Association des Banques Centrales Africaines

Association of African Central Banks

SÉMINAIRE CONTINENTAL DE L'ASSOCIATION DES BANQUES CENTRALES AFRICAINES SUR LE THÈME «INNOVATIONS TECHNOLOGIQUES FINANCIÈRES, CYBERCRIMINALITÉ: DÉFIS POUR LES BANQUES CENTRALES»

N'Djamena, Tchad, 14 - 16 mai 2018
****** / ******

CONCLUSIONS ET RECOMMANDATIONS
----

1. INTRODUCTION

Le séminaire continental de l'ABCA pour l'année 2018 a été organisé par la Banque des États de l'Afrique Centrale (BEAC) du 14 au 16 mai 2018 à N'Djamena au Tchad, sur le thème «Innovations dans les technologies financières, cybercriminalité : défis pour les banques centrales». Cinquante-trois (53) délégués provenant de vingt et une (21) banques centrales membres, six (6) institutions régionales et internationales et une (1) université ont pris part au séminaire. La liste des participants est jointe en annexe.

2. CEREMONIE D'OUVERTURE

La cérémonie d'ouverture a été présidée par M. Ivan Bacale Ebe Molina, Directeur Général des Etudes, Finances et Relations Internationales de la BEAC.

Dans ses propos liminaires, M. Papa Lamine Diop, Secrétaire Exécutif de l'ABCA, au nom du Président de l'ABCA, M. Lesetja Kganyago, Gouverneur de la South African Reserve Bank (SARB), a exprimé sa profonde gratitude à l'Honorable Abbas Mahamat Tolli, Gouverneur de la BEAC, pour avoir accueilli cet événement important de l'Association et pour les excellentes dispositions prises. Il a apprécié la généreuse hospitalité du peuple tchadien et a exprimé ses remerciements les plus chaleureux à Son Excellence, le Président Idriss Deby Itno, au Gouvernement et au peuple tchadiens.

Il a remercié les experts d'avoir accepté de partager leurs connaissances sur les sujets à discuter lors du séminaire ainsi que les représentants des institutions régionales et internationales pour leur soutien multiforme à l'ABCA. En outre, le Secrétaire Exécutif a salué la participation remarquable des banques centrales membres de l'ABCA, qui témoignage de leur forte détermination à contribuer de manière décisive à relever les défis de l'intégration monétaire en Afrique.

Il a indiqué que le Séminaire Continental se déroule dans un contexte caractérisé par un développement soutenu des innovations dans les technologies de l'information, qui entraîne l'émergence de nouveaux acteurs, produits et modèles économiques affectant les principales fonctions des banques centrales et créant de nouveaux cyber-risques.

A cet égard, le Secrétaire Exécutif a indiqué que le séminaire devrait contribuer à une meilleure compréhension des opportunités offertes par les technologies financières, en vue de faciliter les transactions financières et d'accélérer l'inclusion financière. Il vise également à fournir une analyse pertinente des défis et des risques liés aux technologies financières et à réfléchir aux stratégies permettant de tirer parti des avantages des Fintech, tout en évitant les risques qui pourraient favoriser la fraude, le blanchiment d'argent et le financement du terrorisme, ce qui pourraient compromettre la stabilité des systèmes financiers en Afrique.

Dans son discours d'ouverture, le Directeur Général a souhaité aux délégations la bienvenue et un agréable séjour à N'Djamena. Il a également transmis les regrets du Gouverneur de la BEAC, M. Abbas Mahamat Tolli, qui aurait souhaité présider cette cérémonie mais ne pouvait être présent en raison d'autres engagements.

M. Bacale Ebe Molina a noté que le grand nombre de banques centrales représentées reflète leur vif intérêt pour les activités de l'ABCA, en particulier celles visant à relever les défis de l'intégration monétaire et financière africaine. Il a ajouté que le thème était opportun, en particulier compte tenu du développement rapide des technologies financières et de leur impact sur les économies des Etats membres. De plus, le partage d'expériences entre les institutions respectives constitue une source d'enrichissement qui devrait conduire à des conclusions fructueuses.

Le Directeur Général a mentionné certaines actions déjà engagées au sein de la BEAC, auxquelles les conclusions du séminaire pourraient apporter une contribution. Ces actions incluent les méthodes de supervision à adopter pour réduire les risques associés à l'émergence d'innovations financières susceptibles d'affecter la stabilité financière. Elles couvrent également la pratique du de-risking et les mesures appropriées qui peuvent atténuer son impact sur le secteur bancaire.

Il a ajouté que la BEAC, en consultation avec la Commission Bancaire de l'Afrique Centrale (COBAC), a élaboré des textes communautaires spécifiques qui réglementent les conditions d'approbation, d'exercice et de contrôle de l'activité des institutions émettrices de monnaie électronique. D'autres réglementations en vigueur sur la sécurité des systèmes d'information des institutions de crédit et de microfinance imposent à ces institutions des obligations en matière de qualité des informations comptables et financières, d'intégrité et de confidentialité des transactions, de préservation et de disponibilité des informations, de sécurité informatique, ainsi que des procédures de sauvegarde informatique.

Plus récemment, la BEAC a pris une décision établissant des plafonds pour les transactions opérées au moyen d'instruments de paiement électronique, afin d'assurer la liquidité adéquate des institutions émettrices de monnaie électronique et de prévenir le blanchiment de capitaux et le financement du terrorisme.

En conclusion, le Directeur Général a souhaité aux délégués des délibérations constructives, tout en espérant que le séminaire continental atteindra ses objectifs. Dans sa déclaration d'ouverture du séminaire, il a invité les participants à noter avec attention les principaux enseignements tirés du séminaire qui devraient contribuer à la promotion de la stabilité monétaire et financière en Afrique dans les années et décennies à venir.

3. STRUCTURE DU SEMINAIRE

Le séminaire était structuré comme suit. Trois sous-thèmes ont été présentés par des personnes ressources. Les représentants des banques centrales ont ensuite partagé leurs expériences. Enfin, trois ateliers ont été organisés pour discuter de sujets spécifiques et réfléchir sur les actions à mener par les banques centrales, afin de bénéficier des innovations dans les technologies financières et faire des recommandations à soumettre au Conseil des Gouverneurs pour examen.

3.1. Session plénière 1 : Présentation des sous-thèmes

Les trois sous-thèmes suivants ont été présentés respectivement par Dr. Sean Maliehe, chercheur postdoctoral du Programme d'Economie Humaine au Centre pour l'Avancement de la Recherche, à l'Université de Pretoria, M. Adrien Delcroix, Expert en Infrastructure de Marché à la Direction Générale Infrastructure du Marché et Paiement (Division de la surveillance), à la Banque Centrale Européenne (BCE) et M. Danny Brando, Vice-Président en charge de la Politique de cybersécurité du Groupe de surpervision, à la Federal Reserve Bank de New York (FRBNY):

- Monde numérique et économie humaine : mobile money et développement socio-économique en Afrique ;
- Technologies financières : opportunités et défis pour les banques centrales africaines ;
- Cybersécurité : implications pour les pratiques de supervision.

M. Delcroix et M. Brando ont fait leurs présentations par vidéoconférences, respectivement à partir de la BCE, à Francfort, et de la FRBNY, à New York.

Dans sa présentation, le Dr Maliehe a souligné que l'utilisation d'un micro-ordinateur, la connectivité Internet ou la disponibilité de l'électricité demeurent encore un privilège pour quelques-uns en Afrique. Le taux d'accès à Internet est en moyenne de 35,2% sur le continent, inférieur à la moyenne mondiale de 54,4%. Cependant, la pénétration de la téléphonie mobile a enregistré des statistiques plus élevées. En 2011, il y avait 445,6 millions d'utilisateurs de téléphones mobiles au Moyen-Orient et en Afrique. Dans les deux régions, les statistiques ont atteint 745,1 millions en 2018. Il a indiqué que les téléphones mobiles ne sont plus un signe de richesse, de prestige et de privilège. Ils sont devenus un facteur clé d'inclusion financière pour une grande partie de la population africaine et sont devenus des formes indispensables et flexibles de technologies dans la communication quotidienne et l'organisation de l'activité économique.

Dr Maliehe a mentionné le succès du mobile money dans plusieurs pays africains, dont le Kenya, le Lesotho et le Zimbabwe, où les services innovants ont fondamentalement changé la façon dont les gens développent leurs réseaux sociaux. Le mobile money a facilité l'accès à des transactions numériques transparentes et permis aux populations de mieux gérer leurs activités financières. Il a également été une passerelle vers d'autres services financiers, tels que l'assurance, l'épargne et le crédit. De plus, l'argent mobile a permis une croissance économique accrue en fournissant aux entreprises les moyens de se développer en favorisant l'éclosion d'une génération de gestionnaires de marchés émergents.

À la lumière de ces développements, le présentateur a fait valoir que le mobile money et les innovations connexes peuvent être considérés comme des gains socio-économiques pour les populations en Afrique et ailleurs. Ces avantages justifient que les experts en développement et les gouvernements fassent des efforts pour encourager l'utilisation des innovations afin de faciliter l'inclusion financière des populations du Sud.

Il a ajouté que le mobile money est construit autour d'un ensemble d'acteurs ayant des intérêts divergents et généralement les intérêts des entreprises l'emportent sur ceux de la population. Par conséquent, la mise en œuvre des innovations ne doit pas dépendre que de facteurs techniques, juridiques et réglementaires, mais également de la compréhension des conditions socio-économiques des populations.

A la lumière de ces observations, Dr Maliehe a indiqué qu'il est nécessaire d'élargir le rôle des banques centrales et autres régulateurs pour gérer efficacement les entreprises et protéger les intérêts de la population. Il a exhorté les banques centrales à réaliser que la finance numérique n'est pas une panacée mondiale. Certaines situations exigent que des études préalables soient menées afin que les personnes pauvres puissent tirer des avantages socio-économiques du mobile-money et des paiements numériques.

Le deuxième sous-thème «*Technologies financières : opportunités et défis pour les banques centrales africaines*» a été présenté par M. Adrien Delcroix de la BCE. Il a d'abord défini les Fintech comme une innovation financière basée sur la technologie et qui pourrait déboucher sur de nouveaux modèles économiques, des applications, des processus ou des produits ayant un impact tangible sur les marchés financiers et les institutions financières, ainsi que sur l'offre de services financiers.

Sa communication a été principalement centrée sur les principaux produits et services issus des Fintech, les moteurs des innovations dans les Fintech, les implications pour la structure du secteur financier et les risques et opportunités des Fintech ainsi que le rôle des banques centrales et des régulateurs.

En ce qui concerne les principaux produits et services Fintech, il a identifié trois domaines d'innovation, à savoir : (1) les services de crédit, de dépôt et de collecte de fonds (par exemple le crowdfunding, les banques mobiles et la notation de crédit, etc.) ; (2) les services de paiements, de compensation et de règlement qui pourraient porter sur des montants réduits (par exemple les portefeuilles mobiles, les transferts de poste à poste et les monnaies numériques) ou sur de gros montants (par exemple les réseaux de transfert de valeur, les ventes en gros de réserves extérieures, les plate-formes numériques de change) ; (3) les services de gestion d'investissement (par exemple le commerce à haute fréquence, la copie de traders, le commerce électronique et le robot-conseil). Outre ces produits et services déterminants, il a fait état des services d'appui au marché, notamment les portails et les agrégateurs de données, la technologie des registres distribués (blockchain, contrats intelligents), l'internet des objets (les technologies mobiles, l'intelligence artificielle, les écosystèmes, la sécurité et le cloud computing).

M. Delcroix a ajouté que les attentes changeantes des clients et l'évolution de la technologie, notamment l'internet, les méga-données, la technologie mobile et la puissance de calcul, sont les principaux moteurs interdépendants des innovations Fintech, ainsi que des changements dans la réglementation financière et la structure du marché. Il a soutenu que l'impact des innovations Fintech sur le secteur bancaire dépendra du taux d'adoption de la technologie sous-jacente dans la société et du degré, ainsi que de l'omniprésence du savoir-faire technologique au sein de la population entière. Il a noté que plus le rythme du changement est rapide, plus son impact sur la société sera important.

S'agissant des implications pour la structure du secteur financier, M. Delcroix a indiqué que trois grands scenarii pourraient être envisagés. Dans le premier scenario, les banques pourraient adopter la tendance numérique et faire équipe avec les entreprises Fintech. Dans le deuxième scenario, les Fintech pourraient briser la chaîne de valeur de la banque traditionnelle et ces dernières finiraient par perdre des revenus, des parts de marché et des contacts directs avec les clients. Enfin, les entreprises Finfech pourraient être englouties par les grandes technologies, telles que le groupe « Ali Baba » ou d'autres chaînes de vente de détail.

M. Delcroix a identifié les risques liés aux innovations Fintech sur les consommateurs, les banques et le système bancaire. En ce qui concerne les risques sur les consommateurs, il a fait état, notamment, de la confidentialité des données, la sécurité des données et la discontinuité des services bancaires. S'agissant des risques sur les banques et le système bancaire, il a noté notamment les risques de nature stratégique, ceux qui affectent la rentabilité, les risques cybernétique, ceux liés au blanchiment d'argent et au financement du terrorisme, et le risque de liquidité ainsi que ceux liés à l'évolution des sources de financement bancaire.

Toutefois, il a ajouté que les innovations Fintech offrent des opportunités aux consommateurs, aux banques et au système bancaire. Pour les consommateurs, il s'agit de l'inclusion financière, la fourniture de services bancaires de meilleure qualité, plus adaptés, et des services bancaires plus rapides ainsi que des coûts de transaction plus faibles. Pour les banques et le système bancaire, il a noté en particulier des processus bancaires améliorés et plus efficaces, l'utilisation innovante des données à des fins de marketing et de gestion des risques, l'impact positif potentiel sur la stabilité financière, induit par une concurrence accrue et la Réglementation Technologique (RegTech).

Présentant le rôle des banques centrales et des régulateurs, M. Delcroix a indiqué que l'innovation dans le secteur financier influence la façon dont les autorités mènent les activités de réglementation et que les initiatives réglementaires affectent également l'orientation et la rapidité de la transformation dans le secteur financier. Il a recommandé que pour créer un environnement propice à l'innovation, les banques centrales et les

régulateurs doivent soigneusement équilibrer les avantages pour les entreprises et les ménages avec les risques potentiels. Ils doivent également revoir le cadre réglementaire afin de s'assurer qu'il est neutre sur le plan technologique et maintenir des conditions de concurrence équitables entre les nouveaux entrants et les opérateurs historiques et prendre en compte les différents niveaux de risques. Afin de promouvoir des services de paiement efficaces et sûrs, ils devraient éviter la fragmentation en promouvant la normalisation et l'interopérabilité techniques et renforcer la cyber-résilience en encourageant les acteurs du marché à investir dans une stratégie de cybersécurité et un plan d'intervention à part entière.

Le troisième sous-thème «*Cybersécurité : Implications pour les pratiques de supervision*» a été présenté par M. Danny Brando de la Federal Reserve Bank de New York. La présentation a porté sur la supervision du système de la Réserve fédérale, les observations positives au-delà de l'assainissement informatique et l'approche de supervision.

Dans sa présentation, M. Brando a indiqué que la mission de supervision de la Réserve fédérale vise à promouvoir la stabilité du système financier et à minimiser et maîtriser les risques systémiques par un suivi actif et un engagement aux États-Unis et à l'étranger. La supervision du Système de la Réserve fédérale a également pour objectif de promouvoir la sécurité et la solidité des institutions financières, à l'échelle individuelle, et à surveiller leur impact sur le système financier dans son ensemble.

Sur le plan empirique, M. Brando a fait état de statistiques troublantes. En effet, l'étude de l'Institut Ponemon menée en 2017 sur le coût d'une violation de données a révélé que le délai moyen d'identification d'une violation est de 191 jours. En outre, selon le rapport Verizon de violation des données de 2017, une proportion de 24% de toutes les cyber violations et incidents ont affecté des institutions financières (taux le plus élevé de tous les secteurs) et 73% des cyber-violations étaient liées à des motivations d'ordre financier.

Ces violations ont également permis au système de la Réserve fédérale de faire plusieurs observations positives au-delà de l'assainissement informatique. En effet, ils ont permis de mieux identifier et comprendre les menaces, dans le but d'apporter une réponse adéquate. A cette fin, il devrait y avoir une simplification de l'infrastructure et des pratiques de contrôle de sécurité normalisées. Des observations positives ont également été faites concernant l'intégration dans la gestion des risques de l'entreprise et la compréhension au niveau du Conseil d'administration. De plus, l'accent devrait être mis sur le développement et la fidélisation des cyber-talents. Il devrait également y avoir une infrastructure pertinente suffisamment résiliente à la cybercriminalité. Ainsi, l'objectif est de rendre autonomes les entreprises, afin de leur donner les moyens de prévenir toutes sortes d'attaques.

En ce qui concerne l'approche prudentielle, il convient de noter que toutes les institutions américaines s'appuient principalement sur le cadre volontaire de l'Institut National des Normes et de la Technologie (NIST) et sur le manuel des technologies de l'information du Conseil Fédéral d'Examen des Institutions Financières (FFIEC). L'approche de supervision devrait également s'appuyer sur les régulateurs financiers américains, à travers une harmonisation des pratiques en matière de supervision de cybersécurité. L'approche adoptée implique également une participation aux efforts nationaux et internationaux pour identifier et traiter les cyber-risques liés au secteur financier. Il vise à tirer parti des données pour analyser l'interdépendance commerciale et technologique des marchés financiers critiques. Le système de la Réserve fédérale continue également de pousser les entreprises à améliorer l'assainissement informatique de base.

En conclusion, M. Brando a indiqué que pour assurer la survie en matière de cybersécurité, il est nécessaire de mettre l'accent sur la sensibilisation et d'avoir plusieurs mots de passe.

3.2. Session plénière 2 : expériences des banques centrales de l'ABCA

Dix banques centrales membres de l'ABCA ont présenté leurs expériences par rapport au thème central du Séminaire.

4. TRAVAUX EN ATELIERS

Les délégués ont échangé sur trois thèmes à travers des ateliers.

Atelier I : « Implications des technologies financières (y comprises les monnaies numériques et les technologies blockchain) sur la politique monétaire et la stabilité financière en Afrique »

Observations

1. Les domaines d'innovation financière identifiés au cours des discussions étaient : le mobile money, les crypto-monnaies et les technologies de registres distribués (DLT), l'intelligence artificielle (IA), y compris l'utilisation de l'apprentissage automatique (ML) soutenue par la croissance du Big Data et la biométrie.
2. Il a été noté que le mobile money a eu une empreinte dans la plupart des pays, mais n'a pas eu suffisamment de succès dans certains pays. Le mobile-money a été initialement utilisé comme un moyen de transfert d'argent. Il offre à présent des services de crédit, d'épargne et d'assurance.
3. Le mobile money favorise l'inclusion financière en intégrant davantage de personnes dans le système financier formel, ce qui améliore le mécanisme de transmission de la politique monétaire.
4. Les crypto-monnaies ont été considérées comme pouvant avoir l'impact potentiel le plus important sur la stabilité monétaire et financière, malgré leur utilisation actuellement limitée.
5. Une distinction a été faite entre les concepts de crypto-monnaies privées, telles que le Bitcoin, l'Ethereum et le Monero, et les monnaies numériques des banques centrales (CBDC).
6. Il existe différents points de vue sur l'approche des crypto-monnaies, allant de la nécessité de mettre en place une réglementation de l'utilisation de ces monnaies pour les échanges à l'interdiction de l'acceptation de ces crypto-monnaies par les banques.
7. Les analyses basées sur l'intelligence artificielle (AI) pourraient être utilisées pour évaluer la stabilité financière, la réglementation en matière de supervision, les opérations d'open market, l'évaluation du crédit, les conseils en investissement, etc. La biométrie pourrait également être utilisée pour rendre plus sûres l'identification et l'authentification des services financiers.
8. L'arbitrage en matière de réglementation. En raison du caractère transversal des services liés au mobile money, la réglementation devra impliquer les opérateurs de réseaux mobiles et les régulateurs de services financiers.

9. Il n'existe actuellement aucun accord sur la façon dont les crypto-monnaies devraient être considérées et leur traitement réglementaire est donc imprécis. Globalement, certains les considèrent les crypto-monnaies comme des devises alors que d'autres les considèrent comme des marchandises.

Recommandations

1. Les fournisseurs de services devraient promouvoir l'interopérabilité entre les services.
2. Les banques centrales devraient développer ou mettre à jour les cadres réglementaires pour adopter les innovations Fintech actuelles.
3. Les banques centrales devraient coopérer en partageant les informations sur les développements des technologies financières, les activités cybernétiques et illicites.
4. Les banques centrales devraient jouer un rôle d'éducation financière pour s'assurer que les citoyens comprennent les nouvelles technologies.
5. Les banques centrales devraient continuer à suivre l'évolution des technologies financières en vue d'assurer le développement rapide des dispositifs réglementaires, tels que la définition des crypto-monnaies. A cet égard, les banques centrales devraient envisager de mettre en place des structures telles que les « Unités Fintech » et les instruments de régulation.
6. **L'ABCA devrait mettre en place un Groupe de travail Fintech pour harmoniser les approches sur les développements des technologies financières.**

Atelier II : « Services Financiers Mobiles (SFM) : aperçu - risques et défis potentiels ainsi que les recommandations pour les Banques Centrales Africaines »

<u>Introduction</u>

Les innovations dans les technologies financières ont permis au secteur privé, aux gouvernements centraux et aux banques d'offrir des services financiers aux communautés précédemment marginalisées et peu intégrées en Afrique. Les téléphones mobiles en particulier sont passés d'objet de luxe ou de symboles de statut social à des biens de nécessité. Les appareils sont utilisés comme canaux d'accès aux services financiers.

Les services financiers pouvant être fournis par le biais des appareils mobiles comprennent :

1. Les règlements et les envois de fonds des migrants.
2. Le crédit bancaire et l'épargne.
3. Les services d'assurance et de certification.
4. La sécurité et la gestion des investissements.
5. Le soutien au marché.

Risques potentiels / défis

1. **Non-respect de la législation contre le blanchiment des capitaux / lutte contre le financement du terrorisme**

   Dans certaines juridictions en Afrique, les documents d'identité officiels et l'enregistrement de la carte SIM ne sont pas en place pour assurer l'identification des abonnés, ce qui peut constituer un défi pour la conformité à la législation contre le blanchiment des capitaux et la lutte contre le financement du terrorisme.

2. **Risques de cybersécurité**

   Les services financiers mobiles sont exposés aux menaces de la cybersécurité dues aux différents acteurs de la chaîne de valeur tels que les banques, les télécoms, les fournisseurs de solutions et les utilisateurs finaux (les consommateurs des services mobiles).

3. **Arbitrage en matière de réglementation**

   Il existe différentes parties impliquées dans l'offre de services financiers mobiles qui relèvent de différents régulateurs. Différentes normes et réglementations peuvent conduire à des perspectives contradictoires et divergentes, ce qui crée des opportunités d'arbitrage en matière de réglementation.

4. **La responsabilité pour la protection des consommateurs et des données n'est pas clairement située**

   L'implication de diverses parties prenantes dans l'offre des services financiers mobiles peut conduire à une confusion sur les responsabilités concernant la protection du consommateur.

5. **Problèmes de résilience du fournisseur de services**

   Dans certaines juridictions, les fournisseurs de services ne sont pas en mesure d'assurer la disponibilité continue et la reprise rapide des services. Cette situation affecte la qualité du service et dissuade les consommateurs d'utiliser les services financiers mobiles.

6. **Taxes, taux d'intérêt élevés et charges**

   Les taxes imposées par les gouvernements sur les transactions réalisées par paiement mobile les rendent coûteux pour les clients, ce qui est en contradiction avec les stratégies d'inclusion financière. En outre, le taux d'intérêt élevé et les charges sur les services constituent un goulot d'étranglement majeur pour le développement des services financiers mobiles.

Récommandations

1. **Collaboration locale et régionale entre les régulateurs (MOUs) et les parties prenantes clés**

   Il est nécessaire que différents régulateurs impliqués dans la fourniture de services financiers mobiles collaborent à cet égard.

2. **Réglementation et supervision basées sur la prévention des risques**

   Une approche symétrique et basée sur le risque doit être adoptée au lieu d'une approche traditionnelle et normalisée de la supervision. Les régulateurs devraient adopter la technologie dans le cadre de supervision.

3. **Cadres juridiques, contre le blanchiment des capitaux, de lutte contre le financement du terrorisme et de cybersécurité**

   Des cadres juridiques, de lutte contre le blanchiment des capitaux et le financement du terrorisme et pour la cybersécurité devraient être en place.

4. **Directives et réglementations**

   Les lignes directrices et les réglementations publiées pour les modalités d'offre de services financiers mobiles devraient être périodiquement examinés et évalués pour tenir compte des innovations.

5. **Bureaux d'information sur le crédit obligatoires**

   Tous les fournisseurs de services financiers mobiles doivent être interfacés avec le bureau d'information sur le crédit, afin que la solvabilité appropriée du client et des fournisseurs soit vérifiée en temps réel. La banque centrale devrait veiller à ce que le bureau d'information sur le crédit soit en place et pleinement fonctionnel.

6. **La sensibilisation des clients**

   Les organismes de réglementation devraient s'assurer que les fournisseurs de services et les organismes de réglementation ont mis en place un programme de sensibilisation et d'information des consommateurs pour éviter les utilisations malveillantes de ces services.

7. **Interface conviviale pour la clientèle**

   Les fournisseurs de services devraient veiller à ce que les interfaces pour les services financiers mobiles soient conçues de manière à répondre aux besoins des différentes catégories de consommateurs.

8. **Les stratégies nationales sont la clé du succès des services financiers mobiles**

   Des stratégies nationales de promotion des services financiers mobiles devraient être développées.

Atelier III : « Cybersécurité et stabilité financière : défis pour les banques centrales africaines »

Observations

Il existe de nombreux exemples d'incidents cybernétiques à grande échelle pour illustrer l'importance de la cybersécurité pour la préservation de la stabilité financière.

Les domaines de cyber risques qui mettent en avant l'importance de la cybersécurité dans le contexte des banques centrales et du système financier international incluent :

1. La fraude financière, généralement séparée en deux domaines :

    a. A petite échelle - Fraude cybernétique ciblant les systèmes de paiement, y compris les services bancaires sur Internet, les paiements en argent mobile et autres ;

    b. A grande échelle et réserves / avoirs de la Banque centrale - Fraude financière plus importante, comme la fraude liée à Swift constatée sur les réserves des banques centrales et l'impact potentiel sur les systèmes de paiement de gros.

2. L'espionnage, les informations sensibles et/ou les fuites de données :

    a. la fuite d'informations sensibles soutenant ou concernant les décisions stratégiques des banques centrales pourrait avoir un impact important pour les banques centrales ;

    b. la fuite d'autres informations sensibles telles que les rapports des conseils d'administration pourrait exposer les banques centrales à des risques.

3. Les perturbations de l'infrastructure critique :

    a. en raison du rôle critique joué par les banques centrales et de la fourniture de systèmes RTGS, l'infrastructure concernée de la banque centrale pourrait être une cible clé ;

    b. des attaques ciblées sur la région sont également possibles ;

    c. aussi bien l'infrastructure de la banque centrale, que l'infrastructure sous-jacente, par exemple l'électricité et les fournisseurs de services pourraient être concernés.

4. Des risques de réputation affectant la confiance peuvent résulter d'une cyber-violation.

Défis

L'interconnectivité et l'interconnexion des acteurs financiers, y compris les banques centrales, créent le contexte dans lequel les défis ci-dessous doivent être relevés :

1. Compétences, ressources et capacités inadéquates - Les banques centrales africaines disposent d'un grand nombre de compétences informatiques approfondies, mais la demande dépasse de loin l'offre.

2. Sensibilisation à la cybersécurité / la culture du numérique - Les banques sont vulnérables aux cyber-menaces en raison de problèmes de comportement, en particulier du fait de l'évolution constante des menaces.

3. L'absence de politiques, de directives et de lois normalisées rend les banques centrales africaines vulnérables en raison des mesures de sécurité incohérentes appliquées.

4. Les mises à jour de la sécurité logicielle, la complexité et les compétences associées à la gestion des logiciels rendent les banques centrales vulnérables aux attaques.

5. Le manque de gestion adéquate des actifs est une vulnérabilité majeure car il est difficile de protéger les infrastructures et les informations si la connaissance de l'environnement n'est pas suffisante.

6. Le manque de séparation des tâches en raison de la taille des institutions est une vulnérabilité spécifique dans le contexte africain.

7. L'accent est mis de manière incohérente sur la cyber-résilience et le test des dispositifs de récupération.

8. Il n'y a pas de test de pénétration et d'évaluation standardisé qui soit largement accepté pour assurer la cyber-préparation.

9. Il est difficile de mettre en place une capacité de détection / surveillance et d'intervention à la hauteur des enjeux.

10. Le manque de partage d'informations et de renseignements au sein de diverses institutions à travers l'ABCA.

11. Les initiés malveillants qui exploitent les vulnérabilités demeurent l'une des principales préoccupations.

12. Il y a eu une augmentation des compromis par l'intermédiaire de fournisseurs de services tiers.

13. Les menaces à la sécurité physique ont un impact direct sur la cybersécurité.

Recommandations

1. Chaque banque centrale devrait concevoir et mettre en œuvre un programme de cybersécurité qui aborde les différents aspects de la mise en place d'une capacité interne qui assure la prévention, la détection et la réponse aux cyber-incidents. Le programme doit être aligné sur les meilleures pratiques internationales et permettre la collaboration.

2. Création d'un groupe interdépartemental de cybersécurité (impliquant toutes les parties prenantes clés et les départements concernés) au sein de chaque banque centrale. Ce groupe de travail a besoin du soutien approprié du conseil d'administration et de la haute direction, couvrant tous les principaux domaines recommandés par les meilleures pratiques et réglementations internationales (CPMI-OICV, BIS CPMI Wholesale Payment Security Task Force, ISO, NIST, SWIFT CSP).

3. La collaboration entre les banques centrales devrait porter sur le partage des informations et les compétences internes. La collaboration devrait également inclure les institutions financières sous-jacentes dès que cela est possible, car les structures sous-jacentes dans chaque juridiction sont nécessaires pour la facilitation de la collaboration. Cela nécessitera l'expansion de la collaboration aux niveaux national, régional et international. Cela comprendra ensuite les gouvernements et d'autres parties prenantes nationales clés.

4. **L'ABCA devrait faciliter la mise en place d'un groupe de travail / équipe de travail cybernétique couvrant les domaines suivants :**

   a. Supervision, prévention et réglementation :

      i. Partager l'information sur les lois, les règlements, les cadres et les pratiques pour avoir une approche cohérente à travers l'Afrique ;

      ii. Mesurer le potentiel d'évaluation de la cyber-préparation dans les banques centrales sur la base d'une approche de mesure commune ;

      iii. Explorer des évaluations normalisées des menaces cybernétiques, par exemple en se basant sur les compétences du Californian Basic Educational Skill Test (CBEST) ou du Threat Intelligence Based Ethical Red Teaming (TIBER-EU).

   b. Cyber-menace et partage de renseignements :

      i. Partage des informations sur les menaces qui ont une incidence sur les banques centrales et qui peuvent aider à la détection ;

      ii. Définir des protocoles de partage d'informations (par exemple en utilisant le système des signaux de circulation, indiquant avec qui les informations peuvent être partagées) ;

      iii. La mise en place de plates-formes et de technologies de partage, à l'aide par exemple des Malware Information Sharing Plateform (MISP) pour permettre un partage efficace en temps réel des informations techniques sous-jacentes sur les menaces.

   c. Cyber-réponse et rétablissement :

      i. Mettre en place des structures de communication pour coordonner la cyber-réponse aux incidents sur tout le continent et à l'international ;

      ii. Organiser des cyber-simulations pour tester l'état de préparation informatique des membres de l'ABCA.

   d. Mise en place de programmes de développement de compétences cybernétiques pour les banques centrales membres, comprenant :

      i. Le détachement de ressources par le biais de programmes de partenariat ;

      ii. L'organisation de séminaires de formation et de visites sur site facilitées par l'ABCA pour le transfert de compétences et l'apprentissage par les pairs ;

iii. La mise en place de partenariats internationaux pour aider au développement des compétences avec d'autres banques centrales et acteurs du secteur financier.

5. CEREMONIE DE CLOTURE

La cérémonie de clôture a été présidée par M. Annour Mahamat Hassan, Directeur National de la BEAC pour le Tchad. Elle a été marquée par la présentation des conclusions et recommandations du séminaire. Par la suite, les participants ont exprimé leur gratitude à Son Excellence le Président Idriss Deby Itno, au Gouvernement et au peuple du Tchad, ainsi qu'à l'Honorable Gouverneur Abbas Mahamat Tolli et au personnel de la BEAC pour leur chaleureuse hospitalité. En déclarant le séminaire clos, M. Hassan a indiqué que les conclusions du séminaire pourraient fournir des contributions essentielles pour assurer la stabilité financière, une grande grande inclusion financière et une meilleure mise en œuvre de la politique monétaire dans les banques centrales membres. Il a également souhaité un retour en toute sécurité aux participants vers leurs destinations respectives.

Fait à N'Djamena, République du Tchad, le 16 Mai 2018

Annexe

LISTE DES PARTICIPANTS

NOM/NAME	TITRE/TITLE	INSTITUTION	Email
1. M. Josephate Zola	Adjoint / Directeur	**BCEAO**	jzola@bceao.int
2. M. Mohamed Traoré	Chef de Service		motraore@bceao.int
3. M. Annour Mahamat Hassan	Directeur National	**BEAC**	annour@beac.int
4. M. Taoukreo Hemwue	Adjoint / Directeur National		taoukreo@beac.int
5. M. Abba Fanta Madji	Adjoint / Directeur National		abbe@beac.int
6. M. Eloundou Ndeme Jacques	Chef de service		jeloundou@beac.int
7. M. Ducor Mshaa	Chef de service		ducor@beac.int
8. M. Mbede Jean-luc	Responsable Sécurité		mbedejl@beac.int
9. M. Siazo Gini Frederic	Directeur	**BANQUE CENTRALE DU CONGO**	siazo@bcc.cd
10. M. Tshilumba Wa Tshilumba	Manager		tshilumba2050@gmail.com
11. Mr. Ahmed Monir Mohamed	Fintech Specialist	**CENTRAL BANK OF EGYPT**	ahmed.monir@cbe.org.eg
12. Mr. Sheriff Touray	Principal Economist	**CENTRAL BANK OF THE GAMBIA**	shtouray@cbg.gm
13. Dr. Settor Kwabla Amediku	Director	**BANK OF GHANA**	settor.amediku@bog.gov.gh
14. Mr. Michael Ewusi Mensah	Director		michael.mensah@bog.gov.gh

15. Mr. Simon Gichuki	Manager Bank Sup.	**CENTRAL BANK OF KENYA**	gichukisg@centralbank.go.ke
16. Mr. Mike Ombuna	IS Auditor, Bank. Sup.		Ombunamg@centralbank.go.ke
17. Mr. Diakae Al Lewis	Assistant Director	**CENTRAL BANK OF LIBERIA**	dallewis@cbl.org.lr
18. José J. Randriamampionona	Respons. Cont. Séc.	**BANKY FOIBIEN'I MADAGASIKARA**	jj.randriamampionona@bfm.mg
19. M. Saadna Ahmed Jiddou	Directeur	**BANQUE CENTRALE DE MAURITANIE**	saadna@bcm.mr
20. M. Ahmed Baba Moussa Welad	Chef de projet		abwelad@bcm.mr
21. Mr. Gawtam Raiy Kallychurn	Chief Inf. Security Officer	**BANK OF MAURITIUS**	Gawtam.kallychurn@bom.mu
22. Mr. Aderito Abilio Pilica	IT Examiner	**BANK OF MOCAMBIQUE**	aderito.pilica@bancomoc.mz
23. Mr. José Nelson Da Costa Brazäo	Information Sec. Analyst		nelson.brazao@bancomoc.mz
24. Dr. Isa Audu	Deputy Director	**CENTRAL BANK OF NIGERIA**	iaudu@cbn.gov.ng
25. Mr. Victor Ugbem Oboh	Assistant Director		voboh@cbn.gov.ng
26. M. Nimersio Trindade	Directeur Adjoint	**BANCO CENTRAL DE SAO TOME E PRINCIPE**	ntrindade@bcstp.st
27. M. Djalma Trovoada	Tech. Informatique		dtrovoada@bcstp.st
28. Mr. Morlai Bangura	Director	**BANK OF SIERRA LEONE**	mbangura@bsl.gov.sl
29. Mr. Crispin D. George	Assistant Director		cgeorge@bsl.gov.sl
30. Mr. Francis Selialia	Senior Manager	**SOUTH AFRICAN RESERVE BANK**	francis.selialia@resbank.co.za
31. Mr. Gerhard Cronje	Head – Cyber & Info. Sec.		gerhard.cronje@resbank.co.za
32. Mr. Gerhard Van Deventer	Senior Fintech Analyst		gerhard.vandeventer@resbank.co.za
33. Mr. Jabulane Caiphas Dlamini	Head - Financial Sector Strategy	**CENTRAL BANK OF SWAZILAND**	jabulaned@centralbank.org.sz
34. Ms. Philile Nxumalo	General Manager		phililen@centralbank.org.sz
35. Mr. Bhekisisa Sicelo Tsabedze	Economist		bhekisisat@centralbank.org.sz
36. M. Enis Belhassen	Directeur	**BANQUE CENTRALE DE TUNISIE**	enis.belhassen@bct.gov.tn
37. M. Abderrahmen Miled	Sous-Chef de Service		abderrahmen.miled@bct.gov.org

38.	Mr. Enoch Kasajja Matovu	Risk Quantitative Analyst	**BANK OF UGANDA**	ematovu@bou.or.ug
39.	Ms Kugonza Rose Kuteesa	Head-Inf &Publication		rkuteesa@bou.or.ug
40.	Mr. Mathews Lungu	Acting Director -ICT	**BANK OF ZAMBIA**	plungu@boz.zm
41.	Mr. Nicholas Masiyandima	Principal Economist	**RESERVE BANK OF ZIMBABWE**	nmasiyandima@rbz.co.zw
42.	Mr. Douglas Muranda	Head Oversight & Risk Manag.		dmuranda@rbz.co.zw
43.	Dr Lucas Kamau Njoroge	Economist	**COMESA MONETARY INSTITUTE**	lnjoroge@comesa.int
44.	Mr. Alieu Ceesay	Principal Economist	**AMAO / WAMA**	aoceesay70@yahoo.com
45.	Mr. Ismaila Jarju	Director	**WEST AFRICAN MONETARY INSTITUTE**	ijarju@wami-imao.org
46.	Dr. Morenakemang Sean Maliehe	Post - Doctoral Researcher	**UNIVERSITY OF PRETORIA**	seanmaliehe@gmail.com
47.	Mr. Mark Yeon Wook Choi	Manager CBIAS	**FEDERAL RESERVE BANK OF NEW YORK**	mark.choi@ny.frb.org
48.	M. Hugues Tsafack Kamewe	Financial Sector Advisor	**MAKING FINANCE WORK FOR AFRICA**	h.kamewe-tsafack@afdb.org
49.	M. Jean Claude Nachega	Représentant Résident	**FOND MONETAIRE INTERNATIONAL**	jnachega@imf.org
50.	Mr. Papa Lamine Diop	Executive Secretary	**AACB SECRETARIAT**	pdiop@bceao.int
51.	Mr. Acho Theodore Yapo	Research Officer		atyapo@bceao.int
52.	Mr. Balamine Diane	Research Officer		bdiane@bceao.int
53.	Mr. Arthur Konan Koffi	Webmaster		kyakoffi@bceao.int