augmenté par la suite la productivité des banques ainsi que leur capacité à répondre à l'accroissement de la demande.

- **Augmentation de la rapidité des transactions et baisse de leurs coûts :**

Grâce aux systèmes d'informations, les banques ont réduit les opérations ennuyeuses pour le personnel et ont facilité celles qui sont fatigantes, entre autres, les ordres de vente et d'achats des titres financiers, le traitement de dépôts en espèce et le virement bancaire. L'emploi de ces systèmes, qui rendent les banques de plus en plus interconnectées, a conduit à l'augmentation de la rapidité de l'exécution des services bancaire, à la croissance du chiffre d'affaires et à la réduction du personnel permettant ainsi une économie sur la masse salariale.

- **Attraction d'une nouvelle clientèle :**

Une clientèle plus cultivée, plus jeune et plus exigeante est attirée par ces banques modernes grâce à la multiplicité des canaux de communication, et à l'adoption de publicité orientée selon les gouts et les modes d'utilisation d'Internet des clients.

- **Augmentation du volume d'informations collectées :**

D'après Amabile et Gadille, 2003 les TIC « …développent une accessibilité aux informations que l'entreprise pouvait difficilement atteindre auparavant ou, plus simplement, elles peuvent améliorer l'accès à certaines informations »

- **Meilleure connaissance des clients :**

Dans le monde bancaire, la connaissance de la clientèle est indispensable, et pour parvenir à une meilleure connaissance, les banques doivent exploiter les masses de données déjà collectées en les analysant sous plusieurs angles afin d'établir des relations entre les données de la base et d'en tirer des informations utiles ; c'est ce qu'on appelle le data mining. L'économiste Philip A. Fisher a affirmé, suite à une analyse effectuée en 1975, qu'en archivant les informations sur les prêts et les dépôts sous format électronique permettrait une meilleure prise de conscience sur les attentes de la clientèle et ce, en analysant les montants moyens et les fréquences des dépôts.

- **Aide à la prise de décision :**

Les informations tirées par le Data Mining aident non seulement à faciliter la prise de décision mais en plus à améliorer l'efficacité de cette prise de décision. En effet, en connaissant plus finement la clientèle et leurs habitudes, il est plus facile de réaliser des simulations, proposer des services et créer des produits et proposer des services qui correspondent le plus aux besoins des consommateurs ou lancer des campagnes publicitaires plus efficientes.

- **Meilleure gestion du risque :**

Avec la mise en place des systèmes de gestion en temps réel dans toute l'activité de crédit, outillées de système d'alerte, les banques se trouvent en mesure d'accroitre la qualité du crédit, d'assurer un contrôle permanent des risques et de prévenir en cas de leur survenance.

5.2 Les risques de l'investissement dans les TIC :

L'utilisation des TIC et NTIC au niveau du secteur bancaire représente aussi bien des avantages que des limites qui peuvent être classés selon leur nature :

- **Problèmes de rentabilité :**

L'intégration des nouvelles technologies au niveau des banques peut être qualifiée de coûteuse compte tenu du prix du matériel, des logiciels, de la maintenance, de la mise à jour ainsi que du renouvellement sans négliger la formation du personnel nécessaire à la bonne utilisation de ces technologies. Et une fois équipées, il s'avère généralement que le matériel et/ou les logiciels sont sous-utilisés à cause d'un suréquipement classé comme perte financière.

- **L'indisponibilité des services :**

Plusieurs motifs peuvent entrainer l'indisponibilité des services bancaires ; entre autres, les pannes des réseaux, des serveurs d'application ou des bases de données qui peuvent survenir soit par coupure de services essentiels tel que la télécommunication et l'électricité ou à cause d'une erreur de conception ou d'utilisation. Les conséquences de ces pannes peuvent être nuisibles à la réputation de l'établissement et mener même à la perte de la clientèle.

- **La malveillance :**

Toute information confidentielle, au niveau de la base de données de la banque, doit être protégée et sécurisée. Mais avec l'utilisation d'Internet, les informations relatives aux clients utiles à fins commerciales peuvent être exploitées différemment et d'une manière illégale que ce soit pour un travail personnel, un détournement d'information ou de fonds.

Section 2 : La cybercriminalité

L'utilisation des NTIC par le monde de l'entreprise ainsi que par la population est grandissante et est devenue, de nos jours, indispensable que ce soit dans les pays développés ou en voie de développement. Ceci revient en grande partie à la croissance rapide d'Internet, effectivement, la connexion à Internet et d'interconnexion des systèmes a amené à incorporer l'informatique dans de nombreux produits et services tel que les voitures, les infrastructures de transport, la distribution d'électricité, les services bancaires, etc.

Réellement, au tout début, le développement de l'Internet n'a pas pris en considération la sécurité ce qui explique l'exposition de ses composants (logiciels, matériels et protocolaires) à de nombreuses failles favorisant ainsi l'émersion de nouveaux comportements criminels au niveau du cyberespace. C'est ainsi que le phénomène de « cybercriminalité » est né.

Définitions :

Malgré le fait que le terme « cybercriminalité » n'est pas nouveau, la plupart des pays ne lui ont pas encore attribué de définition légale (Wall, 2007). A partir de ce point, nous allons invoquer quelques définitions édictées par différents Etats et d'autres proposées par des organismes tels l'ONU et l'OCDE.

Selon la Convention de Budapest du 23 novembre 2001, l'Europe définit la cybercriminalité comme étant l'« Ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la communication, ainsi que celles dont la commission est facilitée ou liée à l'utilisation de ces technologies ».

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

Aux Etats Unis, le terme « cybercriminalité » diffère selon les Etats membres et les départements de police. Effectivement, d'après le Département de la justice, la cybercriminalité est expliquée comme étant « une violation du droit pénal impliquant la connaissance de la technologie de l'information pour sa pénétration, son investigation ou ses procédures pénales ».

Quant au Code pénal de Californie (section 502), il limite la cybercriminalité à une liste d'actes illégaux qui se concrétise dans 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 ».

En revanche, le Code pénal du Texas (section 33.02) définit la cybercriminalité comme étant tout accès sans autorisation à un réseau, à un ordinateur ou à un système informatique.

Des définitions de la cybercriminalité ont été avancées au sein du 10éme Congrès des Nations-Unies selon lesquelles ce terme recouvre "toutes les formes d'activités criminelles conduites à partir d'un ordinateur dans l'espace d'un réseau local ou d'une entreprise, ainsi que d'un réseau plus large comme Internet", ou encore "toute infraction susceptible d'être commise à l'aide d'un système ou d'un réseau informatique, dans un système ou un réseau informatique, ou contre un système ou un réseau informatique".

Le terme de la cybercriminalité n'a pas été défini par la Tunisie. En revanche, le terme délit informatique a été délimité au niveau du code pénal par la loi n°99-89 du 2 aout 1999. Selon cette loi, la Tunisie définit le délit informatique comme étant tout

- Accès frauduleux dans tout ou partie d'un système de traitement automatisé de données.
- Destruction ou modification apportée, que ce soit intentionnellement ou pas, au fonctionnement du traitement automatisé.
- Introduction frauduleuse de données dans un système de traitement automatisé
- Altération des données que contient le programme ou son mode de traitement ou de transmission.
- Détention, utilisation de documents informatisés ou électroniques ou introduction de modification, de quelque nature qu'elle soit, sur le contenu de ces documents originairement véritables, à condition qu'elle porte un préjudice à autrui.

Il faut mentionner que selon cette loi, la tentative même est considérée comme un délit.

Les définitions proposées par l'OCDE et l'ONU mettent en avant le « comportement illégal ». En effet, ce terme englobe, selon l'OCDE, « tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou de transmission de données » et selon l'ONU, « tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent »

Il est à noter que ces définitions ne sont pas officielles mais plutôt fonctionnelles.

D'autres définitions du terme cybercriminalité ont été proposées par le monde scientifique, notamment par des universitaires, des experts en sécurité informatique et les utilisateurs, mais ils ne jouissent pas d'un accord unanime.

En effet, Schell & Martin (2004) définissent ce terme d'une manière très générale incluant tous les crimes en rapport à la technologie, à l' Internet et aux ordinateurs. Pareillement, la définition proposée par Yar (2013) comprend la totalité des activités illicites assistées par ordinateur. D'autres auteurs ont proposés des définitions sous plus de précision en se limitant aux activités nuisible et criminelles qui visent à acquérir ou à manipuler des informations pour parvenir à des gains personnels (Wall, 2007).

1. La cybercriminalité au niveau du secteur bancaire

Quel que soit le terme utilisé, la cybercriminalité réunit toutes les activités illicites réalisées à l'aide de l'informatique et de l'Internet et qui sont commises soit par la force en cassant les barrières sécuritaires d'entrées à un système, soit par la fraude en détournant les paramètres d'accès de ceux qui en ont droit soit par le leurre des systèmes et/ou des personnes.

Le développement des attaques mises en œuvre par les cybercriminels contre les banques et leurs clients suit un rythme soutenu. Nous avons parfois l'intention que nous assistons à un phénomène nouveau, mais réellement, ce ne sont que les techniques qui changent et se complexifient, quant aux domaines ciblés, ils restent bien identifiés : les systèmes d'information, les comptes bancaires et les moyens de paiements.

Systèmes d'information ;

La mise en réseau des données a accordé aux criminels « classiques » plus de facilité à trouver les informations qu'ils recherchent. Les attaques des cybercriminels peuvent revêtir

plusieurs aspects : changement de données fondamentales au niveau des systèmes d'information financiers; blocage de sites Web et notamment le vol de données stratégiques. Pour parvenir à ces fins, il existe d'innombrables programmes malveillants utilisées par les cybercriminels pour atteindre les systèmes d'information tels que :

- **Le virus informatique :** C'est un malware qui s'introduit dans les programmes ou les fichiers à partir desquels il peut se propager et semer les infections d'un ordinateur à l'autre. Certains virus se limitent à des effets légèrement dérangeants tel que l'affichage d'un message irritant, tandis que, en général, ils peuvent conduire à l'endommagement de matériels, de logiciels ou de fichiers.

  Parmi les malwares les plus récents on trouve ALICE et RIPPER. Ces logiciels malveillants permettent de voler énormément d'argent liquide à partir d'un DAB sans l'utilisation de carte bancaire et peuvent être installés soit sur le réseau des DAB ou sur le système d'exploitation de l'automate via un port USB ou encore par une carte malveillante afin de s'introduire dans le système d'information de la banque ciblée.
- **Le cheval de Troie :** C'est un programme malveillant qui se fait passer généralement pour un logiciel légitime permettant souvent aux cybercriminels d'intégrer les ordinateurs par des portes d'entrée clandestines afin de dérober des informations personnelles et confidentielles d'accès aux comptes bancaires en ligne, comptes de paiement électronique et cartes bancaires.
- **L'attaque en déni de service :** C'est une technique dans laquelle plusieurs systèmes informatiques provoquent la saturation d'une cible par d'innombrables requêtes, qui peut être un site Web ou un serveur par exemple, de sorte qu'il ne soit plus en mesure de répondre à toutes les requêtes reçues. Ceci peut bloquer ou rendre indisponible le système cible entrainant ainsi un déni de service temporaire pour les utilisateurs.
- **Le spyware** : C'est un programme qui installe un logiciel espion afin d'analyser les habitudes de la cible et expédier les informations recueillis sans que cette cible le sache.
- **Le ransomware :** C'est un logiciel informatique malveillant qui prends les données détournées en otage. Ce logiciel bloque et chiffre les fichiers de la cible et demande par la suite une rançon contre le déchiffrement de ces données.

Au cours des années et avec l'évolution des besoins, les systèmes d'information s'adaptent et se complexifient. En effet, durant la période d'installation, la méthode et la place du stockage transmission et traitement des données sont facilement identifiables. Mais, avec

l'introduction de nouveaux équipements et de nouveaux usages, l'identification d'une panne informatique ou d'une donnée compromise devient plus difficile. Chaque composante du système ainsi que les données utilisées devront être inventoriées afin de pouvoir répondre efficacement à un incident.

Comptes bancaires :

Plus les comptes bancaires ont de la valeur, plus leurs données attirent les cybercriminels. En effet, la valeur d'un compte bancaire dépend de différents facteurs, tels que le pays de résidence, la victime elle-même et notamment le solde bancaire.

Ces données confidentielles sont obtenues directement chez les clients et ce par divers moyens tel que le phishing[6] (par l'envoi de faux e-mails de banques les incitant à saisir leurs Coordonnées), les keylogger (logiciels installés sur le système de la cible consistant à mémoriser toutes informations tapées), les virus, les chevaux de Troie et bien évidemment la manipulation des clients trop naïfs.

Moyens de paiements ;

Avec le développement des moyens de paiement électroniques, les cybercriminels ont trouvé de nouveaux moyens d'atteintes aux biens des personnes. En effet, tous les moyens de paiements automatisés sont exposés au risque notamment les chèques et les cartes bancaires.

- **Chèque :** C'est un moyen de paiement encore largement utilisé qui se différencie des autres moyens de paiement scripturaux par son unique support papier et la signature du détenteur comme seul moyen d'authentification de ce dernier par sa banque et dont le coté électronique se manifeste au niveau de la compensation. Les seuls moyens d'utilisation frauduleuse de ce moyen de paiement sont soit par l'utilisation d'un chèque volé ou perdu, la contrefaçon en créant le chèque de toute pièce par le fraudeur qui sera émis sur une banque existante ou une fausse banque ou la falsification en altérant volontairement par grattage, gommage ou effacement de données sur un chèque régulier antérieurement intercepté.

[6] Phishing, c'est une technique qui repose sur l'exploitation non pas d'une faille informatique mais plutôt de la faille humaine en trompant les victimes par des e-mails contrefaits qui semble reçus de la part d'un tiers de confiance, typiquement un site de commerce ou une banque les invitant à se connecter en ligne par le biais de formulaires. Non averti, le destinataire divulgue des informations confidentielles telles que des informations d'identification de connexion ou des informations de comptes ou de cartes bancaires …

- **Carte bancaire :** C'est un moyen de paiement électronique faisant partie des méthodes de paiement dématérialisé, en d'autres termes, ne nécessitent pas l'usage d'argent liquide. Ce moyen de paiement constitue une cible potentielle des criminels. La fraude aux cartes bancaire pourrait être définie comme étant l'utilisation d'une carte par toute personne autre que son titulaire légitime. Les méthodes utilisées pour ce type de fraude sont :

  - L'utilisation d'une carte bancaire interceptée lors de son envoi par la banque au domicile de son titulaire légitime.
  - La contrefaçon d'une carte ; parmi les techniques utilisées on trouve :

Le fameux Skimmer pour l'écrémage de carte, un dispositif permettant de pirater et de cloner des données des cartes bancaires, d'une manière illégale, à travers les TPE, les DAB et les GAB. Ce dispositif peut être installé en interne dans un lecteur de carte bancaire ou en externe en reproduisant une partie ou toute la façade du distributeur automatique de billet ou du terminal de paiement. Une fois la carte bancaire insérée dans le TPE ou le DAB, le dispositif intercepte toute les données nécessaires. Ces informations, seront ensuite copiée sur une autre carte vierge pour être utilisées par le pirate au nom du détenteur du compte.

La technique du « papier d'aluminium » qui peut être utilisée sur n'importe quel TPE par un commerçant malhonnête, pour continuer à utiliser la carte de son client après la lui avoir rendue. Cette technique profite de deux failles du système de paiement par carte à puce, la première s'inscrit au niveau du type falsification et l'autre au niveau de la carte perdue ou volée. La première est basée sur l'interrupteur du TPE. En effet, en insérant une carte bancaire dans le terminal, un contacteur en laiton est bousculé vers un autre et tant que ce contact est maintenu, la transaction a lieu, elle ne prend fin que lorsque l'interrupteur revient en position initiale. Dès lors, il suffit tout simplement se maintenir ce contact après la restitution de la carte par son propriétaire, pour ce faire, les fraudeurs ont opté pour la mise en place de petits morceaux d'aluminium entre les deux têtes en laiton.

La bretelle c'est un système qui consiste à poser une bretelle sur la carte électronique du clavier de saisie du code confidentiel dans les TPE et les DAB permettant d'enregistrer tous les chiffres tapés par les clients.

- Utilisation d'une carte volée ou perdue :

La languette pour utiliser une carte à puce sans connaitre le code secret, le fraudeur utilise une languette de plastique et une deuxième carte dont il connait le code.

Cette technique fonctionne surtout sur les cabines téléphoniques, mais elle fonctionne aussi dans tous les terminaux de paiement avec la complicité du commerçant.

Le décryptage de la piste magnétique le code secret fait partie des données enregistrées sur la piste magnétique. Alors que les autres données sont en clair, le code est crypté avec une clé mathématique spécifique à chaque banque. Néanmoins, les fraudeurs disposant du matériel informatique nécessaire (ordinateur, lecteur de piste magnétique, programme d'encodage/ décodage) sont capables de le décrypter

La technique du « papier d'aluminium » Cette technique a le même objectif que la languette, utiliser une carte à puce sans connaitre le code secret. Selon le protocole de sécurité, le code secret n'est demandé qu'après la lecture et la mémorisation des informations d'authentification du porteur. Avec le procédé du papier d'alu, le fraudeur insère la carte et lors de la demande du code il la retire, trompé, le terminal demande toujours le code, le fraudeur insère alors une carte dont il connait le code. Le TPE valide la transaction avec les, coordonnées de la première carte.

- Détournement des données de cartes sur Internet :

Les données des cartes bancaires (numéro, cryptogramme, date d'expiration ...) sont détournées avec les même techniques utilisés au niveau des fraudes de comptes bancaire et utilisées en vente à distance par le fraudeur alors que la carte physique est toujours en possession du propriétaire. Ce type de fraude concerne la vente à distance.

2. L'histoire de la cybercriminalité au niveau secteur bancaire

Le secteur financier a toujours été l'une des cibles préférées des cybercriminels agissant à but lucratif. En effet, ces derniers vont où l'argent est, et bien évidement, les banques sont les plus susceptibles d'en avoir.

L'évolution de la cybercriminalité au niveau du secteur bancaire est simple à suivre et coïncide certes avec celle des technologies de l'information et de la communication, notamment, avec Internet. Au début, elle a commencé avec des simples « hacks »* afin d'exploiter des informations via des réseaux locaux, tel est le cas d'un caissier d'une banque locale de New York détournant plus de deux millions de dollars par la simple utilisation d'un ordinateur en 1973.Mais à fur et à mesure qu'Internet se développait, les attaques l'étaient aussi.

La prolifération des courriels a provoqué la première vague considérable de cybercriminalité et ce, vers la fin des années 80. Une série de logiciels malveillants et

d'arnaques ont été livrés aux boîtes de réception. L'arnaque du prince Nigérien reste le meilleur exemple à donner; « Salutations, je suis un prince descendant du Nigeria. J'ai besoin d'aide pour sortir des millions de mon pays, tout ce que vous avez à faire est de m'envoyer un peu d'argent pour configurer le transfert. Une fois terminé, je partagerai mes millions avec vous »

La vague suivante dans l'histoire de la cybercriminalité s'est manifestée avec le développement des navigateurs Web durant les années 90. C'était l'époque où le choix des navigateurs était beaucoup plus qu'aujourd'hui, dont la majorité étaient vulnérables aux virus. A chaque visite d'un site Web douteux, les virus était transmis via les connexions Internet. Certains provoquant la lenteur de l'ordinateur, d'autres l'apparition de publicités gênantes qui soit encombrent l'écran ou même redirigent l'utilisateur vers des sites inappropriés. C'est de cette façon que, selon la FBI, plus de 85% des entreprises américaines ont été piratées en 1997, entrainant des transferts financiers que la banque et le titulaire du compte ne le savent même pas.

Avec l'apparition des réseaux sociaux au début des années 2000, la cybercriminalité a vraiment commencé à s'intensifier. En effet, avec le volume énorme d'informations personnelles fournies par les utilisateurs de ces réseaux, le vol d'identité est devenu de plus en plus répandu. Ces bases de données volées ont servi à plusieurs fins tels que l'accès aux comptes bancaires ou l'établissement de demande de cartes bancaires ou de cartes de crédit.

La dernière vague étant la plus menaçante se caractérise par l'apparition d'une industrie criminelle mondiale. Opérant dans des gangs, les criminels sont devenus plus organisés. En effet, ils adoptent des techniques bien conçues et ciblent tout et tous quel que soit le niveau de sécurité fourni.

Les attaques contre le système financier par les cybercriminels ne sont pas nouvelles, mais l'année 2016 a été marquée par une amplification et une diversification de ces attaques. En effet, durant cette année, des banques du monde entier et également les banques centrales ont subi plusieurs attaques majeures engendrant des grandes pertes financières.

Parmi les banques les plus atteintes, la Banque Centrale du Bangladesh, ordonnant un transfert frauduleux, réalisé par des pirates suite à l'atteinte du code d'accès de cette banque au réseau SWIFT, d'un montant de 81 millions de dollars d'un compte américain vers une banque aux Philippines.

Cette attaque a été suivie par une dizaine d'autres similaires visant, parmi d'autres, une banque commerciale du Vietnam et une aux Philippines.

L'existence de failles facilement exploitables au niveau des systèmes bancaires est la raison principale de ces cyber-attaques. Parmi les zones les plus exposées à ce risque, les systèmes accessibles directement aux clients tels les applications mobiles et les sites Internet de plus en plus utilisés et, bien évidemment, les distributeurs automatiques de billets, les terminaux de paiement automatiques et les espaces clients qui représentaient depuis toujours une cible facile rapportant un gain financier important.

3. Les motivations des cybercriminels

Garantissant l'anonymat virtuel et minimisant le risque d'être détecté, les cyber-crimes attirent diverses personnes avec des motivations et des tactiques propres à chacun. Il est certes difficile de reconnaitre toutes les motivations des cybercriminels mais en gros, on peut discerner les trois plus répandues qui demeurent largement inchangées:

La motivation principale de la majorité des cybercriminels est le gain financier direct. Il consiste à voler des données, que ce soit des données bancaires en général et des informations sur les cartes en particulier ou de données confidentielles et critiques sur des établissements tel que les stratégies et les secrets industriels. Ces données seront par la suite revendues ou utilisées pour réaliser des fraudes.

L'espionnage peut être classé juste au-dessous du gain financier dans la liste des motivations des cybercriminels et peut être soit industriel soit étatique, pratiqué par un concurrent ou une puissance économique. Il s'agit réellement du vol des codes secrets et des accès confidentiels ou de l'attaque des systèmes d'information de la cible. Pour ce faire, des moyens plus sophistiqués sont utilisés. Selon Vincent Nguyen, l'espionnage est « Souvent pratiqué par les États pour espionner d'autres États ou des groupes internationaux, ces attaques, plus complexes à réaliser, nécessitent d'avantages de moyens financiers, matériels et humains ».

D'autres cybercriminels utilisent ces attaques pour nuire à des établissements par l'atteinte à son image qui peut être gravement touchée que ce soit par le blocage ou le sabotage

du site Internet ou bien en dégradant la confiance des clients par l'intensification des failles de sécurité.

4. Les types d'attaques des cybercriminels

Les techniques des fraudes cybercriminelles n'en manquent certainement pas, bien au contraire, elles sont assez nombreuses. Ces techniques peuvent être regroupées en deux grandes familles d'attaques ; des attaques de type technologique qui se composent à leur tour en attaques de masse et attaques ciblées et d'autres de type conventionnel.

Attaques de type conventionnel

Motivé par la cupidité, ce type d'attaque profite généralement de la confiance et de la crédulité des utilisateurs pour leurs demander des informations confidentielles et les utiliser plus tard de manière illégale. Plusieurs infractions dites conventionnelles existent, dont le nombre augmente continuellement, parmi lesquelles on peut citer l'extorsion de fonds, les menaces condamnables de type «vengeance», l'usurpation d'identités, l'abus de confiance et les escroqueries diverses, etc.

Ces attaques ne sont en effet qu'un ensemble des crimes et délits « traditionnels » transposés sur les réseaux numériques d'information et de communication.

Attaque de type technologique

Depuis son apparition, ce type d'attaque exploitant les vulnérabilités de l'outil informatique, a connu une forte évolution et une large diversification. L'attaque technologique vise essentiellement la confidentialité, l'intégrité et la disponibilité d'un système informatique ou une combinaison des trois. En général, pour ce faire, les pirates informatique se focalisent sur une des deux alternatives suivantes: les attaques opportunistes et les attaques ciblées.

Les attaques opportunistes, encore appelées attaques de masse, utilisent généralement des techniques peu sophistiquées qui ne visent pas directement des organisations ou personnes, mais qui se soucient plutôt d'atteindre le plus possible de victimes. Parmi les techniques les plus connues, on peut citer : L'« hameçonnage» (phishing) et l' attaque distribuée « distributed denial of service – DDoS »

Parmi les attaques distribuées les plus récentes on peut citer celles effectuée fin janvier 2018 suite à des révélations dans la presse sur le rôle des services secrets néerlandais dans la surveillance et l'identification d'un groupe de hackeurs russes de haut niveau. Visant les trois

plus grandes banques des Pays-Bas, à savoir ING, Rabobank et ABN AMRO, ainsi que l'équivalent local du Trésor Public, ces attaques sont parvenues à paralyser un temps leurs quatre sites Internet.

Ces attaques sont certes sérieuses, mais ne sont pas totalement sombres puisque la prise de contrôle sur les sites ne tarde pas trop, de plus, ces attaques sont très fréquentes ; « des milliers d'attaques par jour » assurait Klaas Knot le président de la banque centrale néerlandaise.

Contrairement aux attaques de masse, les attaques ciblées choisissent soigneusement leurs victimes et sont généralement difficile à neutraliser. Le choix et la connaissance de la cible ainsi que l'emploi de techniques plus ou moins sophistiquées rendent la mise en œuvre de ces attaques beaucoup plus compliquée. Dès l'introduction d' Internet, les cybercriminels n'ont cessé de faire évoluer leurs techniques et d'exploiter les lacunes des systèmes directement accessibles par les clients. Parmi les techniques d'attaque de masse les plus connues le Skimming et les malwares tel que ALICE et RIPPER. L'attaque de 2016 fait partie des attaques les plus connues de RIPPER, visant les DAB en Thaïlande, cette attaque a engendré plusieurs dégâts tel que la fermeture temporaire de tous les distributeurs de billets de la cible, le vol d'une bonne somme d'argent et la perte de confiance de ses clients...

Plusieurs autres techniques de fraude sont utilisées pour les attaques ciblées tel que les malwares très connus de type cheval de Troie largement utilisés pour récupérer des informations confidentielles des clients bancaires et qui n'arrêtent d'évoluer. Certains de ces logiciels malveillants sont développés spécialement pour les smartphones, bien évidemment, pour Android.

5. Etat des lieux de la cybercriminalité financière

Le développement du monde interconnecté présente certes plusieurs avantages au secteur bancaire, mais il présente également pas mal d'inconvénients notamment les attaques pour la fraude des services financiers qui devenaient de plus en plus tournées vers les comptes. Parmi les attaques les plus répandues nous trouvons le Phishing et les malwares financiers ainsi que la fraude aux moyens de paiement sur lesquelles nous allons présenter un bref aperçu basé sur les données collectées par Kaspersky Lab ; une société privée spécialisée dans la sécurité des systèmes d'information.

La fraude aux paiements a tellement pris de l'ampleur qu'elle devrait être traitée séparément. Figurant parmi les huit tendances de cybercriminalité de l'OCTA (Évaluation de la menace de la criminalité organisée) en 2016, la fraude aux paiements continue d'évoluer ainsi que les moyens utilisés pour cette fin. Les attaques logiques et malveillantes contre les distributeurs automatiques de billets ne cessent de croitre et de proliférer, attirant ainsi l'attention de nombreux cyber délinquants individuels et groupés dont la cible est l'infrastructure bancaire et les systèmes de paiement.

Concernant le choix au niveau des méthodes utilisées, il n'en manque certainement pas, après la manipulation des paiements par des cartes sans contact, les chercheurs de Kaspersky Lab ont découvert, parmi d'autres, des méthodes récentes d'attaque des systèmes des distributeurs automatiques de billets via des opérations à distance, de nouveaux logiciels malveillants, et un programme malveillant de ciblage DAB appelé « Cutlet Maker» disponible sur le marché DarkNet contre quelques milliers de dollars muni d'un manuel d'utilisation fournissant les instructions nécessaires pour accéder aux distributeurs.

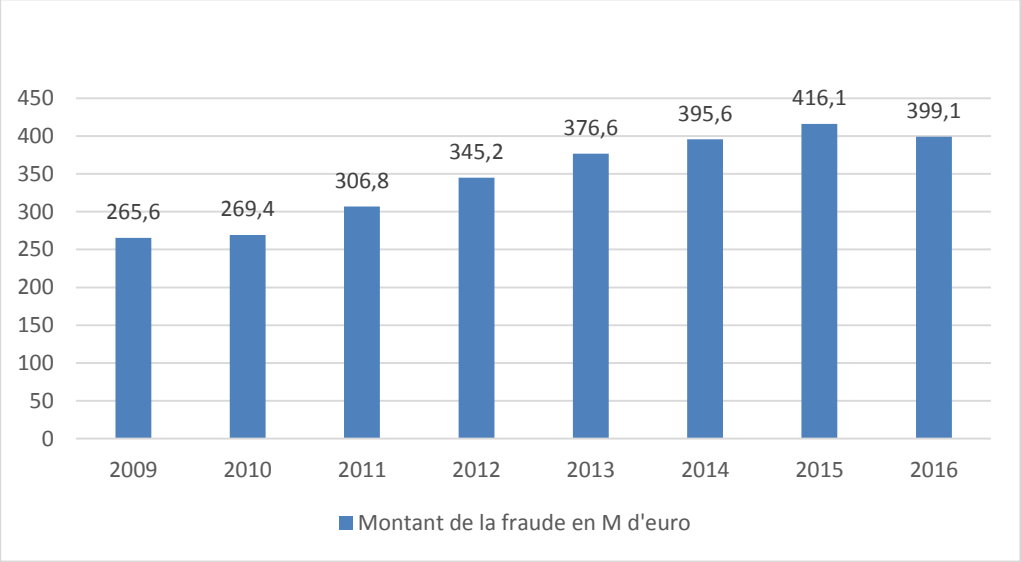
De tels systèmes ont rendu la cybercriminalité accessible même aux non-professionnels provoquant ainsi une augmentation énorme du nombre de cybercriminels.

Outre le nombre de cybercriminels, il est primordial de suivre le montant de la fraude des paiements. Au niveau de notre travail, nous allons prendre l'exemple de la France pour expliciter l'évolution du montant de ce type de fraude.

En France durant l'année 2016, la fraude sur les moyens de paiement scripturaux était de 800 millions d'euros concernant les paiement émis en France. Vu l'importance de son usage, la fraude à la carte bancaire s'est élevée à un peu près la moitié de ce montant (97 % en terme de volume), un tiers est attribué aux paiements par chèque, et le reste concerne les autres instruments de paiement (le virement et le prélèvement principalement)

Suite à une augmentation continue depuis 2004, le montant de la fraude sur les cartes de paiement émises en France a baissé de 4% pour la première fois en 2016 pour atteindre 399,1 millions d'euro pour un taux de fraude de 0.064% contre 416,1 millions d'euro pour un taux de fraude de 0.070% en 2015.

Figure 2:L'évolution de la fraude



Les opérations frauduleuses réalisés suite à l'usurpation de numéros de cartes continuent à gagner du terrain par rapport à celles réalisées suite au vol ou la perte d'une carte : effectivement, les paiements frauduleux à distance ont augmenté de 66.8% en 2015 à 70.1% en 2016 contre une part décroissante des paiements frauduleux par des cartes physiques volées ou perdues passant de 36.1% en 2011 à 29% en 2016.

L'amélioration constatée est sensible pour les trois grands types d'usage dont les taux de fraude enregistrent les niveaux les plus bas en 2016. Effectivement, le taux de fraude de paiement au niveau des points de vente était de 0,008%, de 0.029% dans le cadre d'un retrait et de 0.199% pour le paiement à distance ; un taux moyen de 0,037 % qui est également en diminution sensible depuis 2011.

Quant aux cartes de paiement sans contact dont l'utilisation est de plus en plus croissante, elles représentent un taux de fraude relativement stable de 0.020% dont la vulnérabilité technologique est quasiment nulle du fait que ce taux est uniquement dû au vol de la carte.

En se penchant sur la fraude subie par les transactions transfrontalières, nous constatons qu'elle diminue de 0.077% après huit ans d'augmentation continue, pour passer de 523 millions d'euros à 518 millions dont 182 millions provenant de fraude sur les transactions par cartes émises en France et réalisées à l'étranger et 118 millions de fraude sur les transactions par cartes

émises à l'étranger réalisées en France. Etant de 0.353%, le taux de fraude sur les transactions transfrontalières fut dix fois supérieur à celui des transactions nationales (0,037 %).

Expliquant cette baisse historique en matière de fraude de paiement, l'observatoire cite « la mise en place de moyens d'identification des transactions à risque et d'alerte au titulaire du compte, ainsi que le recours croissant à des mécanismes avancés d'authentification du payeur pour les transactions sur Internet ».

Concernant le Phishing, il existe plusieurs types parmi lesquels le Phishing financier qui représente, de nos jours, à peu près la moitié des attaques d'hameçonnage. Effectivement, d'après les constatations concernant les attaques de Physhing par Kaspersky Lab au cours l'année 2017, il y'a eu à peu près 25 millions de tentatives de consultation de plusieurs types de pages d'hameçonnage dont 53.8% des pages d'hameçonnage financier contre un pourcentage 47.5% en 2016 et 34.3% en 2015 soit une augmentation de 19.4 points en deux ans.

La catégorie « financière » du Phishing peut être décortiquée, selon Kaspersky Lab, en plusieurs types de pages de Phishing. Outre les banques, il existe les systèmes de paiements regroupant les pages qui imitent les différents services de paiements connus telle que Visa, American Express, MasterCard… les boutiques en ligne qui englobent les pages contrefaisant les boutiques en ligne tel Amazon, Apple store… et autres types de pages.

Figure 3:Part du Phishing financier

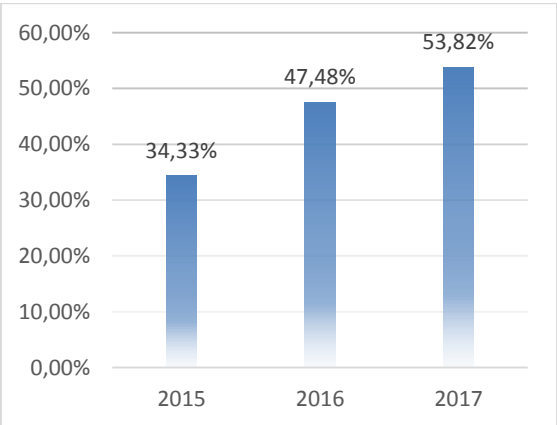
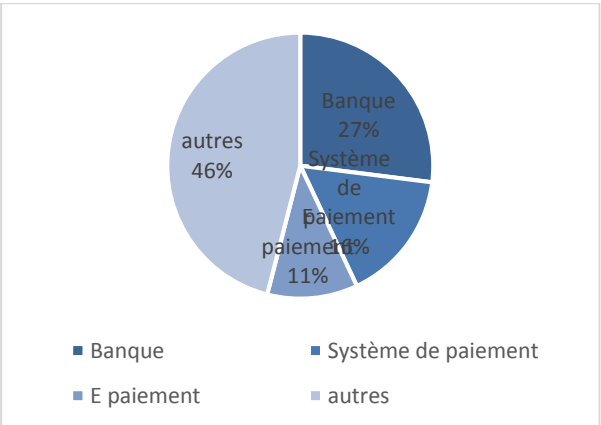


Figure 4:Composition de la part du Phishing financier en 2017



En 2017, enregistrant une augmentation au niveau des trois types principaux, la part du Phishing financier s'est composée de la sorte : 46% des attaques visaient les banques suite à une augmentation de 1.2 points par rapport à 2016, 27% visaient les systèmes financiers contre

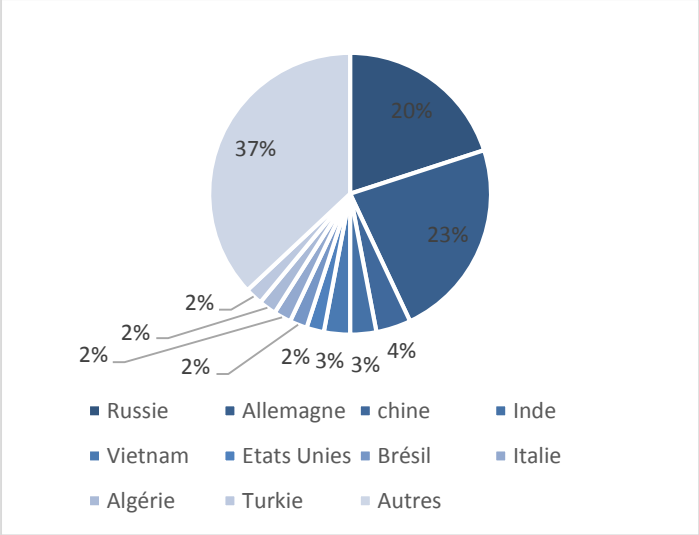
22.7% en 2016, 16% pour les boutiques en ligne avec 0.8 point d'augmentation par rapport à l'année qui précède.

En ce qui concernant les logiciels malveillants financiers développés spécialement pour intercepter les informations confidentielles d'identification nécessaires à l'accès aux comptes du système de paiement ou encore aux comptes bancaires en ligne, nous allons nous concentrer uniquement sur les chevaux de Troie bancaires.

Au cours de l'année 2017, le nombre d'attaques via des chevaux de Troie bancaires a enregistré une diminution de 30% par rapport à 2016 pour passer de 1 088 900 à 767 072 utilisateurs attaquées en 2017 dont 19% des utilisateurs professionnels.

En outre, cette technique d'attaques a des préférences en terme de pays, en effet comme le montre la graphique ci-après, plus de la moitié des attaques réalisées en 2017 se concentrent au niveau de dix pays seulement avec 23% des attaques contre les utilisateurs en Allemagne et 20% en Russie.

Figure 5:Cibles des logiciels malveillants bancaires



Le malware bancaire Android est une menace bien connue depuis des années qui a vécu une croissance explosive durant l'année 2016. En fait, le nombre d'utilisateurs ayant rencontré des logiciels malveillants Android a éclaté durant l'année 2016 pour atteindre 305 000 atteintes au total ; 5,3 fois de plus qu'en 2015. A partir de mi-Janvier, le nombre d'utilisateurs de logiciels malveillants Android attaqués a également commencé à augmenter à un rythme exponentiel pour passer de 3 967 attaques en Janvier à plus ou moins 75 000 en Octobre 2016 touchant en

particulier la Russie. Ce boom était causé spécialement par deux familles de logiciels malveillant connus sous le nom de Asacub et Svpeng.

Néanmoins, avec 2017 le changement de jeu est arrivé, le nombre d'utilisateurs de logiciels malveillants Android ainsi que la part d'utilisateurs attaqués ont commencé à diminuer de plus en plus, passant respectivement de 305 000 et 1,57% en 2016 à 259 828 et 1,01% en 2017.

Conclusion

Quels que soient leurs objectifs, ces attaques menacent la confidentialité, l'intégrité ou la disponibilité des données informatiques. Ces types d'atteintes à la sécurité informatique sont identifiés depuis longtemps et constituent la base de tous les dispositifs de protection. Les établissements financiers, les banques comme les assurances, y sont fortement sensibilisées. L'effort à fournir consiste donc principalement en la nécessité de s'adapter aux nouvelles techniques d'attaques recensées et d'anticiper les techniques encore plus sophistiquées qui pourraient suivre.

Chapitre 2 : Lutte contre la cybercriminalité

Introduction :

S'il existe une industrie qui devrait nous inquiéter le plus au sujet de la cybercriminalité et de la sécurisation des données, c'est celle à qui nous confions notre argent. Effectivement, l'industrie des services financiers présente des caractéristiques qui mènent à des menaces cybernétiques encore plus sérieuses, aussi bien en terme de gravité de leurs impacts qu'en terme de leurs probabilité d'occurrence. Bryan Hamman, responsable du territoire d'Arbor Network pour l'Afrique subsaharienne affirme cela en déclarant que « L'industrie des services financiers est constamment menacée par les cybercriminels et les méthodes qu'ils utilisent pour tenter d'infiltrer les systèmes de sécurité bancaire deviennent chaque jour plus sophistiquées ».

Commençant tôt l'informatisation de leurs métiers, les établissements financiers se trouvent de nos jours totalement dépendants des outils informatiques, qui peuvent s'avérer parfois dépassés et inadaptés aux nouvelles menaces. Au niveau de ce secteur, les systèmes utilisés sont le plus souvent multiples, décentralisés et énormément interconnectés ce qui exige

un suivi par des indicateurs de performance du niveau de protection qui devrait être beaucoup plus élevé que celles des protections classiques, obligeant ainsi les banques à développer constamment des dispositifs plus sophistiqués de détection d'attaques et de sécurisation et à toujours essayer de les perfectionner.

Nous allons scinder ce deuxième chapitre en deux ; au niveau de la première section, nous allons exposer différents moyens de lutte contre la cybercriminalité ; particulièrement les moyens techniques les plus utiles, les moyens légaux au niveau de quelques régions ainsi qu'au niveau international et les moyens humains via la sensibilisation. Dans un deuxième temps, nous allons présenter un moyen de suivi de la performance en sécurisation cybernétique notamment la notation en cyber-sécurité. Au niveau de cette deuxième section, nous allons décrire brièvement l'évolution de ce phénomène et son mode d'évaluation, exposer un panorama des agences de notation en cyber-sécurité les plus répandues ainsi que les avantages et limites de cette notation et en dernier lieu la réponse du secteur à ces limites.

Section 1 : Les moyens de lutte contre la cybercriminalité

Les défis rencontrant la sécurité informatique au niveau du secteur financier sont nombreux. Effectivement, il s'agit non seulement de protéger leurs bases de données internes, mais aussi de contrôler tous les points de contacts avec l'extérieur ; les distributeurs automatiques, les terminaux de paiement, les ordinateurs de leurs employés ainsi que ceux de leur clientèle pour arriver jusqu'aux objets connectés capables d'effectuer des paiements.

Afin de faire face à l'évolution de ces menaces, il faut avant tout assurer les fondamentaux du contrôle interne, car la cybercriminalité ne dépend pas seulement d'informatique et d'informaticiens compétents, elle utilise avant tout des moyens d'accès aux ressources informatiques que nous pouvons les juger de banales tels que l'accès aisé que ce soit aux locaux ou aux informations (numériques ou pas), les bureaux mal fermés, des activités laissées sans contrôle formel …

En second lieu, il faut assurer le « clos et le couvert informatique », en d'autres termes, la capacité de s'assurer du minimum vital en matière de sécurité tels que la protection du site Web, le type de données accessibles depuis Internet, la mise à jour régulière des applications, la mise en place et l'activation des firewalls et des antivirus …

Une fois ce niveau de sécurité est garanti, il est possible de penser à entrer en guerre avec les cyber-délinquants en s'armant par des moyens qui n'en manque certainement pas, parmi lesquels, les moyens techniques, légaux, humains et organisationnels que nous allons exposer ci-après.

Néanmoins, il faut mentionner qu'il n'existe pas de solution miracle pour remédier à ce phénomène, la lutte contre les attaques cybernétiques ne peut en aucun cas se limiter à une solution unique.

1. Moyens techniques de lutte contre la cybercriminalité

A ce stade-là, l'idée d'assurer « le clos et le couvert » ne se pose plus, ce qui importe c'est plutôt de s'assurer que les accès résisteront suffisamment à un pirate armé techniquement.

Plusieurs solutions **technologiques** ont été misent à la disposition des banques parmi lesquelles nous allons présenter celles les plus prometteuses selon Catherine Nohra China, fondatrice et présidente de B2Cloud (une entreprise spécialisée dans la conception et la recommandation de solutions Cloud) en terme de cyber sécurité.

1.1 L'hébergement Cloud et le Cloud Access Security Broker : CASB

Plusieurs banques, tel que la société Générale et la BNP, ont transféré partiellement leurs ressources informatiques vers un fournisseur pour les héberger et les gérer tout en apportant plus de ressources et de résilience, notamment vers le Cloud. En effet, grâce à cet hébergement les données sont sauvegardées plusieurs fois par heure sur les serveurs. Au cas où une panne se produit, cela ne se répercute ni sur la sécurité des données ni sur leur disponibilité.

A part l'élimination des logiciels encombrants et du matériel couteux grâce à l'équipement du fournisseur tiers, cette migration vers le cloud offre aux collaborateurs la possibilité d'accès à différents référentiels de données.

Néanmoins, ce transfert probablement lent et compliqué peut engendrer lui-même un risque de sécurité suite à l'accès d'une multitude d'applications et de dispositifs à ses ressources. D'où l'obligation pour ces prestataires d'hébergement Web d'investir continuellement dans la garantie de sécurité de données tel que la plateforme CASB implémentée entre les utilisateurs des services Cloud et leurs fournisseurs constituant ainsi un point de contrôle central ce qui permet une meilleure visibilité de toutes les applications Cloud.

1.2 La BLOCKCHAIN

La Blockchain est une technologie apparue en 2009 qui offre aux membres d'un même réseau la possibilité de réaliser, en toute sécurité et transparence, des opérations de stockage et de transmission d'informations sans organe central de contrôle. Par extension, une Blockchain se présente sous la forme d'un registre qui contient l'historique de toutes les transactions effectuées depuis sa création, regroupées dans des blocs ordonnés chronologiquement. Cette base de données est distribuée du fait qu'elle est partagée par les différents membres du réseau ce qui rend sa modification par un membre, sans l'accord de l'intégralité du réseau, quasiment impossible.

Disposant de qualités de sécurité intrinsèques, la Blockchain peut ainsi présenter un vrai instrument de lutte contre la cybercriminalité ; avec les bases de données à la fois décentralisées et distribuées proposées, elle assure une grande disponibilité du système, une traçabilité grâce à la conservation de toutes les transactions au niveau du registre ainsi qu'une protection intégrale des données par les mécanismes de validation mutuelle des modifications.

1.3 La Machine Learning

La machine Learning est utilisée dans un « cyber » contexte qui ne remplit actuellement que le rôle défensif. En effet, elle est apte à contribuer au niveau de la sécurité et de faire face à plus de 500 millions d'échantillons de malwares grâce à sa capacité d'auto apprentissage supervisé. On parle ici d'algorithmes ou de programmes qui s'appuient sur des règles prédéfinies ainsi que sur l'expérience pour apprendre et améliorer la qualité des résultats.

Le processus d'amélioration continue adopté par cette machine assure une adaptation à l'évolution continue des cyberattaques permettant ainsi non seulement une détection plus rapide des vulnérabilités, mais également, un accroissement des taux de détection des nouveaux types d'attaques étant indétectables avant, ce qui constitue un point fort en matière de sécurité.

1.4 Cryptogramme dynamique et biométrie

Le « **cryptogramme dynamique** » est une innovation signée Oberthur Technologies, un groupe spécialisé dans la sécurité numérique, qui vise à limiter le risque de fraude sur les paiements en ligne en remplaçant le cryptogramme statique; ce code à trois chiffres établi au dos de la carte par un autre dynamique. Réellement, ce cryptogramme affiché sur un mini-écran change toutes les heures grâce à une mini-pile incrustée dans la carte, d'une durée de vie équivalente à la durée de renouvellement de la majorité des cartes qui est de trois ans.

Selon ses concepteurs, l'adoption du cryptogramme dynamique permettrait une baisse de plus de 70% du total des fraudes à la carte bancaire, en effet, au cas où les coordonnées bancaires ont été volés, ils ne pourront plus servir après le délai de changement du code qui est d'une heure.

Une autre innovation a été développée dans le même but par PW Consultants, cabinet de conseil spécialisé dans l'ingénierie des moyens de paiement, en partenariat avec Télécom SudParis. Cette innovation est le système biométrique « talk to pay », service lancé par la Banque Postale, permettent quant à lui, le paiement en ligne par reconnaissance vocale au lieu de la saisie du code à trois chiffres. Concrètement, le client réclame d'être rappelé sur son smartphone par le robot vocal Talk to Pay, une fois authentifié, un cryptogramme est attribué à chaque paiement.

1.5 Big data

Le Big data est un système qui permet l'analyse de volumes énormes de données que les outils d'analyse classiques, notamment les méthodes statistiques traditionnelles, se trouvent incapable de traiter. Exploitant différentes technologies de traitement, le Machine Learning reste la technologie la plus compatible avec le Big data du fait qu'elle exploite pleinement le potentiel de ce système. En effet, le volume de données traité est beaucoup trop large pour des analyses compréhensives et il est quasi impossible aux analystes de pouvoir tester toutes les hypothèses et de dégager des out put pertinent à cause de l'innombrable relations qui existent entre les données.

2. Moyens légaux de lutte contre la cybercriminalité

A part les moyens techniques mis en place par les banques pour détecter et contourner les attaques cybercriminelles, il est nécessaire d'encadrer ce phénomène par des lois et autres textes juridiques. L'application de la loi est considérée comme l'un des principaux outils pour combattre la cybercriminalité du fait qu'elle peut fournir des informations précieuses sur les cybercriminels ainsi que leurs méthodes d'attaques, soutenir les enquêtes menées et surtout protéger les victimes par des politiques pénales. Réellement, les banques sont déjà soumises à pas mal de législations qui visent à lutter contre l'évasion fiscale, la corruption, le blanchiment d'argent et d'autres délits qui touchent énormément la santé économique des états. Faisant partie de ces délits, la cybercriminalité a été visée et la combattre implique par-dessus tout le renforcement des règlementations en matière de protection de données et d'analyse de risques.

Plusieurs organisations régionales et internationales ont élaboré des accords, des conventions, ou lignes directrices à ce sujet dont nous allons présenter une liste qui n'est certes pas exhaustive, mais qui comportera les travaux les plus intéressants.

- **La convention de Budapest :**

La Convention de Budapest sur la cybercriminalité du Conseil de l'Europe est considérée comme étant un outil juridique qui vise à harmoniser les lois nationales. En effet, elle mise sur une politique pénale commune ainsi qu'une coopération entre tous les Etats membres pour lutter contre la cybercriminalité. C'est le premier traité international à définir les différentes infractions pénales commises à travers Internet ou autres réseaux informatiques qui concernent la fraude informatique, les droits d'auteurs ainsi que la pornographie enfantine. Cet outil juridique comporte également une liste d'outils procéduraux, tels que l'interception de données informatiques et la perquisition de réseaux informatiques.

Même si ce traité est élaboré par le Conseil de l'Europe, il est important de noter qu'il dépasse les frontières européennes pour compter 67 signataires dont les Etats-Unis, l'Australie, le Japon, la Panama.

- **Le rapport « Orientations de l'OCDE pour les politiques sur le vol d'identité en ligne » :**

En 2008, l'Organisation de coopération et de développement économiques a publié un rapport intitulé « Orientations de l'OCDE pour les politiques sur le vol d'identité en ligne » présentant un aperçu sur la définition de ce phénomène, les méthodes qu'utilisent les voleurs d'identités, la définition et des recommandations pour le gouvernement et l'industrie pour combattre ce crime.

- **HIPCAR - Harmonisation des politiques, législation et procédures réglementaires en matière des TIC dans les Caraïbes :**

Le projet HIPCAR, intitulé " Amélioration de la compétitivité dans les Caraïbes au travers de l'harmonisation des politiques, législations et procédures réglementaires en matière de TIC » a été lancé en décembre 2008 par l'Union Internationale des Télécommunications (UIT) et la Commission Européenne (CE) avec la collaboration du Secrétariat de la Communauté des Caraïbes (CARICOM) et l'Union des télécommunications des Caraïbes (CTU).

L’objectif de ce projet consiste principalement à aider le CARIFORUM ; un sous-groupe du groupe des pays d'Afrique, Caraïbes et Pacifique comptant 15 pays indépendants, à harmoniser les politiques, la législation ainsi que les procédures en matière de TIC afin d’améliorer la protection de leurs utilisateurs à travers des modèles de lignes directrices politiques et de textes législatifs visant à harmoniser la législation en matière de cybercriminalité et de procédure pénale

- **La coopération dans le domaine de la sécurité de l'information internationale de l’Organisation de coopération de Shanghai (OCS) :**

L'Organisation de coopération de Shanghai (OCS) est une organisation internationale qui regroupe six pays membres à savoir la Chine, le Kazakhstan, le Kirghizistan, la Russie, le Tadjikistan et l'Ouzbékistan et intégrant officiellement en 2017 l'Inde et le Pakistan.

Les gouvernements des Etats membres de L'Organisation de coopération de Shanghai (SCO) ont conclu un accord sur la coopération dans le domaine de la sécurité de l'information internationale en 2009 et ont déclaré en 2012 que "L'OCS restera ferme pour lutter contre le terrorisme, le séparatisme et l'extrémisme, ainsi que la cybercriminalité internationale "

- **La convention arabe de la lutte contre la cybercriminalité de la ligue des États arabes :**

La Ligue des États arabes a adopté une convention de lutte contre la cybercriminalité le 21 décembre 2010 au Caire, en Égypte. S’imposant aux 22 États membres composant la ligue, cette convention fournit une politique pénale commune et permet de renforcer la coopération entre eux ainsi que de protéger la société arabe contre les délits informatiques.

- **Les directives de l'Union européenne sur les attaques contre les systèmes d'information :**

La directive 2013/40/UE du Parlement européen et du Conseil sur les attaques contre systèmes d'information et de remplacer une décision-cadre du Conseil. Cette directive adoptée le 12 août 2013 vise à renforcer la coopération entre États membres de l’Union Européenne et de rapprocher leurs droits pénaux en matière d’attaques contre les systèmes d'information par la mise en place de règles minimales en ce qui concerne les sanctions pénales applicables et la définition des conduites criminelles.

- **La recommandation BCBS 239 sur le contrôle bancaire défini par le Comité de Bâle :**

En janvier 2013, le comité de Bâle a publié le standard BCBS 239 « Basel Committee on Banking Supervision’s standard numéro 239 ». Enonçant 14 principes, ce document vise à

améliorer les pratiques ainsi que la capacité de production des reportings des banques pour parvenir à des reportings plus fiables et des données sécurisées de meilleure qualité.

- **Le Convention de l'Union Africaine sur la cyber sécurité et la Protection des données à caractère personnel :**

Suite à la réunion du 26 et 27 juin 2014, les 54 chefs d'Etat et de gouvernement membres de l'Union Africaine (UA), ont adopté la Convention de l'UA sur la cyber sécurité et la protection des données à caractère personnel.

Portant sur l'harmonisation et le renforcement du cadre juridique Africain en matière de cyber sécurité et protection des données à caractère personnel, la présente convention se charge de l'engagement des États membres dans l'édification de la Société de l'Information.

• Le Commonwealth - Rapport du Groupe de travail d'experts sur la cybercriminalité (2014) :

L'Initiative du Commonwealth sur la cybercriminalité réunit un groupe multidisciplinaires d'experts en cybercriminalité dont plusieurs organisations internationales tel l'Interpol, le Conseil de l'Europe, l'UIT et l'Organisation des télécommunications du Commonwealth, chargé d'examiner les répercussions des cyber-attaques sur le Commonwealth et de déterminer les meilleurs moyens de coopération et d'application internationale.

Finalisé en 2013, Colin Nicholls QC le président du groupe d'experts, a expliqué que « *Le rapport du groupe propose que les pays conçoivent des stratégies nationales qui incluent le développement et l'amélioration des lois en utilisant une législation type du Commonwealth sur les questions informatiques. Il propose également une amélioration de la coopération en matière pénale entre les pays et une stratégie pour renforcer les capacités, telles que les ressources, l'expertise des fonctionnaires, la coopération avec les prestataires de services et la formation de toutes les personnes concernées, juges, enquêteurs et procureurs...* "

Ce rapport a été adopté par des ministres du Commonwealth à Gaborone, au Botswana, durant la réunion du 6-8 mai en 2014.

- **Le Cybersecurity Tech Accord :**

Le Cybersecurity Tech Accord est un accord technique engageant plus que 40 entreprises mondiales signataires destiné à lutter contre les attaques informatiques. Le nombre de signataires est en croissance, en effet, en Juin 2018, deux mois après avoir annoncé cette initiative, onze entreprises ont rejoints l'accord.

Le texte de cet accord comporte quatre principes. Premièrement, l'engagement à protéger tous les clients et utilisateurs partout dans le monde. Deuxièmement, la conception de produits et services les résistants possibles. Troisièmement, promettre de ne pas collaborer avec des gouvernements attaquant des entreprises ou des citoyens via Internet. Et enfin, la collaboration entre les multinationales signataires pour aider les Etats à lutter contre la cybercriminalité.

3. Moyens humains de lutte contre la cybercriminalité

La cyber sécurité ne concerne pas uniquement les technologies et la législation mais aussi l'humain. La présence du facteur humain s'avère nécessaire pour maintenir un niveau de sécurité espéré. Parmi les fonctions les plus indispensables à la sécurité le RSSI (responsable de la sécurité des systèmes d'information) et l'audit de sécurité informatique.

Suite au changement fondamental de la nature des risques en lien avec les mutations qu'ont rencontré les Systèmes d'Information tel que l'ouverture aux réseaux et les différents domaines complémentaires traités, le rôle du Responsable de la Sécurité des Systèmes d'Information a évolué. Ne pouvant plus être un simple technicien, il est devenu chef de projet aux compétences organisationnelles, de conduite de changement et d'architecte de système d'informations, capable de coordonner sa mise en œuvre, tant sur le plan technique que sur le plan organisationnel ou juridique. Par ailleurs, le rattachement de cette fonction se différencie (à la DSI, à la DG, à la Direction Financière). En général, au niveau du secteur bancaire, le rattachement des RSSI se fait aux directions qui chapeautent les DSI mais pas au DSI lui-même, affirmant ceci, Jean-Paul Mazoyer, membre du comité exécutif du Crédit Agricole décrit "*Le RSSI est rattaché au niveau immédiatement supérieur au DSI, c'est à dire à un DGA ou à un* directeur des fonctions support qui a la compétence informatique dans son périmètre"

En effet, ce choix est dû au fait que si le RSSI est rattaché à la direction des systèmes d'information, il risque d'être à la fois juge et parti. Il doit à la fois appliquer les consignes du Directeur des Systèmes d'Information et auditer la direction, voire la critiquer.

Avec l'installation sauvage des applications souvent vulnérables, des failles exploitables par les cybercriminels se créent d'où la nécessité d'auditer régulièrement l'ensemble du système d'information permettant de garantir le bon fonctionnement des installations informatiques (matériels et logiciels) et ainsi connaitre le vrai niveau de sécurité des infrastructures. Un audit automatisé est capable de garder un certain niveau de sécurité dans le temps. Néanmoins, il reste primordial de faire appel à l'humain pour tester les systèmes. Un besoin auquel répondent les audits de sécurité.

Néanmoins, ce même facteur peut être considéré comme source de risque du fait qu'une simple erreur humaine mal intentionnée peut mettre en péril un système informatique aussi sécurisé soit-il. Or, toute entreprise peut être assimilée à un réseau de personnes d'où la nécessité de sensibiliser le personnel aux cyber risques et renforcer sa vigilance. Affirmant ceci, Jan De Blauwe, Président de la Cyber Security Coalition a dit : "En formant vos collaborateurs aux rudiments de la cybersécurité (cyberhygiène), vous pouvez déjà limiter un certain nombre de cyber risques." En effet, selon une étude faite durant le deuxième semestre de 2017 auprès de 403 entreprises Françaises, les incidents de sécurité proviennent essentiellement des employés actifs à hauteur de 63% suivies des fournisseurs et des partenaires avec un pourcentage de 15% et des anciens employés, 12%. Les employés des banques sont notamment les plus visés par les cybercriminels, comme le montre l'affaire Carbanak en 2015 où un groupe de délinquants sont parvenu à s'introduire sur les postes de travail des salariés de plusieurs banques situés dans plus de trente pays et ce à travers des e-mails personnalisés.

Face à un tel phénomène, il peut s'avérer important de proposer une formation de cyber sécurité pour une meilleure prise de conscience des risques cybernétiques par un panorama des menaces et leurs répercussions sur l'établissement concerné, des techniques des cybercriminels ainsi que des dispositifs de détection et de protection. Destinée aux non-informaticiens, cette formation peut présenter les fondamentaux de la sécurité informatique tel que le choix des mots de passe forts. Plusieurs études exposent les maladresses commises des salariés avec les mots de passe. Parmi ces études, une faite en 2016 en Belgique qui montre que presque la moitié des employés utilisent des mots de passe composés de moins de 8 caractères, qu'un tiers des Belges communiquent leurs mots de passes et qu'un quart entre eux utilisent le même mot de passe dans la vie professionnelle et privée. Miguel De Bruycker, directeur du Centre pour la Cybersécurité Belgique (CCB) a assuré que : "*C'est aux organisations elles-mêmes de sensibiliser leurs collaborateurs dans le domaine de la cyber sécurité. Et cette sensibilisation aura également un impact positif sur la protection de notre pays contre les cyberattaques."*

Afin de garantir un bon niveau de sécurité au sein d'une entreprise, un budget convenable doit être consacré à ce domaine, un spécialiste de la sécurité de la Société générale affirmant cela « entre 6 et 10% de leurs budgets informatiques est consacré à la sécurité quand les autres secteurs d'activité lui accordent 2 à 3% » et il a indiqué avoir multiplié par cinq ses investissements sur la sécurité informatique et ce, durant les cinq dernières années.

4. Moyens organisationnels

Grâce au développement des NTIC, il y'a eu introduction de plusieurs nouveaux services bancaires et accroissement important du nombre d'opérations traitées ce qui a poussé les banques à automatiser et à rationaliser les traitements pour garantir un meilleur service clientèle.

Qui dit automatisation, dit normalisation, effectivement, la normalisation demeure un axe d'innovation et de progrès au niveau des établissements bancaires notamment en matière de sécurité des Systèmes d'Information. La majorité des normes et standards, portant principalement sur le contrôle d'accès et la cyber sécurité, permettent de faciliter le management de la sécurité des données que ce soit financières, confidentielles ou soumises à la propriété intellectuelle.

Parmi ces normes les plus connus pouvant être imposées pour des raisons légales, de gouvernance ou exclusivement Marketing, notamment dans le monde bancaire, nous allons présenter quelques-unes dont l'exigence principale porte sur la sécurité de l'information, notamment, le RGPD, les directives ISO 27001, PCI-DSS

- **Le RGPD :** Le Règlement Général sur la Protection des Données (RGPD) n'est autre que la nouvelle loi régissant la protection des données privées des résidents européens depuis le 25 mai 2018.

  Ce texte vise à protéger tous les citoyens européens du fait qu'il recouvre pratiquement tout le processus relatif à leurs données personnelles, du recueil à la destruction. La spécificité de cette loi réside au niveau de son caractère extraterritorial, en effet, elle s'applique à toute organisme traitant des données de résidents européens partout dans le monde.

- **ISO 27001 :** C'est une norme établie par l'Organisation Internationale pour la Standardisation (ISO) permettant à une organisation de procéder à une amélioration

continue du système de management de la sécurité grâce à une description en détails de la détermination des objectifs et des dispositifs de protection ainsi qu'un suivi des risques identifiés, des mesures définies et des risques éventuels, assurés par des audits réguliers, et ce, même après la certification.Suite à la validation des audits réguliers, le devis de certification est délivré à l'organisation par un certificateur accrédité attestant que cette dernière a pris les précautions nécessaires pour la sécurisation des données sensibles et la prévention d'accès et de modification de toute personne non-autorisées.

- **PCI-DSS :** La norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) est un standard de sécurité mondial mis en place par les cinq plus grands réseaux de paiement, à savoir, Master Card, Visa, American Express, JCB et Discover afin de renforcer le contrôle des données des titulaires de cartes bancaires et des transactions émises afin de diminuer la fraude des instruments de paiement.

  Servant de référence aux exigences techniques et opérationnelles destinées à la protection des informations du titulaire, cette norme concerne tous les acteurs du traitement des cartes de paiement, notamment les banques, les commerçants, les sites marchands, mainteneurs et prestataires de services… ainsi qu'à tout autre acteur de stockage, traitement ou de la transmission des données du titulaire et/ou des données d'identification sensibles.

Section 2 : Agences de notation en cyber-sécurité

La cyber sécurité est une discipline qui souffre désormais d'une insuffisance d'indicateurs clés de performance ce qui rend le suivi de performance sécuritaire quasi impossible. En réponse à ce manque de repères, des agences de notation en cyber-sécurité ont vu le jour en apportant un nouveau service, notamment l'évaluation de la résilience des entreprises entre autres les banques.

L'explosion de la notation :

Selon François-Xavier Vincent, Directeur de la sécurité des informations et délégué à la protection des données à Oodrive, une agence de notation est un tiers neutre qui donne un avis ; une dotation basée sur des critères objectifs concernant le niveau de sécurité d'une entreprise pour ce qui est des agences de notation de cyber sécurité.

Pionnière en matière de services financiers, la notation atteint petit à petit tous les domaines tel que la gestion des ressources humaines et la responsabilité sociale et environnementale pour parvenir aujourd'hui à la notation en matière de cyber sécurité où elle propose à chaque fois un type de notation spécifique, en fonction des objectifs poursuivis.

Toutes ces agences de notation, quelle que soit leur catégorie et la nature de la structure notée, ont un objectif commun qui s'articule autour de l'évaluation et la notation à un intervalle régulier des entités via des procédures et des indicateurs et ce, suite à une demande, que ce soit interne ou externe, pour parvenir à apprécier les politiques ainsi que les stratégies menées par ces dernières. Pour ce faire, ces agences communiquent de l'information, sous forme de notes et/ou d'avis, qui doivent être à la fois crédibles, durables, transparentes et responsables.

Suite à l'explosion du risque cyber et afin de recréer la confiance au sein du marché, des agences de notation en cyber sécurité ont vu le jour tout d'abord aux États-Unis puis maintenant en Europe, avec pour mission l'évaluation de la cyber sécurité et d'apporter une certaine « assurance » aux membres du conseil et aux partenaires des entités notées.

1. Le fonctionnement de système de notation

La simplicité du principe de la notation en cyber sécurité repose sur le fait que la note attribuée par les fournisseurs les plus connus de ce service s'appuie sur un standard de mesure n'utilisant que des données librement accessibles au grand public, captables sans autorisation préalable. Ceci signifie par ailleurs que les organisations peuvent être notées sur leur sécurité

sans qu'elles le sachent. Les scores fournis prennent notamment en compte l'analyse de la vulnérabilité des applications web et la cadence de leurs mises à jour, la sécurité des terminaux, les fuites de données ainsi que le temps pris par l'entreprise pour corriger ces vulnérabilités. Il est à noter qu'il existe des fournisseurs qui proposent des outils de collecte de données internes pour approfondir encore plus la collecte de données et ce en facturant bien évidement une prime supplémentaire. Ces outils n'amélioreront pas forcément la note, mais garantirons assurément une précision supplémentaire.

Les agences de notations présentes dans le marché :

Pionnière en la matière, Bitsight s'est lancée dans le domaine de la notation de cyber sécurité en 2011 et est maintenant leader du secteur avec plus de 1 200 clients qui partagent leurs scores avec plus de 130 000 ce qui fait d'elle l'agence de notation de sécurité la plus utilisée.

Le domaine de notation sécuritaire a commencé, depuis 2015, à attirer de plus en plus l'attention du marché et des fonds d'investissement américains, en effet, multiple fournisseurs spécialisées dans ce service tel que UpGuard, SecurityScorecard et Cyriting se sont développées exclusivement aux Etats-Unis et en Europe, pour certaines d'une manière très rapide suite aux grosses levées de fonds réalisées.

A part ces plateformes de notation spécialisées en cybersécurité, on constate que les agences de notation classiques tel que Standard & Poor's, Moody's et Fitch commencent à intégrer le risque cyber dans les notations de solvabilité. En effet, Stuart Plesser, analyste de Standard & Poor's a indiqué « *nous appréhendons la cybersécurité comme une menace émergente qui a le potentiel de constituer un risque plus grand pour les institutions financières à l'avenir, et qui peut conduire à un abaissement de note* ».

Dans ce cas, l'intégration du risque informatique doit être pris en compte de la manière que d'autres risques exceptionnels tel que les catastrophes naturelles, et ce parce que, comme l'explique Jim Hempstead, directeur général adjoint de l'agence de notation Moody's, « *nous n'intégrons pas explicitement le risque cyber comme un facteur de crédit principal aujourd'hui, mais notre analyse de solvabilité fondamentale intègre de nombreux scénarios de stress-test, et un événement cyber pourrait être le déclencheur de l'un de ces scénarios* ».

2. Les avantages des agences de notation de cyber sécurité

Reposant sur des indicateurs techniques librement accessibles depuis l'extérieur de l'entité notée, les agences émettent une information transparente, objective, responsable et

crédible par le biais de scores et d'avis qui constituent plusieurs avantages clés que ce soit pour les agents internes ou externes aux entreprises notées, parmi lesquels nous allons citer ceux les plus exploitables.

2.1 Respect réglementaire

Dans un contexte réglementaire de plus en plus stricte concernant notamment la règlementation en matière de données personnelles, cette approche occupe un rôle important au sein des secteurs les plus régulés. Ceci explique la présence des banques parmi les premiers demandeurs de service des agences de notation en cyber sécurité.

L'exemple des réformes du RGPD exigeant aux organisations une évaluation régulière des mesures sécuritaires est le meilleur exemple qui puisse expliciter le rôle de ces agences.

2.2 L'amélioration et le suivi de ses performances

Les cotes attribuées par ces agences constituent un vrai apport au plan opérationnel pour assister et améliorer ses performances sécuritaires dans le temps. Concernant le plan stratégique, les notes fournissent des indicateurs de performance en matière de cyber sécurité, grâce auxquels, les responsables sécurité peuvent démontrer d'une manière claire et simple leurs progrès, de justifier leurs budgets et même argumenter une augmentation auprès du comité exécutif.

2.3 Moyen de comparaison

Avant la notation de cyber sécurité, les équipes de gestion du cyber risque ainsi que les responsables des programmes de cyber sécurité n'avaient pas accès à l'analyse comparative vu la rareté des comparables et des métriques au sein de ce domaine.

Effectivement, les scores représentent les premiers outils, facilement compréhensibles par tous, qui permettent les entités notées de se positionner dans le marché par rapport à ce critère et à identifier les pratiques efficaces en matière de cyber sécurité.

2.4 La maitrise du risque fournisseur

Avec le phénomène d'externalisation croissant des entreprise et les menaces qui ne cessent d'apparaitre chaque jour, le risque fournisseur devient de plus en plus répandu. Et par fournisseur, nous désignons toute personne responsable d'une opération externalisée allant de celui s'occupant des médiats sociaux et la compagnie d'entretien ménager aux fournisseurs des services Cloud et des services de comptabilité.

Ayant accès aux données et systèmes appartenant à une entreprise, les fournisseurs attirent de plus en plus les cybercriminels pour devenir même un de leurs canaux d'attaque privilégiés. Afin d'éviter ce risque, plusieurs ont choisi de surveiller les performances de sécurité de leurs fournisseurs à travers les notes attribuées par les agences de notation en cyber sécurité.

2.5 L'évaluation d'une cible dans un processus de fusion-acquisition

L'évaluation de la cible constitue la première étape de toute opération de fusion acquisition. Tous les types de risque sont pris en compte au cours du processus de diligence, allant des risques financiers aux risques juridiques, néanmoins, les cyber-risques sont souvent laissées pour compte, malgré leur importance, à cause leur complexité. En effet, selon une étude récente réalisée par le cabinet d'avocats Freshfields Bruckhaus Deringer,83% des personnes interrogées pensaient que l'opération peut être annulée si la cible a déjà été la victime de cyber-violations et 90% d'eux pensaient que ces violations peuvent abaisser la valeur d'une acquisition potentielle. Vu leur importance, les intervenants à ce type d'opération se sont tournés vers les services des agences de notation du cyber risque permettant une visibilité continue de l'état sécuritaire de la cible.

3. Les limites de la notation en cyber sécurité

Le recours à la notation de cyber sécurité, dont les bénéfices sont bien concrets et les champs d'utilisation sont de plus en plus variés, est devenu graduellement indispensable. Néanmoins, elle n'en dispose pas moins de limites desquelles il faut être conscient.

3.1 L'aspect « boite noire » des évaluations

Pour être judicieuse, la note doit avant tout être établie selon un processus compréhensible et claire en termes de données utilisées, d'indicateurs et de pondération appliquées. Or, avec des algorithmes, constamment mis à jour, propres à chaque agence et des données qui évoluent dans le temps, la note de cyber sécurité attribuée est notamment de genre « boite noire » ce qui suscite la méfiance.

Assurément, cette note risque d'être incohérente dans le temps et surtout invérifiable. L'Out Put de ces agences peut être une source problématique du fait qu'elles sont susceptible de changer soudainement suite à une mise à jour du processus d'évaluation ce qui

peut impacter directement les modèles de gestion des risques des demandeurs du service ainsi que ceux des entités notées. Pire encore, elles peuvent même toucher à la réputation des organismes évalués, influencer ainsi le classement des entreprises en terme de cyber-sécurité d'où un pouvoir de manipulation du choix d'une entité au détriment d'une autre.

3.2 Service intrusif

Vu que la notation d'une entreprise en cyber sécurité peut être basée que sur des données librement accessibles de l'extérieur, les services de ces agences de notation peuvent être perçues comme extrêmement intrusives par les organisations incapables de refuser la notation de leurs performances sécuritaires. En revanche, en cas d'opposition, l'organisation peut uniquement « faire appel » de sa note et réclamer une réévaluation réalisée généralement par un membre extérieur neutre équivalent à un arbitre.

3.3 Les agences de notation : la nouvelle cible préférée des cybercriminels

Les agences de notation peuvent constituer un vrai risque de confidentialité, non pas sur les scores, mais plutôt sur les données techniques nécessaires à l'élaboration de la note. C'est vrai que ces données sont librement accessibles, mais, leur concentration en un seul point faciliterait la tâche à un cybercriminel qui réussirait à y accéder en lui permettant de disposer d'une véritable cartographie des vulnérabilités d'une organisation.

Ce qui pourrait empirer encore plus les choses, l'ajout des données internes plus délicates aux données techniques nécessaires à l'évaluation de la résilience des entreprises et ce volontairement fournies par ces derniers afin d'améliorer leurs notes et décrocher tel partenariat ou contrat.

3.5 Comparaison logique que pour les organisations comparables

Les notes comptent parmi les premiers moyens de comparaison en matière de cyber-sécurité certes, mais ce rapprochement peut ne pas être pertinent du fait qu'il essaye de comparer l'incomparable. En effet, la comparaison ne peut être judicieuse, logique et utile qu'entre organisations comparables que ce soit en terme de secteur d'activité, de taille, de surface d'exposition etc.

4. Les bonnes pratiques des agences de notation en cyber-sécurité

Afin de contourner ces limites et maximiser l'utilité des notations attribuées, les fournisseurs de ce service doivent gagner la confiance des consommateurs en les persuadant que les évaluations se basent sur des informations exploitables et pertinentes selon un algorithme compréhensible et bien articulé. Pour atteindre cet objectif, la notation doit respecter un ensemble de principes.

C'est la raison pour laquelle il y'a eu un processus de collaboration, une quarantaine sociétés membres de la Chambre des États-Unis ont travaillé en collaboration avec les principales agences de notation en cyber-sécurité pour élaborer un certain nombre de principes et de bonnes pratiques, que nous allons présenter ci-après, qui visent à renforcer la confiance et faciliter encore plus leur utilisation.

4.1 Transparence

Afin d'améliorer les notations, les agences de notation doivent assurer une transparence suffisante au sujet de leurs méthodologies, processus et données utilisées et intégrées aux cotes de sécurité et si possible, être ouverts avec les demandeurs du service de notation ainsi que les entités cotées sur la manière dont les évaluations sont obtenues.

Par ailleurs, toute entreprise notée doit avoir le pouvoir d'accès à son évaluation et aux informations ayant une incidence sur la rectification de sa note.

4.2 Litige, correction et appel

Les entreprises qui s'estiment mal notées ont le droit de contester correctement et facilement leurs évaluations et d'avoir en retour soit des données corrigées ou bien clarifiées. Les agences de notation devraient être en mesure de remettre en question leurs out put et de les examiner par un processus d'appel et de règlement de litiges claires. Les évaluations contestées doivent rester comme telles jusqu'à résolution.

4.3 Exactitude et validation

Les évaluations fournies par les agences de notations doivent être fondée sur l'expérience et l'observation, axées sur les données ou notées selon l'avis d'un expert. En outre, ces sociétés de notation doivent valider leurs performances historiques de leurs modèles ainsi que leurs méthodologies de notation par un tiers. Bitsight, leader de marché, est bien la

seule parmi ses concurrents à valider par un tiers la corrélation entre les violations et les évaluations.

4.5 Gouvernance du modèle

Afin de suivre le dynamisme des cyber menaces et d'affiner encore plus les notes, les agences de notation en cyber sécurité mettent à jours leurs algorithmes menant notamment au changement des notes des entreprises ce qui peut les irriter.

Pour éviter cela, et préparer les clients aux mises à jours, les sociétés de notation doivent aviser convenablement leur clientèle avant d'apporter toute modifications à leurs processus d'évaluation et annoncer explicitement les conséquences de ces modifications sur les notes existantes et pourquoi pas aller plus loin en leur proposant des conseils de correction.

4.6 Indépendance

L'indépendance présente une des normes dans la cote de sécurité. Tous le personnel d'une agence de notation doit veiller à la qualité des notes en cyber-sécurité, sans influence ni interférence. Le fait qu'une entreprise soit cliente ou pas de la société de notation, ne doit pas avoir d'impact sur la notation ni sur le droit de contester les résultats; toute entité notée doit être en mesure de consulter et de contester leur note.

4.7 Confidentialité

Toute agence de notation doit respecter une politique de divulgation responsable ; les données collectées auprès d'une entreprise que ce soit pour une évaluation ou une contestation doivent être dotées d'une protection appropriée. Toute information délicate et confidentielle, capable d'emmener à des compromissions du système, ne doit pas être fournie par les fournisseurs de notation à des tiers.

Conclusion

La cybercriminalité peut toucher la réputation, induire à d'importantes pertes financières, ou encore à rendre des services indisponibles ce qui explique bien l'importance de la filière cyber sécuritaire. Hétérogène et décentralisée, cette filière est généralement le résultat de choix spécifiques aux besoins de chaque entreprise qui traite les risques encourus un par un. Néanmoins, seule, une banque, entreprise et même un pays est incapable de lutter contre ce phénomène, d'où le besoin de faire évoluer les mentalités vers la coopération afin de renforcer le système de lutte contre la cybercriminalité.

Il existe bien des mécanismes de coordination entre les Etats et un effort considérable de la part des instances réglementaires et gouvernementales ainsi que des mesures de détection et de défense d'ordre technologique et réglementaire qu'il faut juste utiliser pleinement en parallèle avec les formations de sensibilisation du personnel non-spécialistes qui causent la majorité des défaillances.

Afin de mener à bien le programme de lutte contre la cybercriminalité, il faut avoir des moyens de suivi et des indicateurs de performances de matière de cyber-sécurité, les notes fournies par les agences de notation spécialisées en cyber-sécurité remplissent bien ce rôle. Effectivement ces notes constituent un appui pour la collaboration des entreprises ainsi que pour des échanges productifs en matière de sécurité, chose que les entreprises n'étaient pas en mesure de faire au préalable. Afin d'assurer cette fonction et gagner la confiance de ses clients, les agences de notation en cyber-sécurité doivent promouvoir la précision, la qualité et l'équité dans leurs rapports d'évaluation, être en mesure de mettre en question leur contenu déclaré d'apprécier les fautes commises et garantir la confidentialité dans la divulgation des notes, d'où la divulgation « Principes pour des cotes de sécurité justes et exactes » par la Chambre de commerce des États-Unis.

Si les agences de notation appliquent ces principes et bonnes pratiques et les placent au cœur de leur activité, les notations de cyber-sécurité continueront à gagner de l'intérêt pour devenir aussi importante que les notations financières dans la prise de décisions d'accords partenariats et autres décisions commerciales.

Chapitre 3 : La cybercriminalité en Tunisie

Introduction

Face au développement rapide des technologies de l'information et de la communication, les pays en développement, notamment la Tunisie, se sont penchés sur l'accélération de la modernisation de leur économie dans le but de combler le fossé numérique avec les pays développés. L'Etat Tunisien a conçu pour ce fait un plan national stratégique qui vise à mettre en place le cadre ainsi que les infrastructures technologiques nécessaires au développement de ce secteur d'avenir.

En effet, le secteur du numérique présente un vrai gisement de croissance pour l'économie tunisienne du fait qu'il permet d'augmenter son degré d'innovation et de compétence et de garantir le travail aux diplômés de l'université et ce sans compter sa contribution dans l'augmentation du niveau de la compétitivité des entreprises en général et des banques en particulier.

Au niveau de ce chapitre nous allons, dans un premier lieu, donner un état des lieux de l'intégration des TIC en Tunisie ainsi que leur utilisation au niveau du secteur bancaire. Ensuite nous allons présenter quelques attaques cybernétiques contre les banques Tunisiennes. Et enfin exposer le cadre juridique et les moyens organisationnels de lutte contre ce phénomène.

Au niveau de la deuxième section, nous allons nous focaliser sur la réalité des banques tunisiennes par l'étude et l'analyse d'un questionnaire élaboré par nos soins qui concerne en premier lieu, le niveau d'introduction des TIC au niveau de chaque banque, en deuxième lieu l'ampleur du phénomène de la cybercriminalité, et enfin le degré d'outillage des banques en matière de protection et de sécurité cybernétique.

Section 1 : La Tunisie face à la cybercriminalité

1. Etat des lieux en matière de TIC en Tunisie

Etant un secteur prioritaire, la Tunisie vise, depuis 1980, à renforcer le secteur des technologies de l'information et de la communication (TIC) à la fois en tant que vecteur d'amélioration de compétitivité, de modernisation et de développement des autres secteurs économiques mais aussi en tant que secteur économique à part entière, permettant de créer de la richesse ainsi que des emplois à forte valeur ajoutée.

Effectivement, dans le cadre du plan stratégique national « Tunisie Digitale 2020 » visant à instaurer un tissu d'entreprises compétitives et innovatrices faisant du pays une référence dans le domaine du numérique au niveau internationale, la Tunisie possède aujourd'hui 18 cyberparks totalement consacrés à la recherche et à la formation scientifique et technologique ainsi que trois technoparks orientés TIC.

Selon les statistiques élaborées par l'Institut National de la Statistique (INS) durant l'année 2016, le tissu se compose de mille huit cents entreprises privées, deux cents dix-neuf centres de services partagés, huit centres de développement servant des multinationales contribuant ainsi à 7.2 % du PIB et employant quelques quatre-vingt mille personnes.

En ce qui concerne l'utilisation des TIC, selon la même source, l'année 2016 a enregistré une densité téléphonique de 98,8 lignes pour 100 habitants avec plus de trois millions d'internautes suivant une évolution de 38% par an. Quant à l'accès des familles aux TIC, ça a évolué de 20% durant l'année 2017 avec un accès à Internet passant de 37.5% en 2016 à 44,5% en 2017 selon les chiffres avancés dans un communiqué de presse par le ministère des Technologies de la communication et de l'Economie numérique.

Figure 6 : Propositions des ménages connectés à Internet

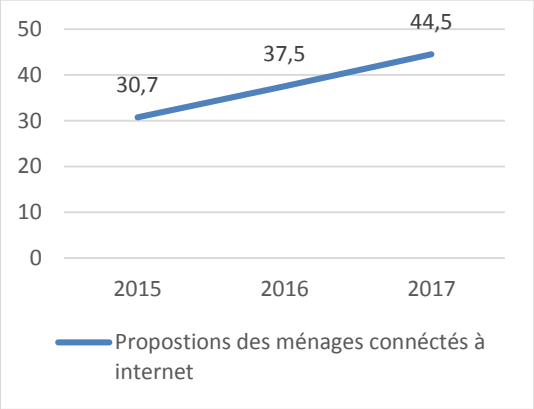
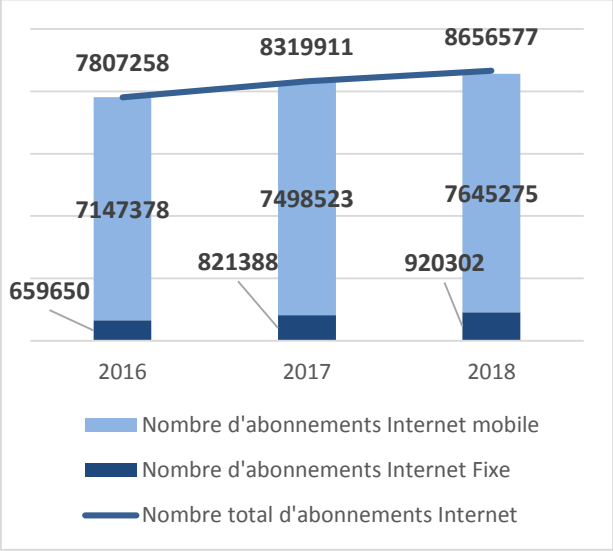


Figure 7: Nombre d'abonnements au réseau Internet (en milliers)



Les chiffres publiés par le ministère invoquent de même une croissance de 12% du taux des usagers d'Internet pour atteindre 55,5% contre 49,6% en 2016. Cette croissance est soutenue par l'augmentation du nombre d'abonnements au réseau Internet que ce soit fixe ou mobile d'une année à l'autre.

L'usage d'Internet sur les équipements mobiles est nettement supérieure à celle sur les équipements fixes vu le nombre d'abonnement au réseau Internet mobile qui représente au fil du temps plus ou moins 90% du nombre total d'abonnements.

- **<u>Les TIC dans le secteur bancaire Tunisien :</u>**

« Tout le monde s'accorde pour dire qu'un des secteurs les plus affectés par les nouvelles technologies financières étant en premier lieu le secteur bancaire » affirme Monsieur Ahmed EL KARM, Président de l'APTBEF. Effectivement, les banques dans leur ensemble jouissent à plein des avantages des nouvelles technologies de l'information et de la communication, et ce ne concerne pas seulement la qualité et la rapidité des services mais aussi celle des opérations entre les différentes agences et avec l'étranger. Les nouvelles technologies touchent de même l'organisation des services ainsi que dans la gestion des institutions financières.

Suite à une consultation approfondie faite par la banque centrale de Tunisie en 1996 dans le cadre de la libéralisation de l'économie, le système bancaire s'est lancé dans plusieurs projets stratégiques de modernisation dont l'étude a été réalisée par des spécialiste sous le pilotage de la BCT. Ce programme de modernisation vise principalement à soutenir la

concurrence des banques étrangères qui, selon l'exigence de l'Organisation Mondiale de Commerce, commenceront à s'installer à partir de 2004 et ce par la mise en conformité des prestations avec les standards internationaux.

Parmi les projets de modernisation mis en place par la Tunisie, nous allons présenter ceux mis en place au fil du temps, qui sont devenus indispensables à l'activité du secteur - bancaire.

- **Système de la Télécompensation :**

Le système tunisien de télécompensation interbancaire a été mis en place le 1er Novembre 1999 avec la création de la Société interbancaire de télécompensation (SIBTEL), fixant comme objectif principal la dématérialisation des supports de crédit notamment les effets les chèques, les virements et les prélèvements et la réduction des délais d'exécution qui en 9 Mai 2011 ont achevé leur migration vers la version des 24 heures.

Ce système surveillé par la BCT et dont la gestion est confiée à la SIBTEL, assure l'échange électronique des valeurs à compenser, le traitement de ces valeurs au moyen d'un centre de calcul des soldes de compensation ainsi que la préparation des situations nettes des différentes institutions adhérentes, à savoir, la BCT, les établissements bancaires de la place et la Poste. Par la suite, la SIBTEL centralise les données informatiques relatives aux valeurs télécompensées, et procède à l'archivage électronique des images scannées de ces valeurs pour toute consultation ultérieure par les adhérents.

Grâce à l'automatisation et l'unification de la chambre de compensation, les institutions adhérentes jouissent d'une sécurité supplémentaire des paiements et d'une amélioration de la qualité des informations transmises.

- **Système de la Monétique :**

La monétique est le domaine qui regroupe la monnaie électronique, les transactions bancaires électronique ainsi que les systèmes et moyens de paiement électronique. En Tunisie, le système de la monétique a été conçu en 1989 autour d'un ensemble de moyens et de traitements électroniques, informatiques et télématiques permettant la gestion des transactions monétiques sécurisées par cartes bancaires et des transactions associées. En fait Monétique Tunisie est une société qui s'est spécialisée dans la conception, l'intégration, l'exploitation et l'infogérance de solutions monétiques.

L'évolution permanente des moyens de paiement, la diversification des services bancaires dans le monde et notamment la recherche continue d'une meilleure sécurité des transactions par carte ont incité les opérateurs tunisiens à suivre cette évolution. Pour ce faire le système de la monétique a opté pour la migration vers la carte à puce par l'adoption de systèmes compatibles aux normes internationales au niveau du domaine de cartes à puce et il s'est mis en conformité avec le standard PCI DSS (Payment Card Industry Data Security Standard) dont la démarche consiste à sécuriser les données relatives aux cartes durant toutes les étapes de la transaction et ce afin de répondre aux nouvelles méthodes criminelles et renforcer la confiances des porteurs de cartes

L'activité de Monétique Tunisie s'est beaucoup développée durant la période 2010-2016. En effet, au cours de cette période, l'utilisation des cartes bancaires avait enregistré une hausse de 450% et elle a continué à évoluer pour atteindre les 3 818 887 cartes émises en Juin 2018, 2649 distributeurs automatiques de billets (DAB) et à peu près 18569 commerçants équipés de terminaux de paiement électronique (TPE) en cette même date selon les statistiques de l'Association Professionnelle Tunisienne des Banques et des Etablissements Financiers (APTBEF).

- **SWIFT.NET :**

SWIFT(Society for Worldwide Interbank Financial Telecommunication) est un outil de transmission des ordres de paiement interbancaires mondiaux. Mis en service en 1977, cette plate-forme de messagerie approuvé et utilisé par plus de 11 mille institutions financières dans environ 200 pays et territoires du monde entier a su décrocher sa place et s'imposer comme un standard de la communauté financière internationale garantissant l'échange clair et facile des données entre les institutions tout en maintenant un heut niveau de sécurité.

Les banques tunisiennes ont réussi leur migration vers le nouveau réseau de « SWIFTNet » et ont officiellement entamé la phase d'exploitation normale de nouveau système à partir d'août 2004 pour arriver à traiter aujourd'hui environ de 3 813 339 messages par an.

- **Système de paiement brut :**

Dans le cadre du programme de modernisation du système bancaire, la Banque Centrale Tunisienne a mis en place en Novembre 1987 le Système de Virements de Gros Montant Tunisien (SGMT) géré par elle-même; un système qui constitue une infrastructure de transfert automatique de fonds en temps réel permettant d'effectuer des paiements rapides et hautement

sécurisés entre les institutions financières participantes pour leurs propres comptes ainsi que pour le compte de leurs clients et ce à partir de 100 000 dinars.

Selon la Banque Centrale Tunisienne, le SGMT traite aux alentours de 722 paiements par jour d'une valeur de 3,255 Milliards de Dinars.

- **Centrale d'information :**

La centrale d'information et des impayés, a été mise en place par la Banque Centrale Tunisienne pour un double objectif de transparence et d'aide à la décision des banques Tunisiennes dans leur activité courante.

Ces centrales fonctionnant en temps réel et dont l'alimentation se fait via le Système d'Echange de Données (SED) regroupant toutes les banques de la place, se présentent sous forme de bases de données qui contiennent toutes les informations nécessaires sur les clients des banques tels que l'identité, la classification des créances, la situation des impayés, les bilans etc.

2. La cyber-sécurité

2.1 Cadre juridique et réglementaire

La majorité des textes qui traite de sujet de la cyber sécurité ont vu le jour entre 1999 et 2005 en parallèle la libération du secteur des TIC. Ce mouvement législatif constitue la base pour la création de structures dynamiques et le développement d'une expertise technique assez riche.

En fait, le cadre juridique tunisien comprend des lois fixant les règles générales de protection dans différents domaines à savoir la loi n° 2004-5 du 3 février 2004 relative à la sécurité des systèmes informatiques et des réseaux, la loi organique n° 2004-63 du 27 juillet 2004 qui porte sur la protection des données à caractère personnel, la loi n° 2000-83 du 9 août 2000 concernant les échanges et le commerce électroniques (certification et signature électronique), la loi n° 2005-51 du 27 juin 2005 portant sur le transfert électronique de fonds et la circulaire n°19 publiée par la BCT le 11 avril 2007 qui se soucie du renforcement des mesures de sécurité informatique dans les établissements publiques. Le secteur des télécommunications a aussi été sujet de réformes juridiques, en fait, le Code des Télécommunications (CT) a été promulgué par la loi n° 2001-1 (15 janvier 2001), la loi n° 2002-46 (7 mai 2002), la loi n° 2008-1 (8 janvier 2008) et enfin par la loi n° 2013-10 (2 avril 2013).

A part les règles de protection, les textes de lois Tunisiennes se sont penchés sur l'angle pénale du phénomène l'escroquerie informatique notamment l'accès illégal, l'entrave au bon fonctionnement des systèmes et l'atteinte à l'intégrité des données par article 199 bis ainsi que la falsification informatique par les articles 199 ter et 172 de la loi n° 99-89 du 2 aout 1999.

De même, les procédures à suivre en cas de crime commis ont été édicté via le code de procédure pénale comprenant les règles de droit commun de poursuite, instruction et jugement et le décret n° 2013-4506 du 6 novembre 2013 qui porte sur la constitution de l'agence technique des télécommunications, une agence considérée comme référence technique aux investigations judiciaires en ce qui concerne les crimes des systèmes d'information et de la communication, ainsi que sur la fixation des modalités de son fonctionnement et son organisation administrative et financière.

Néanmoins les limites de ce cadre juridique Tunisien se ressentent et s'alourdissent de plus en plus sur les différents acteurs de l'économie du pays du fait qu'il est considéré relativement statique et est devenu ancien par rapport à l'avancement du savoir et de la technologie, ceci en sus de l'absence d'une vision de long terme, intégrée et globale; une lacune qui se traduit par un manque de réactivité du système et des incohérences textuelles.

Effectivement, jusqu'aujourd'hui, la loi pénale en Tunisie n'aborde pas le sujet du détournement de données et d'escroquerie commises sur Internet connu sous le nom de « la cybercriminalité ». Cette loi constituant un passage obligatoire pour garantir un espace de confiance a, en fait, été traité et il existe bien un projet de loi sur la cybercriminalité amorcée en 2009, finalisée et passée en conseil de ministres en 2010 mais qui traine encore à voir le jour à cause du changement successifs des pouvoirs publics.

Il faut noter que la cyber sécurité ne porte pas sur les textes de lois uniquement, mais plutôt, sur une combinaison de plusieurs facteurs. Affirmant ceci, Chawki Gaddes, président de l'Instance nationale de protection des données personnelles a indiqué « La cyber-sécurité ne peut pas être seulement une question d'encadrement juridique, c'est à la fois un comportement, une prise de conscience et une culture qui fait aujourd'hui, défaut en Tunisie. Pour réussir à la mettre en place, il faut commencer à agir très tôt sur les mentalités, depuis l'école primaire ».

2.2 Structures

La cadre règlementaire Tunisien a de même prévu depuis l'année 1999 la création de différentes structures dédiées à la sécurité informatique.

Effectivement, ceci a commencé en 1999 par le lancement d'une « Unité micro-CERT ». C'est une unité composée d'expert Tunisiens spécialisés dans le domaine de la sécurité informatique crée selon le décret n°99-2768 du 6 décembre 1999 au sein du Secrétariat d'État en Informatique dont objectif principal consiste à veiller à l'amélioration continue de la sécurité des applications et infrastructures nationales critiques et à sensibiliser les administrateurs ainsi que les décideurs de systèmes d'informations.

Un an plus tard, l'Agence Nationale de Certification Électronique (ANCE) a été créée par la loi n°2000-83 du 9 Août 2000. Parmi les missions assignées à cette agence figure la sécurisation des transactions et des échanges électroniques.

A partir de 2002, le rôle de l' « Unité micro-CERT » a connu des modifications pour se charger, en plus de ses fonctions de base, de développer une stratégie nationale et un plan national en matière de sécurité des technologies de l'information et de la communication et d'assurer leurs mises en place. L'outil exécutif de cette stratégie ainsi que du plan national a été créée, en Janvier 2003, suite aux décisions du conseil des ministres. Ces décisions ont annoncé de même l'obligation de procéder à une évaluation périodique dans le domaine de la sécurité informatique et la Création d'un « organe d'auditeurs certifiés » en matière de sécurité des Systèmes d'Informations.

En 2004, l'Agence Nationale de la Sécurité Informatique (ANSI) a été créée en vertu de la Loi N° 2004-5 sous l'autorité du ministère des technologies de la communication. Cette agence est chargée d'effectuer un contrôle général des réseaux et des systèmes informatiques des différents organismes Tunisien que ce soit publics ou privés et notamment de veiller à la bonne exécution du plan et de la stratégie nationale développées par l'unité.

L'ANSI a accueilli en septembre 2005 le tunCERT, une Equipe nationale de réponses aux urgences informatiques qui offre l'assistance gratuite à l'ensemble de la cybercommunauté Tunisienne, aux citoyens comme aux professionnels, pour tout problème lié à la sécurité des systèmes d'informations. Ce centre vise aussi à sensibiliser la communauté nationale sur le sujet de la cybercriminalité en leurs informant de tous les incidents recueillis en les guidant sur les moyens de protections nécessaires.

Il existe également une entité de lutte contre les cyber-attaques dédiée spécialement aux banques Tunisiennes, à savoir, le CERT bancaire relevant de l'Association Professionnelle Tunisienne des Banques et des Etablissements Financiers (APTBEF).

2.3 Coopérations internationales

Avec l'accroissement rapide du risque cybernétique, la coopération trouve toute son importance. Effectivement, l'échange d'expériences et des bonnes pratiques s'avère très utile en matière de cyber-sécurité, un domaine qui ne cesse d'évoluer. C'est la raison pour laquelle la Tunisie entretient différentes relations de coopération en matière des Technologies de l'Information et de la Communication d'une manière générale, et en particulier, de la cyber-sécurité.

Parmi les coopérations entretenues par la Tunisie nous pouvons citer les différents Mémorandums d'Entente en matière des TIC signé avec divers pays, la convention des Nations Unies de lutte contre la criminalité transnationale, la convention arabe contre les crimes liés aux technologies d'information.

Récemment, la Tunisie s'est engagée dans le projet "CyberSud" de coopération avec l'Union Européenne en matière de cybercriminalité qui a été officiellement annoncé en Mars 2018 et a été officiellement invitée, en Février 2018, par le Conseil de l'Europe (CE) à devenir membre de la Convention de Budapest sur la cybercriminalité.

Section 2 : Evaluation de la cyber sécurité des banques tunisiennes

La vague des mises à jour qu'a connu le système bancaire Tunisien en terme de Technologies de l'Information et de la Communication aussi bien au niveau du système de paiement qu'au niveau du système d'information, avait pour objectif principal la modernisation de l'infrastructure bancaire et des outils utilisés. L'introduction de ces nouvelles technologies a été, bien évidemment, accompagné de nombreux risques numériques internes soient-ils ou externes rassemblés sous le concept de cybercriminalité.

Face un manque énorme de chiffres concernant la cybercriminalité notamment au niveau du secteur bancaire, nous avons opté pour une étude quantitative pour répondre à la problématique « Quel est le degré d'exposition des banques Tunisiennes à la cybercriminalité et est-ce qu'elles sont bien outillées contre un tel phénomène ».

Comme l'intitulé l'indique, cette section nous conduit au dépouillement des données collectées sur terrain grâce à un questionnaire que nous allons dans un premier temps le présenter. Puis il sera question d'analyser les résultats de l'enquête et y apporter quelques explications y afférentes pour enfin essayer de proposer un plan d'action basé sur les failles et les vulnérabilités du système bancaire Tunisien.

1. Présentation du questionnaire

Pour avoir une idée claire sur l'exposition des banques Tunisiennes au risque de la cybercriminalité, les attaques menées contre elles ainsi que les actions et outils sécuritaires déployés par ces dernières, nous avons mené une enquête par questionnaire destinés aux Responsables de Sécurité des Systèmes d'Information (RSSI) de toute les banques de la place. Ce choix est basé sur les connaissances nécessaires pour répondre à toutes les questions posées notamment celles portant sur la sécurité informatique au niveau stratégique telle que le budget alloué à la sécurité informatique.

En effet, le questionnaire diffusé est un questionnaire fermé de type descriptif qui comprend 3 volet, le premier étant relatif aux technologies de l'information et de la communication au sein de la banque, nous permettra d'avoir une idée plus ou moins claire sur le degré d'intégration des TIC. Le deuxième volet portera sur les risques numériques auxquels

font face les banques Tunisiennes et leurs degré d'exposition au phénomène de cybercriminalité. Et enfin un dernier volet portant sur les connaissances, les outils et les dispositifs relatifs à la sécurité informatique déployés pour gérer les risques cybernétiques et maintenir un bon niveau de sécurité.

Cette structure nous permettra de tirer une conclusion à la fin sur le degré d'outillage des banques Tunisienne face à ce phénomène mondiale.

2. Analyse et interprétation des résultats de l'enquête

Vu la délicatesse du sujet traité, nous avons opté pour des questions plutôt vagues afin de garantir le respect du cadre de la confidentialité des banques et collecter le plus d'information possible auprès des différentes banques de la place.

Le questionnaire a été diffusé auprès des 23 banques résidentes qui peuvent être structurées selon la nature de l'actionnariat de la sorte :

Tableau 2:

Banques publiques	STB - BNA - BH - BTS - BFPME - BFT - BZ
Banques à capitaux étrangers	ATB - ATTIJARI - UBCI - UIB - Citibank - Bank ABC - BTK - QNB - AlBaraka - WIB
Banques à capitaux privés tunisiens	Amen Bank - BIAT - BT
Banques mixtes	TSB - BTE - BTL
Total	**23**

Par ailleurs, il est a noté qu'uniquement 21 banques ont accepté de le remplir et ce pour deux raison distinctes l'une de joignabilité et l'autre de confidentialité.

Nous allons donc nous contenter d'analyser et de conclure à partir des réponses requises, à savoir, 16 banques universelles, deux banques spécialisées dans le microcrédit et le financement de petites et moyennes entreprises ainsi que trois banques islamiques.

Le traitement statistique de ces réponses a été effectué grâce au logiciel SPSS « Statistical Package for the Social Sciences », un logiciel dont l'objectif est de permettre de réaliser la totalité des analyses statistiques habituellement utilisées en sciences humaines. Dans notre cas, nous allons nous contenter de simples pourcentages représentatifs des réponses des différentes banques.

2.1 Intégration des Technologies de l'Information de de la Communication au niveau des banques Tunisiennes

L'introduction des TIC au niveau de secteur bancaire touche en premier lieu leurs connectivité grâce à l'automatisation des opérations en ligne et la normalisation de l'échange de données. Ces technologies peuvent, en effet, prendre en charge une partie ou la totalité des tâches liées à la communication bancaire que ce soit interbancaire via Intranet, entre la banque et ses clients via Extranet ou Internet ou bien entre les banques via le réseau SWIFT.

Par analogie, nous pouvons avoir une idée sur le niveau d'intégration des TIC en étudiant le taux de connectivité des banques qui s'avère bon au niveau de la majorité des banques.

Tableau 2 :

		Effectifs	Pourcentage
Valide	Entre 20% et 50%	1	4,8
	Entre 50% et 80%	5	23,8
	A plus de 80%	15	71,4
	Total	21	100,0

Effectivement, selon les réponses nous pouvons constater qu'à peu près 72% des banques, à savoir 15, sont connectées à plus de 80%. En ce qui concerne les 6 banques restantes, elles s'estiment connectées entre 50% et 80% exception faite d'une unique banque connectée à plus de 20% et moins de 50%.

Il est à noter que, d'après les remarques obtenues, maintes banques ne sont pas totalement connectées à Internet tel que les trois banques publiques qui utilisent principalement l'Intranet surtout au niveau des agences sous prétexte d'une meilleure sécurité des données.

Les résultats de la première question s'avèrent parfaitement compatibles avec ceux de la question qui suit relative au taux d'équipement ; la banque la moins connectée est la même banque qui se considère peu équipée. De même pour les autres banques, les 15 ayant répandu par plus de 80% au niveau de la première question se considèrent assez équipées.

Tableau 3 :

		Effectifs	Pourcentage
Valide	Peu équipée	1	4,8
	Moyennement équipée	5	23,8
	Assez équipée	15	71,4
	Total	21	100,0

Ceci peut garantir une estimation fiable du degré d'introduction des nouvelles technologies au sein des banques Tunisiennes qui jusque-là peut se qualifier de satisfaisant.

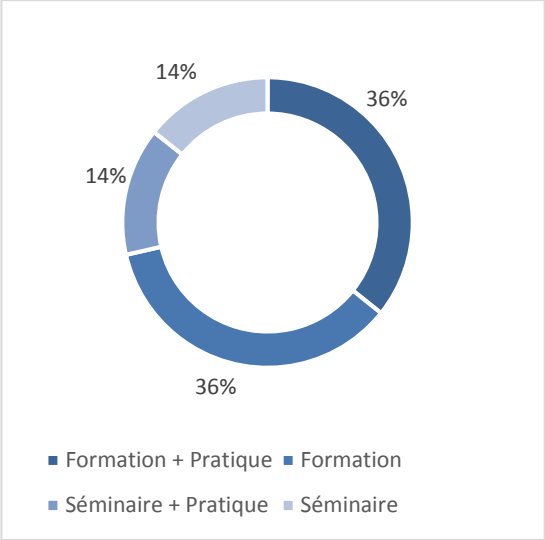
La modernisation qu'a connu ce secteur a été accueilli par une difficulté au niveau d'adaptation par la majorité des banques.

Tableau 4:

		Effectifs	Pourcentage
Valide	Non	14	66,7
	Oui	7	33,3
	Total	21	100,0

Effectivement, plus de 60% des banques ayant répandu à ce questionnaire ne se sont pas adaptés facilement aux NTIC introduites au niveau de leurs services et afin de remédier à cette difficulté elles ont dues se tourner vers les formations et les séminaires de perfectionnement ou simplement par la pratique ou une combinaison de deux.

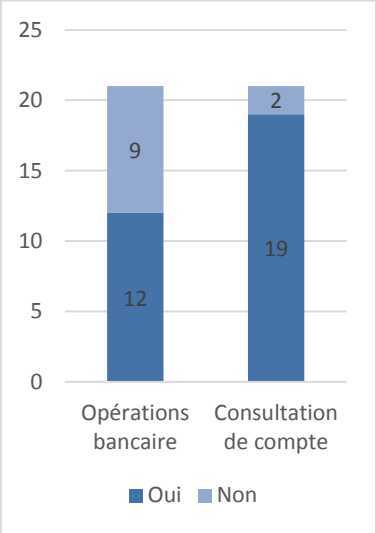
Figure 6:Solution d'adaptation



Selon les réponses collectées, 5 banques ont opté pour la solution da la formation accompagnée de l'adaptation par la pratique et 5 banques par la formation uniquement. Pour le séminaire de perfectionnement, il représente de loin la solution la moins utilisée; 2 banques seulement l'ont adapté l'une isolé et l'autre accompagné de l'adaptation par la pratique et enfin 2 banques se sont contenté simplement de l'adaptation par la pratique.

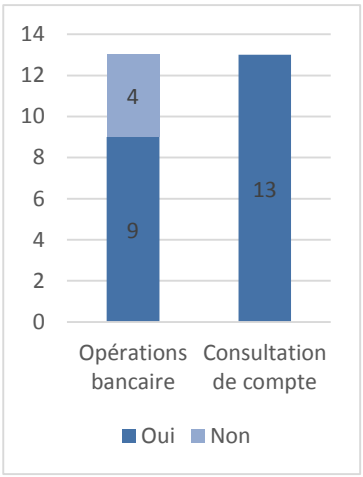
Cette introduction affecte de même l'accessibilité des banques qui s'est améliorée grâce aux systèmes de libre-service dédiés aux clients tels les applications mobiles et les sites Web qui sont devenus de plus en plus présents en Tunisie.

Figure 7:Sites Web



En effet, toute les 21 banques possèdent des sites WEB dont uniquement 2 qui ne sont pas apte de consultation de compte à savoir les deux banques spécialisées dans le microcrédit et le financement de petites et moyennes entreprises. Quant aux opérations bancaires, 12 banques parmi les répondants possèdent des site web qui permettent d'effectuer des opérations bancaires tel que les virements, les demandes de crédit ou de chéquiers …

Figure 8: Applications mobile



En ce qui concerne l'application mobile, la majorité des banques en possède déjà. En effet, 8 banques parmi les 21 interrogé n'en ont pas encore dont 7 prévoient introduire leurs propres applications mobiles. Toute les applications mobiles des banques tunisiennes permettent la consultation de compte et uniquement 9 permettent les opérations bancaires.

Ces technologies introduites au niveau des banques contribuent de même à l'élimination des logiciels encombrants et couteux et permettent l'utilisation à distance et en toute sécurité des ressources d'exécution et de stockage notamment via les services Cloud. La pratique de l'hébergement Cloud n'est pas très exploité par les banques Tunisiennes, à part l'UBCI n'ayant pas répandu à cette question, uniquement 30% des banques ayant répandu procèdent à l'hébergement Cloud.

Tableau 5:

		Effectifs	Pourcentage valide
Valide	Non	14	70,0
	Oui	6	30,0
	Total	20	100,0
Manquante	Système manquant	1	
Total		21	

Les explications avancées par les banques concernant ce faible taux d'utilisation sont au nombre de deux. La première se relie à la stratégie adoptée par les banques plutôt averses au risque refusant d'externaliser le stockage le leurs données. Quant à la deuxième, elle est de nature juridique, les articles 51 et 52 de la loi organique 63-2002 du 27 juillet 2002, et l'article 11 du décret numéro 2007-3002 du 27 Novembre 2007 interdisent la pratique de transfert de données à l'étranger exigeant ainsi non seulement une implantation en Tunisie mais aussi la connexion via un réseau Internet Tunisien.

2.2 Exposition des banques Tunisiennes au phénomène de la cybercriminalité

La modernisation du secteur par l'intégration des Techniques de de l'Information et de la Communication présente certes plusieurs avantages au secteur bancaire, mais elle comporte également, pas mal d'inconvénients notamment les attaques cybernétiques qui s'articule autour de trois cibles principales à savoir les systèmes d'informations, les comptes bancaires et les moyens de paiements.

Tableau 6:

Les systèmes d'informations			
		Effectifs	Pourcentage
Valide	Non	13	61,9
	Oui	8	38,1
	Total	21	100,0
Les comptes bancaires			
		Effectifs	Pourcentage
Valide	Non	13	61,9
	Oui	8	38,1
	Total	21	100,0
Les moyens de paiement			
		Effectifs	Pourcentage
Valide	non	6	28,6
	oui	15	71,4
	Total	21	100,0

Selon les réponses collectées, les moyens de paiement représentent la cible préférée des cybercriminels au niveau du secteur bancaire Tunisien et ce selon 15 banques sur les 21 banques ayant répandu au questionnaire.

Quant aux systèmes d'informations et les comptes bancaires, ils occupent tous les deux la deuxième place avec le même pourcentage (40%) de banques les considérant comme cible principale à savoir 8 banques sur 21.

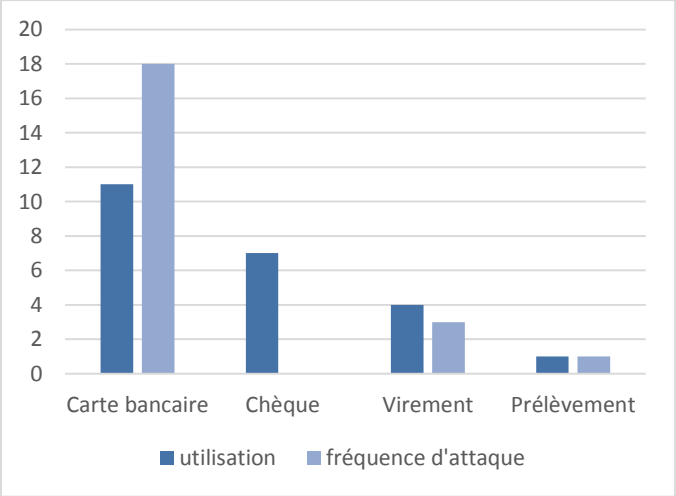
Nous allons essayer de décortiquer ces trois cibles une à une pour pouvoir estimer leurs niveau d'exposition au risque cybernétique.

Commençons par les moyens de paiements ; en se basant sur les réponses du questionnaire, nous constatons que 52.4% des banques (11 banques) considèrent la carte comme le moyen de paiement le plus utilisé et pour 33.3% des banques (7 banques) questionnée c'est plutôt le chèque et uniquement 4 banques considèrent que c'est le virement. D'où le dernier classement en terme d'utilisation revient aux prélèvements.

En ce qui concerne la fréquence d'attaques tournée vers les différents moyens de paiements, selon 18 banques, les cartes bancaires représentent le moyen de paiement le plus visé par les cyber-délinquants. Et comme la carte représente le moyen de paiement le plus utilisée, nous pouvons affirmer que son degré d'exposition au risque cybernétique plutôt élevé.

Le deuxième moyen de paiement en terme de fréquence d'attaque selon les banques tunisiennes (3 banques) est le virement bancaire, le moyen de paiement considéré comme le plus utilisé par 4 banques d'où un degré d'exposition modéré.

Figure 9:

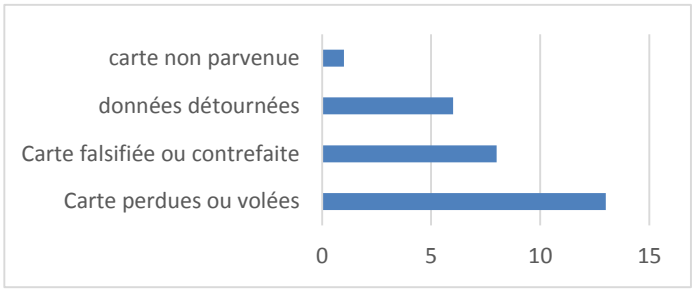


Etant le moyen le plus exposé au risque, nous allons essayer de faire le tour de question de la fraude de la carte de paiement

Nous avons essayé en premier lieu de déterminer le moyen le plus utilisé par les cyber-délinquants pour réaliser cette fraude au niveau du secteur Tunisien. En étudiant les résultats, il s'est avéré que ce type de fraude est le plus souvent réalisé via des Cartes physiques, en

d'autre termes, d'après 13 banques le moyen préféré des fraudeurs est l'utilisation de cartes volées ou perdues suivies des cartes falsifiées ou contrefaites et ce d'après 8 banques sur 21.

Figure 10:



Les fraudeurs des cartes préfèrent utiliser en troisième lieu des données de cartes détournées par des modifications apportées aux DAB et aux TPE ou via les sites marchands et dans ce cas, la fraude ne peut se réaliser que via Internet.

Il existe un autre moyen utilisé par les fraudeurs dans le monde mais qui, selon les banques répondantes, ne figure pas parmi les moyens préférés au niveau du secteur Tunisien, à savoir, la carte non parvenue, une sorte de fraude interne qui consiste à détourner la carte avant même que le client en prend possession.

Nous avons déjà mentionné que le troisième moyen préféré des cyber-délinquants est bien le détournement des données via différents réseaux, quels est alors le réseau le plus exposé ?

Selon les réponses collectées, nous pouvons classer les réseaux selon le degré d'exposition décroissant comme suit, les sites marchands (15 banques) suivies des distributeurs automatiques de billets et des Terminal de paiement électronique avec un même nombre de réponses positives à savoir 7 banques chacune.

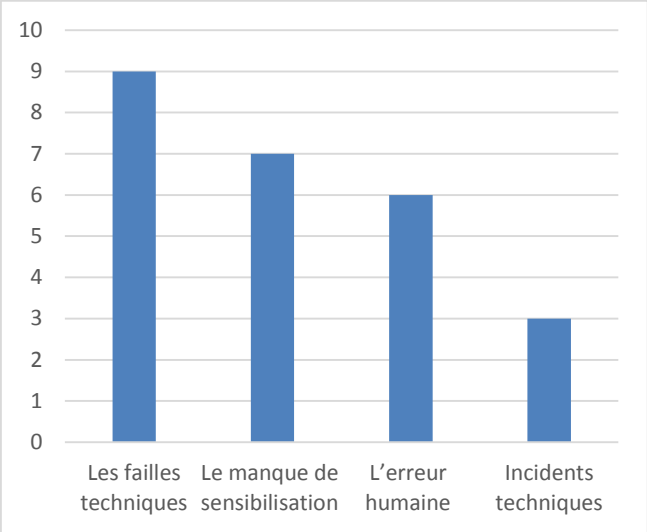
Passons à la deuxième cible préférée des criminels ; le système d'informations. Il existe deux types de systèmes d'informations adoptés au niveau des banques, le global bancaire et l'ensemble de modules imbriqués. IL est à noter que le deuxième type adopté par 30% des banques s'avère plus risqué que le deuxième implanté au niveau de 15 banques parmi les 21 questionnés.

Tableau 7:

		Effectifs	Pourcentage
Valide	Un ensemble de modules imbriqués	6	28,6
	Global bancaire	15	71,4
	Total	21	100,0

Afin de s'introduire aux systèmes d'informations des banques, les cybercriminels exploitent leurs vulnérabilités pour pouvoir s'incruster et atteindre leurs objectifs.

Figure 11: Source des vulnérabilités



Selon l'échantillon des banques Tunisiennes étudiées, ces vulnérabilités proviennent en premier lieu des failles techniques (9 banques) tel que les problèmes de conception des systèmes … en deuxième lieu (7 banques) du manque de sensibilisation qui se reflète principalement au niveau du choix de mot de passe, des mises à jour faite régulièrement etc… En troisième lieu l'erreur humaine (6 banques) et enfin les incidents techniques tel que les coupures d'électricité …

Comme déjà annoncé, les attaques de Phishing visant la clientèle ainsi que le personnel des banques fait partie des attaques les plus répandues tournées vers les comptes bancaires au niveau du secteur bancaire Tunisien, une des préférées des cybercriminels à étudier.

Effectivement, selon les réponses des 21 banques, plus que la moitié ont déjà reçu des réclamations de la part des victimes de Phishing bancaire. A part la banque n'ayant pas répandu précisé la cible de ces attaques, 5 banques ont reçu ces réclamations de la part de leurs clientèles uniquement, 3 de la part de leurs personnels et 2 banques ont vu leurs clients ainsi que leurs personnels attaqués de la part de ces criminels.

Avez-vous reçu des réclamations de la part des victimes de PHISHING bancaire?

Tableau 8:

		Effectifs	Pourcentage
Valide	Non	10	47,6
	Oui	11	52,4
	Total	21	100,0

Ces différents types d'attaque peuvent, en effet, être des attaques d'origine externe par toute personne n'ayant pas de relation directe avec la banque ou interne de la part du personnel utilisant que ce soit leur pouvoir d'accès ou des failles de sécurité qu'ils ont pu intercepter.

Tableau 9:

		Effectifs	Pourcentage
Valide	**20% - 80%**	2	9,5
	30% - 70%	5	23,8
	40% - 60%	4	19,0
	50% - 50%	1	4,8
	70% - 30%	1	4,8
	80% - 20%	2	9,5
	90% - 10%	6	28,6
	Total	21	100,0

Au niveau du monde bancaire Tunisien, la perception de l'origine des attaques cybernétiques varie trop d'une banque à l'autre.

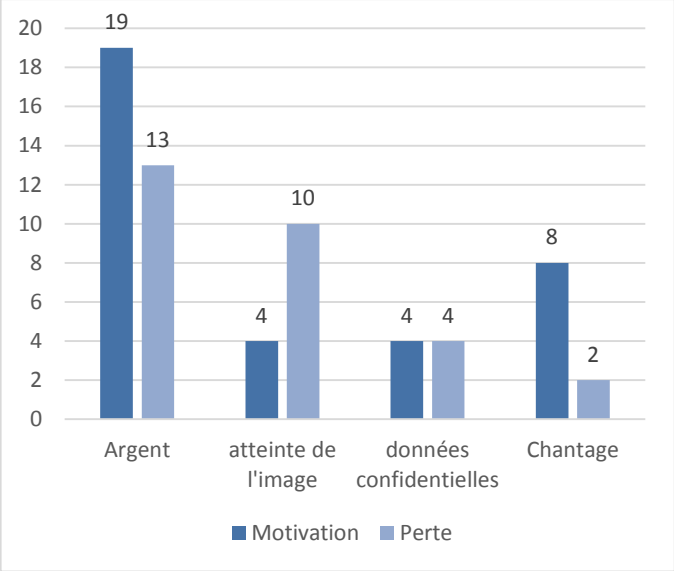
Effectivement, comme les chiffres le montre, à peu près 28% des banques considèrent que ces attaques sont 90% d'origine externe et 10% d'origine interne, alors que presque 24% à savoir 5 banques considèrent que 30% des attaques sont externe et 70% sont internes.

D'après les remarques recueillies, cette divergence au sujet de l'origine des attaques est probablement dû à un manque de connaissance ainsi que d'une mauvaise circulation de l'information concernant les attaques cybernétiques des banques

Ces attaques sont commises pour différentes raisons qui changent d'un cybercriminel à un autre. Effectivement, les motivations les poussant à commettre ces crimes n'en manquent certainement pas. Néanmoins, la raison principale reste les gains financiers. Effectivement, selon notre enquête, 19 banques sur 21 confirment cette hypothèse. Quant aux autres motivations, 8 banques considèrent que le chantage fait partie de la liste principale des finalités des cybercriminels, ainsi que le détournement de données confidentielles (4 banques) et la

détérioration de l'image des banques (4 banques). Une seule banque sur les 21 considère que l'espionnage industriel fait partie des motivations des criminels Tunisiens.

Figure 12:Confrontation entre les motivations et les pertes



Il est à noter le détournement des données confidentielles peut emmener la banque à faire face à un risque pénal. Quant au chantage il mène généralement à l'exposition du personnel.

Les réponses à la question qui suit confirment le classement de la motivation pécuniaire des cybercriminels. Réellement, les banque admettent que les dommages causés par les attaques cybernétiques contre le secteur bancaire tunisien consistent principalement selon 13 banques en la perte financière suivie d'après 10 banques de l'atteinte de l'image de la banque. A part ces deux pertes subies à causes des attaques cybernétiques, les banque peuvent faire face selon 4 banques à un risque pénal et en dernier lieu à l'exposition de son personnel (2 banques).

Ce qui est rassurant dans tout ça, c'est la conscience de la grande majorité des banques de l'importance et de la valeur ajoutée de l'intégration des TIC au niveau du secteur bancaire. En effet, presque toutes les 21 banques considèrent ces technologies comme ressource stratégique plutôt que source de risque ou charge financière comme perçue par une seule et unique banque représentant 5% de l'échantillon étudié.

Tableau 10:

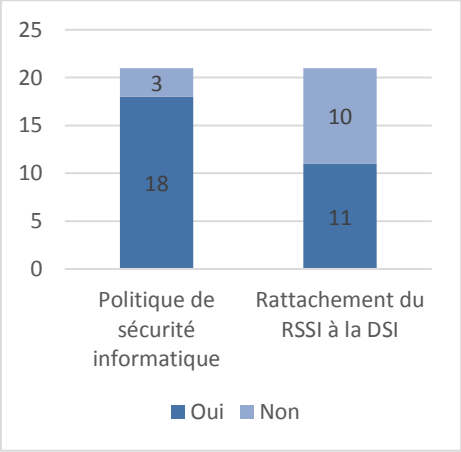
		Effectifs	Pourcentage
Valide	Une ressource stratégique	20	95,2
	Une charge financière	1	4,8
	Total	21	100,0

2.3 Moyens utilisées par les banques tunisiennes pour faire face au phénomène de la cybercriminalité

Travaillant principalement avec des données confidentielles, les banques doivent figurer parmi les secteurs les plus conservateurs dans le domaine des technologies de l'informations et s'inquiéter le plus au sujet de la sécurité informatique voire cybernétique. Pour ce faire, les banques doivent harmoniser les différents volets de sécurité informatique à savoir, organisationnel, technique, humain et juridique et ce en négligeant aucun d'entre eux.

Le volet organisationnel comprend généralement la politique de sécurité informatique prenant la forme d'un plan d'actions qui vise à protéger les informations et déterminer des objectifs à atteindre pour contourner les risques principalement cybernétiques et les bonnes pratiques à suivre. D'après notre enquête, 18 banques sur les 21 questionnées suivent une politique de sécurité bien précise.

Figure 13:Prise en compte du volet organisationnel



Parmi les bonnes pratiques de sécurité informatique, le rattachement du responsable de la sécurité informatique à la direction générale et non à la direction informatique afin d'éviter de tomber dans la situation de juge et parti. En réalité, grâce à notre enquête nous avons pu avoir une idée sur l'application de cette pratique qui se limite à uniquement 10 banques sur 21.

Plus les banques intègrent les nouvelles technologies dans leur activité, plus la sécurité informatique gagne de la place et plus les dépenses y afférentes augmentent suivant le même rythme. Nous pouvons avoir une idée sur l'importance de la sécurité informatique au sein d'une banque en observant le pourcentage des dépenses consacrées à la sécurité informatique par rapport au budget dédié à l'informatique en général.

Tableau 11:

		Effectifs	Pourcentage
Valide	Moins de 3%	2	9,5
	Entre 3% et 8%	2	9,5
	Entre 8% et 12%	6	28,6
	Plus que 12%	11	52,4
	Total	21	100,0

Depuis les résultats du questionnaire, 80% des banques investissent plus que 8% du budget alloué à l'informatique dans la sécurité dont à peu près 50% d'elles investissent plus que 12% dans ce domaine. Ces observations reflètent une la conscience des banques Tunisiennes de l'importance de la sécurité. Confirmant ceci, uniquement 2 banques investissent en la sécurité entre 3% et 8% du budget informatique, à savoir, les deux banques spécialisées en micro crédits et financement des petites et moyennes entreprises et 2 autres à moins de 3%.

Quant au volet technique, il englobe tous les moyens technologiques et informatiques employés par la banque pour atténuer les risques cybernétiques et traiter les incidents lors de leur survenance.

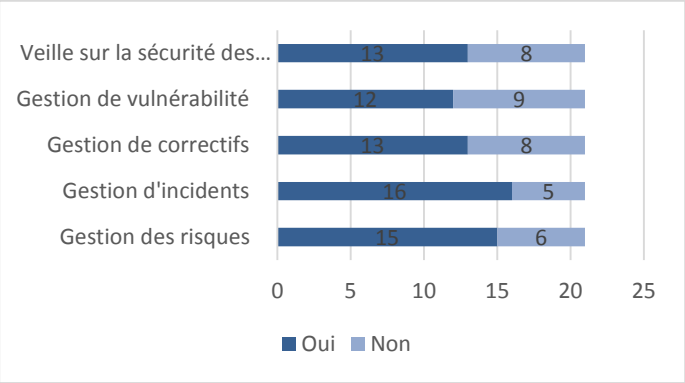
Tableau 12:

		Effectifs	Pourcentage
Valide	Non	3	25,0
	Oui	9	75,0
	Total	12	100,0

Nous avions déjà vu un peu plus tôt qu'il existe pas mal de banques au niveau du secteur bancaire Tunisien dont les applications mobiles et les sites web permettent d'effectuer des opérations en ligne. Afin d'améliorer leur niveau de sécurité ces banques peuvent procéder à une authentification forte pour les clients utilisant ce type de service. La réalité Tunisienne montre que 75% des banque possédant au moins un site web qui autorise ce type d'opération ont déjà penser à les sécuriser d'une manière efficace ce qui est notamment rassurant.

Quant aux systèmes de sécurité informatique, ils sont certes variés. Afin d'étudier le degré d'équipement des banques en cette matière, nous avons choisi une liste de systèmes les plus utiles (selon les spécialistes) sur laquelle nous avons mené notre enquête.

Figure 14:Utilisation des différents systèmes de sécurité informatique



Selon les réponses collectées nous pouvons remarquer que tous les systèmes sont utilisés par les banques Tunisiennes mais non pas avec le même degré.

Afin d'avoir une idée plus claire, nous nous sommes penchés sur le taux d'équipement par banque.

En réalité, 8 banques parmi les 21 sont parfaitement équipés par ces systèmes et uniquement 2 banques possèdent 4 systèmes parmi ces cinq. En ce qui concernes les banques les moins équipées, ils sont au nombre de 3 pour celles possédant 3 systèmes et 3 pour celles possédant 2 systèmes uniquement. Ce qui est un peu inquiétant, c'est le nombre de banques munies d'un seul système parmi ces cinq considérés comme essentiels qui est en fait 5 banques sur les 21 répondantes.

Passons au volet humain, l'erreur humaine ainsi que manque de sensibilisation figurent parmi les vulnérabilités principales des systèmes d'informations Tunisiens.

Pour faire face à un tel risque et afin de garantir une meilleure sécurité des systèmes d'informations, 17 banques parmi les 21 font des sessions de sensibilisation en matière de sécurité informatique selon différentes fréquences ; 8 entre elles le font une fois par an, 4 banques 2 fois par an, 4 banques 4 fois par ans et 1 banque le fait mensuellement.

A part les sessions de sensibilisation, il existe des formations en sécurité de l'information que 16 banques parmi l'effectuent que ce soit annuellement (6 banques) semestriellement (6 banques) ou trimestriellement (4 banques).

La cyber sécurité dédie un volet entier au moyens juridiques qui aident à cerner et à lutter contre ce phénomène.

Malheureusement, uniquement 12 banques parmi les 21 banques ayant répondu au questionnaire connaissent les loi Tunisiennes relatives à la sécurité informatique.

Appliqué depuis fin mai 2018, le Règlement général sur la protection des données (connu par GDPR : General Data Protection Regulation), constitue le nouveau cadre européen relatif à la protection des personnes physiques au sujet du traitement et de circulation des données à caractère personnel. Couvrant l'ensemble des résidents Européens, ce texte

oblige toute entité manipulant des données personnelles concernant des Européens à se conformer à cette réglementation notamment la Tunisie.

Selon l'enquête menée, 16 banques connaissent cette nouvelle réglementation européenne et supposent que le secteur bancaire tunisien est concerné. Parmi ces 16 banques une seule juge qu'elle n'est pas prête à se conformer avec cette norme.

Conclusion

Face à une intégration satisfaisante des TIC, le secteur bancaire Tunisien se trouve moyennement exposé au risque cybernétique. En effet, les cybercriminels attirés par ce secteur sont tournés en premier lieu vers les moyens de paiement, notamment les cartes bancaires et en deuxième lieu vers les systèmes d'informations dont l'exposition est faible grâce à l'adoption des global bancaire par la majorité des banques et les comptes bancaires.
Il faut mettre l'accent sur le fait que, de nos jours, les attaques cybernétiques que subissent nos banques se comptent sur le bout des doigts et surtout ne dépassent pas le cadre de tentatives, néanmoins, ce phénomène reste grandissant dont les motivations principales restent les gains financiers et l'atteinte de l'image des institutions visées.

C'est à ce niveau que la sécurité trouve sa place, en effet, elle s'avère primordiale pour garantir l'avenir d'une banque ainsi sa pérennité. Conscientes de l'importance des TIC et du risque inévitable lié à ces technologies, les banques Tunisienne se sont penchés majoritairement sur la sécurité, néanmoins, en arrivant au volet juridique, une ignorance du cadre réglementaire attire l'attention, une faille sur laquelle le secteur ne devrait pas fermer les yeux.

Conclusion Générale

L'objectif de notre travail est focalisé sur la réalité des banques tunisiennes en matière d'exposition à la cybercriminalité et leur degré de préparation face à un tel phénomène mondial. Afin de parvenir à cette fin, nous avons articulé notre mémoire autour de trois chapitres. Les deux premiers chapitres étaient purement la théorique, quant au dernier chapitre, il avait porté sur une étude quantitative qui étale des chiffres représentatifs de l'état actuel de préparation des banques tunisiennes en matière de sécurité informatique.

Au niveau du premier chapitre, nous nous somme focalisés sur deux notions fondamentales, à savoir, les technologies de l'information et de la communication et la cybercriminalité. En effet, nous avons tenté de démystifier ces deux notions en étalant les différentes définitions proposées à leurs sujets ainsi que leurs états de lieux dans le monde en général et au niveau du secteur bancaire en particulier.

Tout au long du second chapitre, nous avons mis l'accent sur la lutte contre la cybercriminalité. Dans un premier temps, nous avons exposé les différents moyens utilisés pour lutter contre ce phénomène mondiale, allant des moyens techniques sophistiqués utilisés par les professionnels, passant aux moyens légaux assurés par les Etats, les moyens humains qui peuvent se résumer par des sessions de sensibilisation des utilisateurs des TIC et enfin les moyens organisationnels. Dans un deuxième temps, nous avons présenté un moyen de suivi de la performance en sécurisation cybernétique notamment la notation en cyber-sécurité tout en évoquant ses avantages et ses inconvénients.

Le dernier chapitre était consacré à une étude quantitative centré sur le cas tunisien. D'abord, nous avons tenté d'exposer un bref aperçu sur l'état du secteur des technologies de l'information et de communication au sein de la Tunisie et son intégration au niveau du secteur bancaire. Nous avons, également, essayé de donner une idée sur l'exposition de ces institutions au risque cybernétique en énumérant quelques incidents survenus récemment. Pour enfin arriver à énoncer les différents moyens utilisés par l'Etat tunisien pour affronter ce phénomène.
Au niveau de la deuxième section, nous nous somme penché sur l'étude de la réalité des banques à travers un questionnaire scindé en trois parties.

Les réponses collectées dans le cadre de cette enquête démontrent que les banques tunisiennes s'avèrent suffisamment outillés et terme de TIC. Fortement connectées, la totalité des banques disposent de sites Web bancaire ainsi que d'applications mobiles pour la quasi-majorité d'entre elles. Par contre, l'externalisation des données via l'hébergement Cloud reste faiblement adopté en Tunisie.

Face à une intégration satisfaisante des TIC, le secteur bancaire Tunisien reste moyennement exposé au risque cybernétique. En effet, les attaques cybernétiques visant les institutions financières tunisiennes sont tournés en premier lieu vers les moyens de paiement, notamment les cartes bancaires. Face à un tel risque, a société monétique de la Tunisie ainsi que les deux autres banques (BIAT et UBCI) entretenant des relations directes avec les fournisseurs de réseaux de paiement se sont dotée de la certification PCI DSS ; un ensemble de pratiques garantissant un meilleur niveau de sécurité des instruments de paiement.

La deuxième cible préférée est les systèmes d'informations dont l'exposition est plutôt faible grâce à l'adoption des global bancaire par la majorité des banques et les comptes bancaires.

Néanmoins, la cybercriminalité reste un phénomène très dynamique et de plus en plus menaçant dont les motivations principales restent les gains financiers et l'atteinte de l'image des institutions visées.

Conscient de l'importance des TIC et du risque inévitable lié à leur utilisation, le secteur bancaire tunisien se montre plutôt soucieux de la sécurité informatique et cybernétique.

Toutefois, le volet juridique est plutôt mis à coté par les institutions financières ainsi que par l'Etat tunisien. En effet, malgré le manque de réglementation concernant ce type de crime, son ignorance de la part de ces institutions attire l'attention ; une faille sur laquelle le secteur ne devrait pas fermer les yeux.