REPUBLIQUE DE COTE D'IVOIRE

Union - Discipline - Travail

BUREAU NATIONAL D'ÉTUDES TECHNIQUES

ET DE DÉVELOPPEMENT (BNETD)

LES ENJEUX DE LA CYBERSECURITE POUR LES PME ET PMI DE LA ZONE UEMOA

COURS EN LIGNE

JUILLET 2015

bnetd Bureau National d'Etudes Techniques et de Développement - Boulevard Hassan II, Cocody Abidjan Côte d'Ivoire
04 BP 945 Abidjan 04 - Tel:+225 22 48 34 00 fax:225 22 44 56 66 - Site Internet: www.bnetd.ci - email: contact@bnetd.ci

PLAN DU COURS

NOTE DE SYNTHÈSE

Les Petites et moyennes entreprises PME et les Petites et moyennes PMI représentent une source importante d'emplois et d'innovations. Elles évoluent aujourd'hui dans un environnement de plus en plus numérique, qui favorise incontestablement leur compétitivité et leur croissance. Pour autant, les technologies de l'information et de la communication (TIC), lorsqu'elles sont mal maîtrisées, peuvent être à l'origine de vulnérabilités et faciliter les attaques sur l'entreprise. Pour y faire face, les PMEPMI n'ont pas toujours la possibilité de recruter des profils dédiés à la sécurité informatique. Afin de promouvoir un environnement favorable au développement économique et de préserver le patrimoine immatériel de ces entreprises, il convient aujourd'hui, dans une démarche d'intelligence économique, de mettre en place des solutions humaines et techniques adaptées aux spécificités des PMEPMI. La formation de référent en cybersécurité interne au profit des PME/PMI permettra de répondre en partie à ce défi. L'objectif général de la formation est de faire du participant un « référent en cybersécurité interne.

A la fin du cours, le participant devra être en mesure de :

- maîtriser les enjeux de la cybersécurité pour l'entreprise ;
- identifier et utiliser les outils nécessaires à la protection des informations sensibles (personnelles et professionnelles) sur les différents réseaux;
- identifier et comprendre les menaces liées à l'utilisation de l'informatique et des réseaux internet, réseaux privés d'entreprises, réseaux publics ;
- mettre en œuvre les démarches de sécurité.

INTRUDUCTION

L'internet a fondamentalement transformé notre société et notre économie. De par son évolution réellement planétaire et ubiquitaire en tous points du globe, l'internet continuera, à travers son impact, son influence et son importance, à se développer. De même, une nouvelle génération de citoyens adeptes de l'internet, ayant grandi avec le Net et étant à l'aise avec toutes ces dimensions, est aux avant-postes de la création de nouvelles applications, de nouveaux services et usages. Les cyberpirates n'épargnent personne. Institutions, grands groupes industriels… Mais aussi collectivités territoriales, PME-PMI, particuliers… qu'elles visent les utilisateurs publics ou privés d'internet, leurs attaques coûtent aujourd'hui 380 milliards d'euros par an (27400 milliards de FCA) et pourraient représenter 2 200 milliards d'euros de pertes pour l'économie mondiale d'ici 2020. En Côte d'Face c'est près de 26 milliards de Fcfa de perte pour l'économie. À ces énormes enjeux, la cybersécurité est désormais une priorité, non seulement pour les états, mais également pour tout un chacun naviguant sur internet ou travaillant avec des outils connectés pour commercialiser ses produits. Les PME/PMI représentent une source importante d'emplois et d'innovations. Elles évoluent aujourd'hui dans un environnement de plus en plus numérique, qui favorise incontestablement leur compétitivité et leur croissance. Pour autant, les technologies de l'information et de la communication (TIC), lorsqu'elles sont mal maîtrisées, peuvent être à l'origine de vulnérabilités et faciliter les attaques sur l'entreprise, car les cyberpirates n'épargnent personne (Institutions, grands groupes industriel, collectivités territoriales, PME-PMI, particulier). Qu'elles visent les utilisateurs publics ou privés d'internet, les attaques des cyberpirates coûtent aujourd'hui 380 milliards d'euros par an et pourraient représenter2 200 milliards d'euros de pertes pour l'économie mondiale d'ici 2020. En Côte d'ivoire c'est près de 26 milliards de FCFA de perte pour l'économie ces trois dernières années. À ces énormes enjeux, la cybersécurité est désormais une priorité, non seulement pour les états, mais également pour tout un chacun naviguant sur internet ou travaillant avec des outils connectés pour commercialiser ses produits. Pour y faire face, les PME/PMI n'ont pas toujours la possibilité de recruter des profils dédiés à la sécurité informatique. Qui plus est, l'approche

qu'elles ont de la gestion des infrastructures informatiques varie en fonction de l'utilisation qui en est faite, de leur taille, du secteur économique et du budget qui y est consacré. De fait, à l'exception de certains secteurs très spécifiques, le niveau de perception et de prise en charge du cyber-risque dans les PME/PMI dans l'espace UEMOA est aujourd'hui très faible. Tout de de même l'évolution exponentielle des outils informatiques apporte de profondes mutations dans les usages et les acteurs économiques sont de plus en plus dépendant d'internet et des TIC dans le cadre de leurs activités commerciales et sociales ; et l'intégrité du réseau est éprouvée quotidiennement par des attaques sévères et sophistiquées d'où l'intitulé du thème : « Les enjeux de la cybersecurité pour les PME et PMI de la zone UEMOA ». Ce cours est divisé en quatre parties. La première partie présente la zone UEMOA avec ses missions, ses objectifs et les activités économiques liées aux tics et la cybersécurité et cybercriminalité. La seconde partie définie les différents thèmes liés à la cybersécurité. La troisième est relative aux infractions liées à la cybersécurité, quand la quatrième présente les responsabilités pénale de ces infractions dans l'espace UEMOA. La dernière partie concerne la mise en œuvre de démarches de sécurité et précautions techniques et juridiques pour faire face aux attaques.

OBJECTIFS

A la fin du cours, le participant pourra être à mesure de

- Maîtriser les enjeux de la cybersécurité pour les PME-PMI
- Identifier et utiliser les outils nécessaires à la protection des informations sensibles (personnelles et professionnelles) sur les différents réseaux.
- Identifier et analyser des problèmes de cybersécurité dans une perspective d'intelligence et de sécurité économiques dans l'espace UEMOA ; Connaître les obligations et responsabilités juridiques de la cybersécurité pour les PME et PMI ;
- Identifier et comprendre les menaces liées à l'utilisation de l'informatique et des réseaux internet, réseaux privés d'entreprises, réseaux publics ;
- Mettre en œuvre les démarches de sécurité inhérentes aux besoins fonctionnels
- Savoir présenter les précautions techniques et juridiques pour faire face aux attaques

PROBLÉMATIQUE

Quels sont les grands enjeux de la cybersécurité ? La cybersécurité et cybercriminalité est-elle dans l'espace UEMOA parfaitement appréhendée, notamment par la puissance publique et les états ? Le domaine n'est-il qu'un simple complément à l'univers de la sécurité ou, au contraire, déjà perçu comme un véritable enjeu stratégique et industriel ?

Comme la mer, le cyberespace est un assemblage que les États s'efforcent aujourd'hui de réguler. Ses ports sont des hébergeurs, ses détroits sont des fournisseurs d'accès, ses sous-marins sont des chevaux de Troie. Cet océan a même ses pirates, et ses flibustiers, des Anonymous, ainsi que des corsaires, disposant de lettres de course transmises par des États ou des entreprises en mal de marchés. Dans cette configuration, il reste trois rôles à attribuer : celui de navires marchands (vulnérables) – il revient au monde économique ; celui de marines nationales – à donner à la Défense ou à l'Intérieur, la question sera ici de savoir où s'arrête la cyberdéfense et où commence la cybercriminalité ; enfin celui de navigateurs – il reviendra aux industriels qui devront se montrer capables d'ouvrir dans cet océan des routes sécurisées. Avec cette image nous pouvons clairement identifier tous les intervenants et leur rôle dans le cyberespace de l'espace UEMOA.

PARTIE I L'ESPACE UEMOA

1 Missions et objectifs

L'Union Économique et Monétaire Ouest Africaine (UEMOA) qui constitue un prolongement de l'UMOA (Union Monétaire Ouest Africaine) a été créée le 10 janvier 1994 à Dakar par les Chefs d'État et de Gouvernement de sept pays de l'Afrique de l'Ouest : Bénin, Burkina Faso, Côte d'Ivoire, Guinée-Bissau, Mali, Niger, Sénégal et Togo.

L'UEMOA est une intégration institutionnelle et de marché ayant pour objectifs :

- renforcer la compétitivité des activités économiques et financières des États membres dans le cadre d'un marché ouvert et concurrentiel et d'un environnement juridique rationalisé et harmonisé ;
- assurer la convergence des performances et des politiques économiques des États membres par l'institution d'une procédure de surveillance multilatérale ;
- créer entre les États membres un marché commun basé sur la libre circulation des personnes, des biens, des services, des capitaux et le droit d'établissement des personnes exerçant une activité indépendante ou salariée, ainsi que sur un tarif extérieur commun et une politique commerciale commune ;
- instituer une coordination des politiques sectorielles nationales, par la mise en œuvre d'actions communes et éventuellement de politiques communes notamment dans les domaines suivants : ressources humaines, aménagement du territoire, transports et télécommunications, environnement, agriculture, énergie, industrie et mines ;
- harmoniser, dans la mesure nécessaire au bon fonctionnement du marché commun, les législations des États membres et particulièrement le régime de la fiscalité.

En dépit des contraintes et difficultés, l'UEMOA dispose d'un certain nombre d'atouts pour la réalisation effective du marché commun : une unité monétaire commune (FCFA) ; un tarif extérieur commun (TEC) et une politique commerciale commune ; des règles communes de concurrence ; un marché financier régional et une bourse régionale des valeurs mobilières (BRVM) ; une forte mobilité de la

main d'œuvre et une complémentarité relative des structures économiques, un patrimoine historique et culturel commun et l'usage de langues locales communes et de la langue française.

Cependant, la réalisation du marché commun de l'UEMOA dépendra principalement des efforts de diversification des appareils productifs et d'exportation des pays membres, de la réalisation d'infrastructures régionales de transport et de facilitation de transits routiers, de l'élimination des barrières non tarifaires, de la coordination des politiques économiques, du renforcement du dialogue politique et de la bonne gouvernance démocratique dans l'espace UEMOA, mais aussi du renforcement des relations commerciales et économiques avec les autres blocs régionaux, et plus particulièrement, la coopération et le partenariat UE-UEMOA dans le cadre des accords APE.

Aussi l'approche institutionnaliste et de marché du processus d'intégration économique régionale de l'UEMOA n'a-t-elle pas montrée ses limites ? Il urge donc d'orienter dorénavant ce processus vers une conception globale avec une approche organisationnelle et sectorielle d'intégration économique régionale qui mettra l'accent sur une forte coopération sectorielle régionale et un développement des échanges commerciaux transfrontaliers.

.

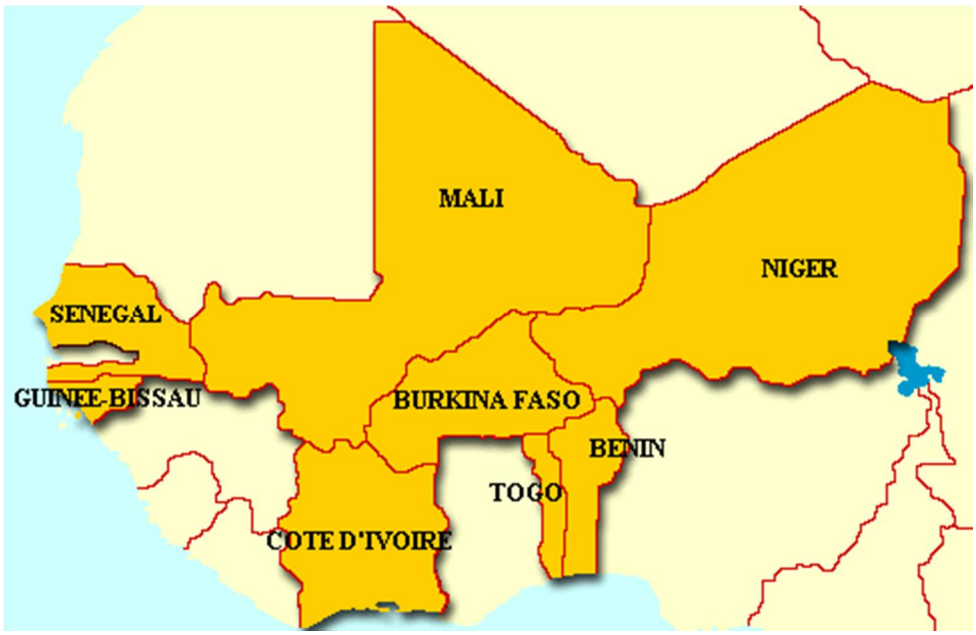


Figure 1

2- L'ESPACE UEMOA EN CHIFFRES

L'UEMOA regroupe huit États membres

Superficie: 3 509 600 km2

Population: 80 340 000 habitants

Taux de croissance démographique: 3%

Taux de croissance démographique: 3%

PIB nominal: 24 332,6 milliards de F CFA

PIB réel (à prix constant): 18 458,8 milliards de F CFA

Taux de croissance du PIB réel: 4,3%

Taux d'inflation annuel: 4,3%

3-Taux d'utilisation des TIC en Afrique de l'Ouest (Espace UEMOA)

En Afrique généralement et particulièrement dans les pays de l'Afrique de l'ouest, il est difficile de déterminer avec certitude le nombre d'utilisateurs d'internet. Il est par conséquent très difficile d'évaluer la pénétration d'internet dans ces pays. En effet, un abonnement à internet est partagé par plusieurs personnes et beaucoup de personnes ont un accès à Internet sur leur lieu de travail. Aussi, les cybercafés urbains et les CMC (Centre Multimédia de Communautaire) en milieu rural, sont les principaux moyens de connexion à Internet dans la plus part des pays de l'Afrique de l'ouest.

Face à cette difficulté, nous utiliserons les chiffres fournis par la banque mondiale. Soulignons que ces chiffres sont les plus récentes (elles datent de 2012), et qu'ils concernent le nombre d'utilisateurs de l'internet filaire haut débit (ne sont donc pas pris en compte, l'utilisation d'internet mobile et d'internet sur les mobiles).

Le graphique ci-dessous montre le nombre d'utilisateurs pour cent habitants dans l'ensemble des 16 pays de l'Afrique de l'ouest.

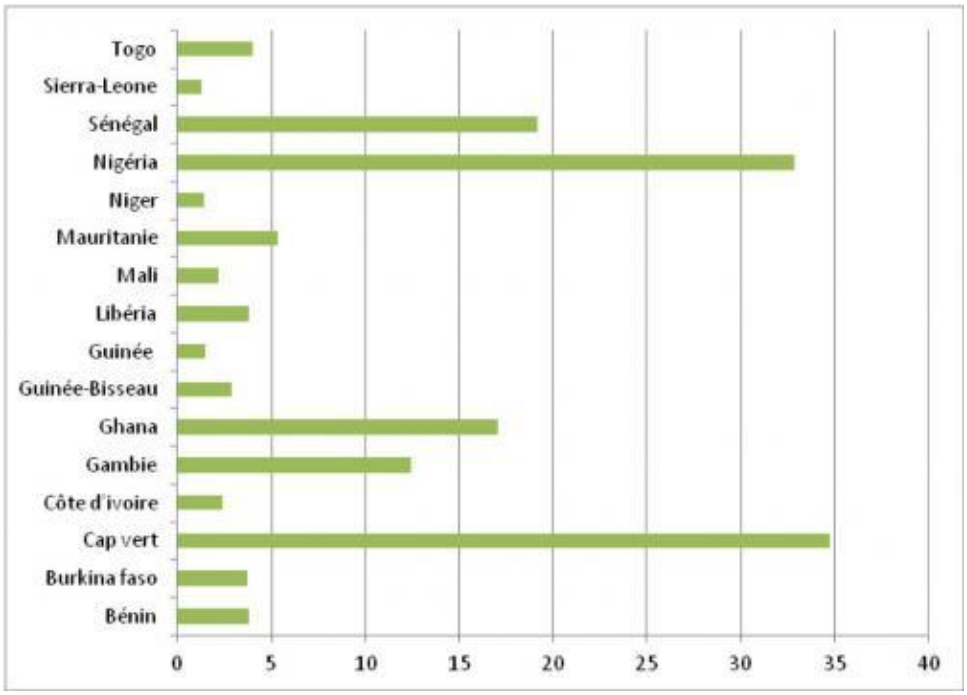


Figure 2

Les statistiques ci-dessus montrent que les pays peuvent être répartis en trois groupes:

Le premier considéré comme celui des pays de l'Afrique de l'ouest à forte connectivité à internet sont ceux qui ont franchi la barre des 30.Il s'agit du le Cap vert (32,87) et le Nigéria (34,74). Ces deux pays, se démarquent nettement des autres. Ils représentent seulement. Le second groupe de pays est celui des pays considérés comme ayant un taux de pénétration internet moyen c'est-à-dire compris entre 10 et 20 personnes/cent. On a dans ce groupe trois pays que sont le Sénégal (19,20), le Ghana (17,10), la Gambie (12,44). Enfin, le troisième groupe (celui dans lequel se retrouve la Côte d'Ivoire), rassemble les pays dont le taux de pénétration Internet est moins de 5. Ce groupe qualifié des « traînards » est composé de la plupart des pays, d'où le faible taux de pénétration en Afrique de l'ouest. Ce sont : la Mauritanie (5,36), le Togo(4), le Bénin (3,79), le Burkina-Faso (3,72), la Guinée-Bissau (2,89), le Liberia (3,79), la Côte d'Ivoire (2,37), le Mali (2,16), la Guinée (1,49), le Niger (1,40) et la Sierra-Leone (1,3). Au vu des chiffres, il apparaît clairement que le nombre d'utilisateurs d'Internet pour cent habitants reste faible pour l'ensemble des pays de l'Afrique de l'ouest. Aussi, se dessine une sorte de fracture numérique régionale. En effet, nous avons d'une part 5 pays soit 31,25% dont le taux d'utilisateurs d'internet est au-dessus de 10% et d'autre part, les 11

autres pays soit 68,75% dont le taux d'utilisateurs d'internet ne dépasse même pas les 5%.

4-Activités économiques liées à l'utilisation des TIC dans l'Espace UEMOA

L'espace UEMOA devrait connaître un taux de croissance de 7,4% d'ici la fin de l'année, a-t-on appris lors de la 18ème session de la Conférence des chefs d'Etat et de gouvernement de l'Union économique et monétaire ouest-africaine qui s'est déroulée lundi à Cotonou. Dans le marché tes TIC, des initiatives importantes ont été prise depuis 2007, dans le cadre de l'émergence et de la consolidation du marché intérieur des TIC. Des textes communautaires ont été élaborés en vue de l'harmonisation des politiques réglementaires des Télécommunications/TIC. De plus la promotion de l'intégration financière à travers les paiements transfrontaliers par téléphone mobile offre des perspectives très prometteuses, sans parler des avantages qui en découlent pour l'inclusion financière au niveau national et de la sous-région. Même si le taux de pénétration de l'internet en Afrique et plus précisément dans l'espace UEMOA ne dépasse pas les 10%, il est important de faire ressortir que ces quatre dernières années, nous assistons à un ensemble activités économiques liées à l'usage des TIC. Au niveau d'internet nous pouvons remarquer des activités annexes comme les parie en lignes. Aujourd'hui la majeure partie des paiements pour une inscription ou un jeu se fait en ligne avec des moyens de payement mobile vu que le taux de bancarisation est encore faible. On assiste même à des transfère de fond entre opérateurs mobiles et banques. Beaucoup de paiement quelques soit le secteur l'activité s'effectue par mobile. Les transactions par carte bancaire sont rares du fait que la cote d'ivoire est blacklisté par beaucoup de site et pays. Certains opérateurs bancaires ont lancé des solutions de paiement de la banque par internet (d'Internet Banking) en temps réel pour les particuliers comme pour les entreprises. En ce qui concerne le commerce électronique, ce secteur de l'économie (numérique) est aujourd'hui en plein essor. On constate aujourd'hui l'existence de beaucoup de site marchand qui propose des achats (jumia.ci kaymu.ci diayma.com) qui proposent des articles avec des règlements et des moyens de paiements à distance utilisant les TIC.

5-Identification des problèmes de cybersécurité dans l'Espace UEMOA

Les PME et PMI sont généralement les cibles d'infraction qui est la cybercriminalité 3O% des attaques ciblées visent en générale toutes les entreprises. Les problèmes qu'ils ont en générale sont liés à une absence de :

- Politique de la sécurité informatique
- Contrôle à l'accès du wifi et d'Internet de l'entreprise
- Homogénéité du parc informatique
- Mise jour régulière des logiciels informatiques
- Gestion de la sécurité de la flotte de mobiles (smartphones laptop)
- Filtrage de sites
- Formation du personnel à la sécurité informatique

PARTIE II CYBERSECURITE

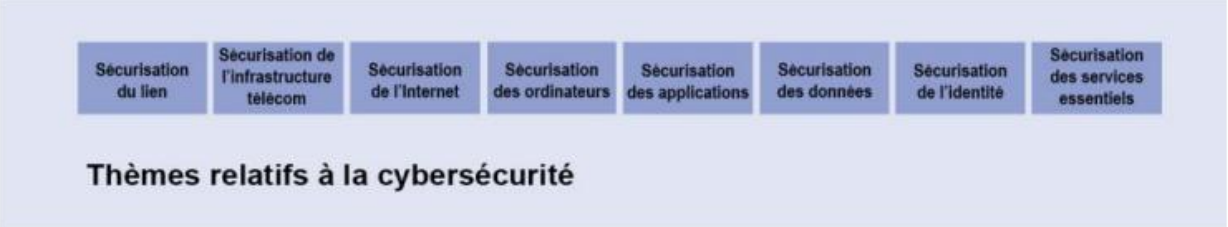
1-Définition évolutive de la cybersécurité

La cybersécurité est un terme général qui évolue au fil du temps et dont la signification ne fait pas consensus. À partir de cette expression, on peut dresser une liste quasi-infinie de thèmes liés à la sécurité de l'internet, parmi lesquels les problèmes techniques et les vulnérabilités, les problèmes sociaux et comportementaux et les activités criminelles. La cybersécurité désigne tout ce qui englobe les problèmes liés à la sécurité spécifique à l'internet et les solutions techniques et non-techniques possibles.

La cybercriminalité est l'ensemble des infractions susceptibles de se commettre sur un ou au moyen d'un système informatique généralement connecté à un réseau ciblant l'outil informatique comme les atteintes aux systèmes automatisés de données, celles ou les réseaux sont utilisés comme moyens pour commettre des crimes ou délits classiques (escroqueries, fraudes, blanchiment d'argent) et notamment celle ou les délinquants utilisent les technologies numériques comme support d'infractions de contenus illicites tels que la pédopornographie ou le racisme.

2-Thèmes de la cybersécurité

Le tableau de la figure ci-dessus est une représentation simplifiée des différents éléments qui constituent la cybersécurité. Ce diagramme ne se prétend pas exhaustif, mais il fournit un schéma simple pour pouvoir aborder les différents aspects de la cybersécurité. Chaque encadré du tableau représente une catégorie générale des services de sécurité. Étant donné l'étendue du champ d'application de la cybersécurité, il s'avère utile de décomposer celle-ci en catégories ou thèmes généraux. Chacun de ces thèmes peut être l'objet d'une description détaillée



2-1 Sécurisation des connexions

Les paquets Internet ne sont intrinsèquement dotés d'aucune sécurité. Ils sont complètement ouverts et toute personne équipée d'un simple outil logiciel peut facilement inspecter les contenus de chaque paquet qui sont transmis sur l'ensemble du réseau. La Sécurisation du lien consiste à mettre en place des mécanismes élémentaires protection des blocs de données de l'architecture de l'internet. Pour éviter tout « reniflage » ou toute écoute clandestine, on réalisera vite qu'il est nécessaire de trouver un moyen de crypter la transmission de données sensibles avec des solutions de cryptage gratuite (SSH, SSL/TSL).

2-2 Sécurisation des infrastructures

La sécurité de l'internet et la sécurité des télécom se distinguent l'une de l'autre dès lors qu'il s'agit de définir la cybersécurité ; chacune de ces entités dispose de sa propre infrastructure particulière et d'organisations standards. Les regrouper peut brouiller les pistes, car les solutions visant à sécuriser une infrastructure nationale des télécommunications (*systèmes fermés fortement régulés au sein desquels évoluent une poignée d'acteurs majeurs sur chaque marché, organisés de manière hiérarchique, des monopoles naturels, et des infrastructures physiques vieillissantes*) sont des solutions différentes de celles requises pour sécuriser l'infrastructure de l'internet *(savoir des systèmes ouverts en grande partie non régulés qui se construisent sur la base d'infrastructures de télécommunications nationales et internationales multiples et qui ne disposent d'aucun centre organisationnel apparent)*. De plus en plus, la cybersécurité englobe des problèmes de sécurité liés aux réseaux de télécommunication de type mobile et satellite et aux installations de diffusion et de micro-ondes.

2-3 Sécurisation des ordinateurs

Chaque fois qu'un appareil se connecte à l'internet, il s'expose à une intrusion. En grande majorité, les attaques les plus réussies de hackers, de criminels et autres acteurs malveillants sont menées contre des serveurs et des ordinateurs d'utilisateurs finaux connectés à l'internet. Bon nombre d'organisations ne ménagent pas leurs efforts pour installer des pare-feux et des systèmes de sécurité sur les points finaux, que l'on appelle habituellement outils « antivirus » ou « anti-maliciels ».

2-4 Sécurisation des applications

Toute application sur un appareil tel qu'un ordinateur personnel ou un smartphone, connectée et communicant sur l'internet, est une « application internet ». À titre d'illustration, deux des applications internet les plus courantes, le courrier électronique (email) et la navigation du Web, quand il s'agit de sécurisation des applications Internet. Il existe cependant de nombreuses applications sur l'internet et leur nombre ne cesse de croître au fur et à mesure de l'acceptation des nouveaux usages de l'internet. Cette sécurisation prend en compte :

- Sécurisation des emails
- Sécurisation des applications Web

2-5 Sécurisation des données

La sécurité et la confidentialité des données (consentement compris) sont les autres domaines habituellement associés à l'expression « cybersécurité ». La sécurité des données désigne toute stratégie ou toute mesure – légale, technique, sociale ou autre – utilisée pour protéger des données. En tant que canal ultime pour le transfert transfrontalier des données, l'internet permet aux populations du monde entier d'envoyer et de recevoir des données en tous points du globe. Les différents protocoles de l'internet fournissent des degrés divers de sécurité des données.

2-6 Sécurisation des identités numériques

Un lien sécurisé n'est bon qu'à partir du moment où les points finaux sont considérés comme des entités légitimes autorisées à mener à bien une transaction donnée. Des mécanismes qui permettent d'accroître la confiance et de valider l'identité permettent à l'internet de proposer des canaux pour une communication sécurisée, fiable et privée entre les entités, susceptibles d'être clairement authentifiées d'une manière mutuellement comprise. Ces mécanismes doivent disposer de moyens raisonnables pour que les entités puissent gérer et protéger les détails concernant leur identité.

2-7 Sécurisation des ressources critiques

La sécurisation des ressources critiques concernent des infrastructures et services numériques, qui lorsqu'elles sont attaquées, provoquent des dégâts bloquent tout le système. Les conséquences d'une attaque réussie contre un ordinateur qui gère ou contrôle ces types de ressources critiques sont désastreuses.

PARTIE III les infractions liées à la cybersécurité

Certains phénomènes sont qualifiés de cybercriminels parce qu'ils sont commis au moyen des technologies de l'information et de la communication. L'objectif de cette est de montrer de façon générale toutes les infractions utilisés. A ce titre, il est possible de distinguer, selon les intérêts atteints par ces phénomènes, entre les atteintes aux intérêts des Etats, les atteintes aux personnes, les atteintes aux biens publics comme privés (PMEPMI) et les atteintes à la propriété intellectuelle le

1- cyberterrorisme et les atteintes aux intérêts des Etats.

Les phénomènes cybercriminels commis au moyen des technologies donnent une portée nouvelle au terrorisme et, plus généralement aux différentes atteintes aux intérêts des Etats on peut citer entre autre :

- La trahison pour livraison à une puissance étrangère ou à ses agents, sous quelque forme ou par quelque moyen que ce soit, un renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé qui doit être tenu secret dans l'intérêt de la défense nationale ;
- Acte d'espionnage destiné à s'assurer, par quelque moyen que ce soit, la possession d'un tel renseignement, objet, document, procédé, donnée informatisé ou fichier informatisé en vue de le livrer à une puissance étrangère ou à ses agents ;
- La destruction, complicité de destruction de tel renseignement, objet, document, procédé, donnée numérisée ou fichier informatisé en vue de favoriser une puissance étrangère

2-Les atteintes aux libertés individuelles et à la vie privée

L'Internet et, de manière plus générale, les TIC, ont multiplié les occasions d'atteintes à différentes libertés individuelles et d'intrusion dans la vie privée des personnes. Aussi, dans le cadre de la lutte contre la cybercriminalité, une attention soutenue est-elle accordée à la protection contre différentes sortes d'atteintes aux libertés et à la vie privée. Elles sont multiples et multiforme. Elles peuvent porter atteinte à l'identité de la personne (ex. usurpation d'identité), à son image, sa voix, au secret de sa correspondance… Ainsi, de nombreux cas de cybercriminalité basés sur le vol d'identité ou, plus généralement, de données d'identification personnelle ont été rapportés dans les diverses études nationales.

Le développement des réseaux sociaux constitue un amplificateur de tels phénomènes. L'étude sur le Nigeria relève une recrudescence de la cyberdélinquance basée sur le vol d'identité, notamment par le biais de réseaux sociaux comme facebook, pour commettre toutes sortes de crimes.

3-Les atteintes spécifiques aux droits de la personne au regard du traitement des données à caractère personnel

Les TIC multiplient les occasions de porter atteinte aux personnes, notamment à l'occasion du traitement de données personnelles. De ce point de vue, la protection de telles données recèle nécessairement une dimension liée à la cybercriminalité. C'est pourquoi des infractions sont instituées en vue de protéger les personnes à l'occasion du traitement des données personnelles.

4-Association de malfaiteurs informatiques

Cette infraction se caractérise par la participation à une association formée ou à une entente établie en vue de préparer ou de commettre une ou plusieurs des infractions prévues par la loi sur la cybercriminalité.

5-Les atteintes aux biens

L'infraction d'escroquerie sur les réseaux est relevée dans la plupart des études nationales. La forme la plus classique est celle qui utilise l'Internet, mais elle n'est pas exclusive. De plus en plus d'escrocs utilisent des réseaux de téléphonie (notamment le GSM). Le mode opératoire généralement utilisé est l'envoi massif d'e-mails ou de sms prometteurs de contrats d'affaires, de transferts d'importantes sommes d'argent issues d'un héritage, des gains substantiels à des loteries étrangères ou encore, à plus petite échelle, de promotion au travail, voire de mauvaises nouvelles concernant un proche. Il s'agit principalement pour les cyber-délinquants de demander une assistance pour transférer des fonds d'un pays à un autre moyennant une contrepartie financière ou de solliciter un transfert de crédit téléphonique ou un simple appel vers un numéro de téléphone souvent surtaxé. Cette infraction, dont les conséquences peuvent aller jusqu'à la commission d'homicides, est devenue une véritable industrie en Afrique et particulièrement au Nigeria, encore appelée « fraude 419 », selon la section 419 du Code pénal nigérian.

6-Le spamming et le fishing

Les atteintes à la propriété se commettent principalement par la voie de l'escroquerie de façon générale, mais de manière plus spécifique à travers les instruments de paiement électroniques. L'exemple typique en Afrique de l'Ouest reste le « 419 scam » (fraude 419). Ce procédé consiste à envoyer à une victime potentielle un spam, mail non sollicité. Le contenu du spam sera alléchant et reproduira à peu près ceci: « *Je vous demande de l'aide pour sortir illégalement une très grosse somme d'argent du Nigeria. En échange, vous toucherez une commission sur cette somme. Il vous suffit de donner votre numéro de compte en banque afin que l'argent y soit versé*»

7-L'abus de confiance

L'abus de confiance n'est pas un acte cybercriminalité en tant que tel mais Il consiste dans le fait de porter atteinte à la fortune d'autrui en détournant ou détruisant ou dissipant tout bien susceptible d'être soustrait et qu'on a reçu à charge de le conserver, de le rendre, de le représenter ou d'en faire un usage déterminé. Tout bien peut faire l'objet d'abus de confiance qu'il soit corporel, comme un ordinateur, ou incorporel, comme la connexion Internet.

8-Les atteintes à la propriété intellectuelle

Les atteintes à la propriété intellectuelle qui sont favorisées par les technologies de l'information et de la communication sont les délits de contrefaçon. La contrefaçon est prévue en matière de brevet d'invention, de marque de produits ou de services, de modèle d'utilité et de droit d'auteur. Dans toutes ces matières, il s'agit d'atteinte au monopole d'exploitation conféré par le titre protégé. Cette atteinte se réalise très souvent par les moyens classiques de fabrication, de vente ou d'exposition de produits physiques. Mais elle peut également se réaliser par le moyen des technologies de l'information et de la communication. Dans la société de l'information, ces atteintes aux créations charriées par le cyberespace sont devenues une véritable préoccupation pour les titulaires de droits de propriété intellectuelle. C'est le cas par exemple des logiciels. L'atteinte à la propriété intellectuelle peut également porter sur un nom de domaine qui bénéficie d'une protection.

9-Les infractions relatives aux moyens de paiement électroniques

Le développement des moyens de paiement électroniques a offert de nouveaux moyens d'atteintes aux biens des personnes. C'est pourquoi les infractions liées aux cartes ou virements électroniques, par exemple visent à protéger contre de telles atteintes. Par ailleurs, sans doute certaines particularités des sociétés africaines constituent-elles également des facteurs de développement de fraudes aux cartes bancaires. Ainsi, de nombreux cas de remise de codes de cartes bancaires à des proches ont été relevés. Cet acte est mis en œuvre à travers la réception d'informations personnelles, confidentielles ou encore protégées par le secret professionnel par l'usage de manœuvres frauduleuses quelconques ou en utilisant de faux noms ou de fausses qualités. Enjeux de société, enjeux économiques, enjeux politiques, enjeux humains, qu'elle soit dénommée sécurité de l'informatique et des télécoms ou cybersécurité, la sécurité informationnelle touche à la sécurité du patrimoine numérique et culturel des individus, des organisations et des nations

1. PARTIE IV cybersécurité et responsabilités pénales dans l'Espace UEMOA

Virus, piratage, espionnage, phishing, malware, «défaçage» ou «défacement»…plus de 84 % des utilisateurs tes TIC dans le monde se déclarent inquiets de l'usage qui peut être fait de leurs données personnelles et que trois entreprises sur quatre Europe reconnaissent avoir vu leur système attaqué. Des formations sur la cybersécurité et cybercriminalité, devrait mobiliser citoyens, décideurs et entrepreneurs, mais aussi élus et collectivités territoriales. Car tout le monde plus précisément les PME/PMI peuvent aussi voir leur responsabilité pénale engagée, en cas de divulgation de données, suite à une cyberattaque sur un système non sécurisé. Les réponses aux actes cybercriminels laissent la place à de très grandes particularités nationales, la matière pénale constituant un domaine de souveraineté des états fortement marqué par le caractère strictement national des réponses étatiques de politique criminelle, singulièrement, celles qui relèvent de responsabilité pénale.

1-Les sanctions prévues selon certains états de l'Espace UEMOA

Au regard des études nationales, il est possible de relever deux tendances, d'une part à la sévérité dans la répression et d'autre part, à la diversité des peines retenues à titre principal, accessoire ou de sûreté. La sévérité des peines prévues semble dénoter du fait que l'ensemble des Etats concernés soient sensibilisé à la gravité du phénomène de la cybercriminalité et de l'importance des menaces que ce phénomène fait peser sur les Etats, les économies, les sociétés et les personnes. La diversité des peines révèle, quant à elle, le souci de prendre en compte la complexité du phénomène de cybersécurité et cybercriminel pour y apporter des réponses adaptées.

Toutefois, il existe un risque réel d'incohérence tant au sein des états qu'entre les Etats. Au sein des Etats, les risques d'incohérences proviennent, d'une part, du possible concours entre les sanctions aux infractions dites « classiques » contenues dans les Codes pénaux et les sanctions nouvelles issues des textes destinés à répondre spécifiquement aux phénomènes cybercriminels et d'autre part, de la multiplication des interventions des législateurs face à la diversité des phénomènes cybercriminels. Et entre Etats, les risques d'incohérence et surtout d'inefficacité

viendraient de l'absence d'harmonisation des réponses nationales aux niveaux communautaire et international face à un phénomène qui ignore les frontières.

2-Les sanctions pénales

Il existe une très grande diversité dans les sanctions prévues face aux phénomènes de cybersécurité plus précisément de cybercriminalité. Une telle diversité est aisément compréhensible au regard de deux facteurs essentiels : d'une part, la variété des sanctions constitue le pendant de l'hétérogénéité des phénomènes relevant de la cybercriminalité et d'autre part, les sanctions sont propres à chaque Etat et, dans de rares cas, à chaque région (Exemple de l'Afrique centrale ou occidentale en ce qui concerne certaines infractions liées aux systèmes et moyens de paiement électroniques) ou Organisation régionale (Exemple de l'OAPI en ce qui concerne les infractions en matière de propriété intellectuelle dans les Etats membres).

- Peines principales :

Il est possible de relever certaines tendances qui semblent se dégager des diverses études. Ainsi, aux peines privatives de liberté s'ajoutent souvent des peines pécuniaires comme peines principales, peines privatives de liberté. Des peines d'emprisonnement demeurent présentes, dans tous les pays, comme peine principale pour les infractions retenues. Elles peuvent être cumulatives ou alternatives avec des peines pécuniaires, notamment. Mais il semble que la prison demeure encore un principe important de réponse pénale à la cybercriminalité.

- Peines pécuniaires (amendes)

Il convient de noter que les peines privatives de liberté s'accompagnent, ou peuvent être remplacées, dans certains cas, de manière quasi systématique, d'amendes retenues en tant que peines principales. Ainsi, il semble que les infractions relevant de la cybercriminalité mettent souvent en cause des intérêts économiques, même si certaines portent atteinte à d'autres valeurs ou principes comme la sûreté de l'Etat ou la dignité des personnes. Dès lors, il est important pour les états de l'espace UEMOA de mettre en place de sanctions pénales adaptées qui tiennent compte de forte dimension économique des phénomènes cybercriminels. Aussi, les cybercriminels sont-ils souvent frappés « dans leurs portefeuilles » par des amendes

dont les montants sont considérables. Ces amendes sont, par ailleurs, adaptées aux personnes morales délinquantes.

- Peines complémentaires

Les peines complémentaires peuvent être obligatoires (la publication de la décision judiciaire sur un support de communication numérique) ou facultatives. Les juges ont ainsi une large palette de peines complémentaires facultatives qui peuvent consister dans :

- la coupure de l'accès au site ayant servi à commettre l'infraction ;
- l'interdiction d'émettre des messages de communication numérique ;
- l'interdiction à titre provisoire ou définitif de l'accès au site ayant servi à commettre l'infraction ;
- la l'interdiction de l'hébergement du site ayant servi à commettre l'infraction ;
- la fermeture de sites ou d'établissement.

3-Les autres types de sanctions prévues

- Les sanctions administratives

Les sanctions administratives ne sont prévues que dans les pays ayant consacré des dispositions spécifiques. Elles peuvent être diverses et consistent, par exemple, dans des interdictions temporaires, des retraits d'autorisation, voire des amendes.

- Les sanctions civiles

Les sanctions civiles existent dans tous les Etats. Elles consistent, notamment, dans la réparation des dommages qui sont causés à la victime du cybercrime.

4-La coopération internationale

La cybersécurité et cybercriminalité présentent la particularité d'ignorer les frontières étatiques. Elles sont transfrontalières car non seulement les auteurs, complices et victimes des infractions peuvent se trouver dans des pays ou des continents différents, mais aussi l'élément matériel de certaines infractions peut être localisé sur des territoires différents. Or elle menace, au-delà des individus, les Etats eux-mêmes qui se trouvent ainsi soumis à des atteintes à leur sûreté et, particulièrement au risque de terrorisme. Face à un tel phénomène, il est évident qu'une réponse strictement nationale serait inefficace. Les Etats consentent ainsi plus aisément à coopérer dans le domaine de la lutte contre la cybercriminalité.

PRÉCAUTION ET GÉNÉRALE CONCLUSION

1 Rédaction d'une politique de sécurité

La sécurité informatique ne s'improvise pas et ne se bâtit pas en réaction à la suite d'une attaque ou en réaction à un fait d'actualité. Il faut poser sur le papier quels sont les périmètres du système d'information à protéger, de quelle façon y parvenir. Il est essentiel de bien définir les responsabilités de chacun, les procédures à mettre en place pour faire face à un problème de sécurité informatique afin de ne pas réagir dans la précipitation en cas de problème avéré.

2 Mise en place d'une sécurité sur le Web

Il s'agit d'appliquer des procédures relatives aux points ci-dessus

- La Protection des renseignements personnels et professionnels en
- La navigation Web sécuritaire
- Les médias sociaux
- L'ingénierie sociale
- La sécurité logicielle
- L'hébergement sécuritaire et sécurité des entreprises sur le Web
- Les programmes malveillants
- Les pratiques exemplaires en matière d'authentification

Sécurité des points de vente

Sécurité du courrier électronique

Sécurité des données

Sécurité de l'accès à distance

Sécurité des appareils mobiles

Sécurité matérielle