Association des Banques Centrales Africaines

Association of African Central Banks

SÉMINAIRE CONTINENTAL AU TITRE DE L'ANNÉE 2025 SUR LE THÈME :
« CYBER-RISQUES ET TECHNOLOGIES FINANCIÈRES INNOVANTES :
DÉFIS ET MESURES STRATÉGIQUES »

Organisé par : Bank Al-Maghrib

(Rabat, Maroc, du 21 au 23 juillet 2025)

RAPPORT

1. INTRODUCTION

Conformément à la décision prise lors de la réunion du Conseil des Gouverneurs tenue à l'Île Maurice le 4 septembre 2024, le Séminaire Continental au titre de l'année 2025 de l'Association des Banques Centrales Africaines (ABCA) a été accueilli par Bank Al-Maghrib. Il s'est tenu du 21 au 23 juillet 2025 à Rabat au Maroc sur le thème « Cyber-risques et technologies financières innovantes : défis et mesures stratégiques ». Quatre-vingt-cinq délégués provenant des Banques Centrales membres et des institutions régionales et internationales ont participé au Séminaire. La liste des participants est jointe en annexe.

2. CÉRÉMONIE D'OUVERTURE

La cérémonie d'ouverture était présidée par Monsieur Abdellatif JOUAHRI, Honorable Gouverneur de Bank Al-Maghrib.

Dans ses remarques liminaires, Dr Djoulassi Kokou OLOUFADE, Secrétaire Exécutif de l'ABCA, au nom du Président de l'Association, Dr Rama Krishna SITHANEN, G.C.S.K., Honorable Gouverneur de Bank of Mauritius, a exprimé ses sincères remerciements à Bank Al-Maghrib pour avoir accepté d'accueillir le Séminaire Continental au titre de l'année 2025 et pour avoir fait des efforts exceptionnels dans l'organisation dudit Séminaire. Il a exprimé sa profonde gratitude au Chef de l'État et Commandeur des croyants, Sa Majesté le Roi Mohammed VI - que Dieu l'assiste -, ainsi qu'au Gouvernement et au peuple marocains pour les excellentes dispositions prises afin de rendre le séjour agréable. Il a également remercié les experts d'avoir accepté généreusement de partager leurs connaissances sur les sujets discutés au cours du Séminaire. Par ailleurs, il a félicité les participants pour leur participation massive, démontrant leur ferme engagement à contribuer au processus d'intégration monétaire et financière en Afrique.

En outre, le Secrétaire Exécutif a ajouté que l'ABCA travaille pour atteindre ses objectifs en promouvant l'échange d'idées et d'expériences liées aux questions monétaires, financières, bancaires et économiques en Afrique. Le Séminaire Continental, qui a lieu chaque année, est un événement important pour atteindre ces objectifs. Le thème du Séminaire, axé sur les cyber-risques et les technologies financières innovantes, s'inscrit dans un contexte de transformation numérique accélérée des systèmes financiers africains, marqué notamment par l'essor des services mobiles, de l'Intelligence Artificielle (IA), des plateformes de paiement numériques et du cloud computing. L'Afrique se distingue par une dynamique dans les innovations inclusives, illustrée par une forte progression des transactions via le mobile money.

Cependant, cette digitalisation croissante s'accompagne d'une exposition accrue aux risques cybernétiques, compromettant la stabilité financière, la protection des données et la confiance des usagers. Le Secrétaire Exécutif a souligné l'ampleur des menaces identifiées par la Banque Mondiale et INTERPOL, notamment la recrudescence des attaques par ransomware et des fraudes technologiques, qui affectent aussi bien les Banques Centrales que les services publics et les entreprises privées. Dans ce contexte, le Séminaire vise à analyser les opportunités

offertes par la technologie pour renforcer l'inclusion financière, tout en identifiant les vulnérabilités et en partageant les bonnes pratiques réglementaires.

Pour conclure son allocution, le Secrétaire Exécutif a exprimé sa confiance quant à la qualité des échanges et des recommandations à soumettre aux Gouverneurs lors des prochaines Réunions Annuelles de l'ABCA à Yaoundé, en novembre 2025.

Dans son discours d'ouverture, Monsieur Abdellatif JOUAHRI, Honorable Gouverneur de Bank Al-Maghrib, a souhaité la bienvenue à tous les participants ainsi qu'un agréable séjour dans la ville de Rabat, capitale du Royaume du Maroc. Il a aussi exprimé sa gratitude à l'ABCA pour avoir bien voulu accepter la proposition de Bank Al-Maghrib d'accueillir un événement aussi important au Maroc qui a enregistré des participants provenant des Banques Centrales africaines et des institutions régionales et internationales partenaires.

Il a souligné que le thème de cette année, « Cyber-risques et technologies financières innovantes : défis et mesures stratégiques », est particulièrement pertinent et opportun, compte tenu du fait que ces dernières années ont été marquées par une vague d'innovations numériques qui impactent profondément les pays africains, ouvrant des perspectives sans précédent, notamment pour le secteur des services financiers. Il a souligné qu'il revient aux Banques Centrales de soutenir l'innovation pour répondre à leurs propres besoins et à ceux du secteur financier privé, tout en restant vigilantes quant aux risques qui leur sont associés et en développant leurs capacités à faire face aux menaces qui pèsent sur la stabilité du système monétaire et financier.

Selon le Gouverneur de Bank Al-Maghrib, les stratégies digitales, notamment en matière de cybersécurité pour les paiements numériques transfrontaliers et la lutte contre le blanchiment d'argent/financement du terrorisme, nécessitent une coopération régionale portée par l'ABCA pour partager les meilleures pratiques et cadres réglementaires. Les technologies financières sont un moteur de développement, surtout dans les économies émergentes, révolutionnant la finance par l'élargissement de produits, l'amélioration des services, la réduction des coûts et la réinvention de l'expérience client.

L'Honorable Gouverneur de Bank Al-Maghrib a précisé que le mobile money, les virements instantanés et les transferts Peer-to-Peer ainsi que les FinTechs ont permis des performances notables dans plusieurs pays africains. De nouveaux modèles de crédit basés sur des données alternatives émergent, facilitant l'accès pour les petites entreprises et les particuliers. Les banques africaines doivent s'adapter en nouant des partenariats avec les FinTechs pour faire face à la croissance des "Big Techs" dans le crédit stimulée par l'IA.

Il a indiqué qu'un rapport de McKinsey (2024) prévoit une multiplication par cinq des revenus des FinTechs africaines d'ici à 2028, bien que cette croissance soit concentrée sur 11 marchés clés. Les défis des FinTechs incluent une rentabilité fragile, un accès limité aux financements, une pénurie de talents, une gouvernance perfectible et un cadre réglementaire insuffisant. Le développement de grandes plateformes technologiques mondiales (paiement, cryptoactifs et stablecoins), souvent hors cadre réglementaire, menace les systèmes de paiement nationaux et accentue la fragmentation.

Selon les propos du Wali de Bank Al-Maghrib, ces évolutions renforcent le rôle des Banques Centrales dans la régulation des systèmes de paiement et l'amélioration de leur résilience. Le Système Panafricain de Paiement et de Règlement (PAPSS), récemment intégré par Bank Al-Maghrib, est crucial pour l'innovation, l'efficience et l'autonomie du continent. Les autorités doivent encadrer les cryptoactifs et stablecoins qui posent des risques de blanchiment d'argent et de désintermédiation.

Il a ajouté que la transformation numérique rapide accroît l'exposition des Banques Centrales aux cyber-risques, rendant la cyber-résilience essentielle pour la stabilité financière. Aussi, la prolifération des attaques (phishing et fraudes aux paiements digitaux) exige un renforcement continu de la cybersécurité. En 2024, le coût moyen d'une cyberattaque pour une institution financière africaine dépassait 2,5 millions de dollars US, justifiant le constat de l'Interpol selon lequel l'Afrique est particulièrement vulnérable aux cyberattaques.

En outre, l'Honorable Gouverneur de Bank Al-Maghrib a mis l'accent sur les cyber-risques croissants à l'échelle mondiale et la nécessité de renforcer la cyber-résilience à travers une coopération, particulièrement au niveau continental. Le rôle du Groupe de Travail sur la cybersécurité de l'ABCA a été souligné, de même que les efforts du Maroc pour bâtir un cadre réglementaire robuste. Ensuite, le Wali de Bank Al-Maghrib a appelé à une mutualisation des efforts africains, à l'harmonisation réglementaire et à la création de centres d'excellence pour répondre collectivement aux défis numériques. Il a conclu en exprimant son soutien et ses remerciements au travail remarquable de l'ABCA et aux experts mobilisés pour ce Séminaire.

3. STRUCTURE DU SÉMINAIRE

Le Séminaire est structuré en deux séances plénières, un partage d'expériences et des travaux en ateliers. Pour la première séance plénière, des personnes ressources ont présenté trois sous-thèmes et la deuxième séance s'est articulée autour d'un partage d'expériences des représentants des Banques Centrales. Quant aux travaux en ateliers, ils ont porté sur trois sous-thèmes dont les conclusions et recommandations ont été restituées en plénière.

3.1. Session plénière 1 : Présentation des sous-thèmes

Cette session a été présidée par M. Wilner Junior BOUSSOUGOU, Chef de Service Administration des Systèmes des Opérations Financières et Activités Bancaires, Banque des États de l'Afrique Centrale (BEAC). M. Soulaimane LAHRECH, Fondateur de Talaty (FinTech), M. Mohamed TAZI, Directeur Sécurité des Systèmes d'Information, Groupe Attijariwafa Bank et Mme Najwa BENMADANI, Directrice du Pôle Investigations et Renseignement Financier, Autorité Nationale du Renseignement Financier (ANRF), ont présenté respectivement les sous-thèmes ci-après :

- Utilisation de l'analyse de Big Data et de l'Intelligence Artificielle pour le commerce transfrontalier et intercontinental ;
- Défis des technologies financières innovantes face aux risques croissants de cybercriminalité et aux stratégies d'inclusion financière ;

- Transactions numériques transfrontalières, cybersécurité et mesures pour lutter contre le blanchiment de capitaux et le financement du terrorisme.

a) Utilisation de l'analyse de Big Data et de l'Intelligence Artificielle pour le commerce transfrontalier et intercontinental

Dans sa présentation, M. LAHRECH a partagé avec les participants une réflexion sur les mutations profondes à l'œuvre dans le commerce transfrontalier, à la lumière des avancées en Intelligence Artificielle et en analyse des Big Data. Ces technologies ne relèvent plus du domaine expérimental car elles redéfinissent déjà, de façon concrète, les pratiques en matière de logistique, de conformité, de financement et d'analyse des risques et de traitement des flux. Pour les institutions publiques comme pour les opérateurs privés, elles représentent des leviers puissants d'efficacité, de réactivité et de transparence, dans un contexte où les échanges sont à la fois plus rapides, plus complexes et plus risqués.

Poursuivant son propos, le Présentateur a indiqué qu'il convient de poser les bases technologiques de cette transformation. L'IA, dans sa forme la plus évoluée, est désormais capable d'apprendre de l'expérience, de détecter des motifs subtils et de prendre des décisions en quasi-autonomie. Le Big Data, de son côté, permet de traiter des volumes massifs de données hétérogènes en temps réel, bien au-delà des capacités humaines ou des outils traditionnels. Il a également abordé des concepts plus avancés, comme l'IA générative, capable de produire des contenus ou des analyses inédites, et l'IA agentique, qui donne naissance à des systèmes autonomes pouvant agir seuls dans des environnements complexes. L'Intelligence Artificielle Générale (AGI), bien qu'encore théorique, ouvre la voie à des perspectives en rupture complète avec les méthodes traditionnellement admises dans tous les secteurs.

Cependant, M. LAHRECH a souligné que ces concepts ne restent pas abstraits. Ils trouvent aujourd'hui des applications concrètes, parfois déjà déployées à grande échelle. À titre d'exemple, des plateformes d'analyse prédictive permettent désormais d'anticiper la congestion portuaire grâce à la combinaison de signaux maritimes, d'imagerie satellite et de capteurs Internet des Objets (IoT). De telles solutions, en anticipant les goulets d'étranglement logistiques, offrent aux Banques Centrales des signaux avancés sur les flux commerciaux, bien avant la publication des données officielles, ce qui constitue un avantage stratégique pour piloter les politiques de change ou les réserves.

Le Présentateur a donné à titre d'exemple le cas emblématique de la douane japonaise qui utilise depuis plusieurs années un système automatisé de contrôle à base d'images par rayons X et d'apprentissage automatique. Ce système identifie en temps réel les marchandises illicites tout en améliorant la fluidité du commerce légal. Il renforce également la qualité des statistiques commerciales et contribue à limiter les sorties illicites de devises, une problématique bien connue de nombreuses autorités monétaires africaines.

Dans le domaine du commerce intra-africain, la solution Jetstream Africa illustre tout le potentiel d'une IA appliquée au financement du commerce. Connectant des milliers de PME et de transitaires dans 14 pays, elle automatise le traitement des documents, anticipe les

besoins de trésorerie et facilite les décaissements multidevises. Cette plateforme permet non seulement d'accélérer les échanges, mais aussi de fournir aux Banques Centrales une visibilité précieuse sur les besoins en devises et les risques de sous-facturation.

Enfin, le domaine de la conformité réglementaire connaît lui aussi une transformation en profondeur grâce aux IA agentiques. Ces agents intelligents surveillent en continu les listes de sanctions, les schémas d'actionnariat et les transactions, y compris sur blockchain, pour générer des alertes précises, avec un taux réduit de fausses alertes. Une démonstration de salle de crise ("Agentic Crisis Room") a même montré comment ces systèmes pouvaient appuyer en temps réel la réponse à des perturbations majeures du commerce mondial, tout en assurant la traçabilité des décisions pour les régulateurs. Au moment où les chaînes de valeur se reconfigurent, les règles de conformité se durcissent et la compétitivité devient vitale, l'intégration de l'Intelligence Artificielle et des Big Data dans les systèmes commerciaux n'est plus un choix technologique. C'est un impératif stratégique. La question n'est donc plus d'y aller simplement, mais plutôt de savoir comment accélérer la mise en œuvre au service des économies africaines.

Les discussions ont exploré de manière approfondie le rôle croissant de l'IA et des Big Data dans la transformation des opérations transfrontalières, notamment dans les domaines du commerce, de la conformité douanière, de la logistique et des paiements. Plusieurs cas d'usage ont été mis en avant, à savoir le contrôle autonome par rayons X, la surveillance des flux de devises, la gestion automatisée de la conformité et la détection avancée des risques financiers. Ces technologies, déjà déployées dans certains contextes, permettent des interventions plus rapides et précises des Banques Centrales, notamment en matière d'anticipation des chocs inflationnistes ou de choix de politiques d'intervention sur le marché des changes.

Les discussions ont souligné l'importance stratégique de développer des infrastructures souveraines pour traiter les données localement, tout en reconnaissant l'intérêt de coopérer à l'échelle régionale via des systèmes fédérés et sécurisés. L'un des enjeux clés évoqués est la qualité et l'harmonisation des données entre pays et institutions financières, condition sine qua non pour assurer l'efficacité des systèmes d'IA. Les intervenants ont insisté sur la montée en puissance des algorithmes explicables permettant de concilier puissance analytique et transparence décisionnelle. Le développement de modèles hybrides intégrant des indicateurs comportementaux, fiscaux ou politiques a également été mis en exergue pour améliorer la prévision de l'inflation.

Enfin, plusieurs questions ont porté sur la gouvernance, la cybersécurité, l'explicabilité des décisions prises sur la base d'analyses IA et l'adaptabilité de ces innovations dans les pays à faible capacité technique. L'exemple du Maroc, avec le déploiement de startups spécialisées dans la détection des cybermenaces et la création d'un hub d'innovation, illustre l'approche proactive de certaines Banques Centrales. L'idée centrale reste que l'IA ne doit pas seulement être régulée, mais aussi stimulée, notamment en favorisant les initiatives locales, la mutualisation des bonnes pratiques et l'anticipation des risques nouveaux dans des écosystèmes financiers de plus en plus intégrés.

b) Défis des technologies financières innovantes face aux risques croissants de cybercriminalité et aux stratégies d'inclusion financière

Le deuxième sous-thème, présenté par M. TAZI a porté sur les défis posés par les technologies financières innovantes face aux risques croissants de cybercriminalité, dans un contexte où l'inclusion financière progresse rapidement sur le continent africain. Il a souligné que les FinTechs africaines jouent un rôle déterminant en matière de souveraineté économique et d'intégration des populations non bancarisées. L'exemple de la collaboration entre Bank Al-Maghrib et les startups locales illustre ce potentiel : l'agilité des FinTechs combinée à la légitimité des institutions bancaires a permis une nette amélioration du taux de bancarisation. Cette dynamique est renforcée par le développement du mobile money qui représente désormais plus de la moitié des comptes mobiles dans le monde, avec un ancrage fort en Afrique.

Dans ce contexte d'expansion digitale, la cybersécurité devient un enjeu stratégique majeur. M. TAZI a attiré l'attention sur l'augmentation rapide du nombre de cyberattaques sur le continent, avec une hausse de 23% des attaques hebdomadaires en Afrique depuis 2023. Il a notamment précisé que 80% des banques africaines ont subi au moins une cyberattaque, avec un coût moyen estimé à 2,5 millions de dollars. Les cybermenaces sont de plus en plus sophistiquées, allant des ransomwares aux faux virements, en passant par le phishing et les deepfakes. L'utilisation croissante de l'Intelligence Artificielle par les cybercriminels accentue la vulnérabilité des systèmes existants, notamment dans un environnement marqué par la digitalisation des services, l'adoption du cloud et l'interconnexion avec des prestataires externes.

Face à cette menace, le Présentateur a mis en exergue les grands axes d'un dispositif global de cyber résilience adapté aux réalités africaines. Parmi les mesures clés figurent l'adoption d'une architecture Zero Trust, l'intégration de la sécurité dès la conception (security-by-design), le renforcement de la sécurité chez les partenaires et prestataires, le déploiement de centres opérationnels de sécurité (SOC) et la formation continue du personnel à la cybersécurité. Il a également cité l'exemple du Maroc, où la loi n° 05-20 sur la cybersécurité, promulguée en 2020, constitue un modèle de cadre juridique moderne, notamment pour les secteurs critiques comme les banques, les télécoms et les assurances.

Enfin, M. TAZI a conclu en appelant à une gouvernance continentale renforcée dans le domaine de la cybersécurité. À travers l'« Appel de Casablanca », il a plaidé pour une coordination entre les Banques Centrales africaines, estimant que seule une réponse collective permettra de faire face aux menaces systémiques. Il a illustré ce point par une métaphore évocatrice : « La fourmi qui voyage seule arrive vite, mais la colonie traverse le désert ». Cette image souligne l'importance de la solidarité, de la mutualisation des ressources et du partage des bonnes pratiques pour bâtir un écosystème financier africain sécurisé, résilient et inclusif.

Les discussions ont mis en lumière l'essor rapide de la transformation numérique et de l'innovation financière en Afrique, avec un accent particulier sur le développement des technologies FinTechs. Les interventions ont souligné les progrès significatifs réalisés dans le domaine des paiements numériques, de l'inclusion financière ainsi que la mise en place de

cadres réglementaires favorables. Plusieurs initiatives structurantes, comme les sandboxes réglementaires, les fast-tracks pour l'agrément FinTech ou encore les dispositifs d'accompagnement illustrent la volonté des autorités monétaires africaines de stimuler un écosystème dynamique. Des acteurs régionaux majeurs comme HighTech Payment Systems (HPS) ont été cités comme piliers de cette dynamique.

Par ailleurs, les participants ont largement insisté sur l'importance cruciale de la cybersécurité face à l'amplification des risques liés à l'expansion numérique. Les Banques Centrales africaines ont été appelées à renforcer la résilience des systèmes financiers face aux cybermenaces, à travers des cadres réglementaires harmonisés, la protection des données personnelles, la signature électronique ainsi que l'adoption des meilleures pratiques internationales. L'appel a été lancé pour une mutualisation des efforts, à travers la mise en place des Computer Emergency Response Teams (CERTs) aux niveaux nationaux et régionaux, le partage d'informations sur les cyberattaques et la création d'une gouvernance continentale renforcée. Trois recommandations clés ont été formulées, notamment le partage d'information, l'harmonisation des textes réglementaires et le renforcement des capacités en cybersécurité.

Enfin, l'importance d'une gouvernance efficace et proactive a été mise en avant, tant au niveau des Banques Centrales que des établissements financiers opérant sur plusieurs continents. Cette gouvernance doit intégrer les enjeux de cybersécurité au plus haut niveau, garantir la conformité réglementaire et assurer une gestion rigoureuse des risques liés aux prestataires externes. Le rôle stratégique de la souveraineté numérique et de l'hébergement des données a également été évoqué, notamment face à l'absence de Big Techs africaines. Les discussions se sont conclues sur un appel fort à la coopération continentale, à la solidarité institutionnelle et à l'intégration des technologies dans une approche sécurisée, inclusive et durable du système financier africain.

c) Transactions numériques transfrontalières, cybersécurité et mesures pour lutter contre le blanchiment de capitaux et le financement du terrorisme

Dans son intervention, Mme Najwa BENMADANI a proposé une analyse approfondie des enjeux liés à la criminalité financière à l'ère de la digitalisation. À l'entame de ses propos, elle a rappelé les principes directeurs du Groupe d'Action Financière (GAFI), organisme intergouvernemental chargé d'élaborer les normes internationales de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT). Elle a notamment mis en lumière les 40 recommandations du GAFI qui constituent le socle normatif international, ainsi que les missions d'évaluation mutuelle des dispositifs nationaux. Elle a également présenté le rôle du Groupe d'Action Financière du Moyen-Orient et de l'Afrique du Nord (GAFIMOAN), dont le Maroc est membre fondateur et a récemment assuré la présidence.

Mme BENMADANI a ensuite abordé les risques spécifiques associés à la montée des transactions numériques transfrontalières. Si ces dernières permettent une accélération significative des transferts de fonds et favorisent le dynamisme du commerce international, elles introduisent également de nouvelles vulnérabilités que sont l'anonymat, l'opacité, la rapidité d'exécution et la multiplicité des intermédiaires. Ces caractéristiques techniques sont

parfois exploitées par des réseaux criminels et des organisations terroristes à des fins de blanchiment de capitaux ou de financement illicite. C'est dans ce contexte que les recommandations n°15 et 16 du GAFI prennent tout leur sens, imposant des exigences précises aux pays et aux institutions à travers la surveillance des actifs virtuels (cryptomonnaies), la traçabilité des flux, l'obligation d'identification des parties aux transactions et la mise en œuvre de la règle de voyage GAFI, qui impose la transmission d'informations sur les expéditeurs et bénéficiaires lors de tout transfert dépassant un certain seuil.

La deuxième partie de la présentation a été consacrée à l'ANRF, la Cellule de Renseignement Financier du Royaume du Maroc, créée par la loi 43-05 qui a été promulguée en 2007 et instituée en 2009. Cette autorité administrative indépendante est rattachée au Chef du Gouvernement et joue le rôle de coordonnateur national de la lutte contre le blanchiment de capitaux et le financement du terrorisme. Son organisation repose sur plusieurs pôles spécialisés (affaires juridiques et conformité, investigations et renseignement financier, coopération internationale et coordination nationale, affaires administratives et financières, ainsi que le système d'information et de communication), et son conseil regroupe les principales institutions publiques concernées (ministères, régulateurs, autorités judiciaires, Bank Al-Maghrib, Office des Changes, etc.). L'ANRF constitue le nœud central du dispositif national, tant pour le volet préventif (sensibilisation et coordination interinstitutionnelle) que pour le volet répressif (analyse, transmission aux autorités judiciaires et coopération internationale).

Sur le plan opérationnel, Mme BENMADANI a détaillé les techniques utilisées par l'ANRF pour détecter les circuits de blanchiment. Celles-ci reposent sur une analyse financière tactique fondée sur la détection d'opérations atypiques par rapport aux profils économiques des clients, notamment des mouvements incohérents, le fractionnement des dépôts, l'usage de prête-noms, etc. Ces analyses sont renforcées par une analyse stratégique, orientée sur l'identification de schémas structurés ou de typologies récurrentes, comme le smurfing (fractionnement volontaire de transactions pour échapper au seuil de déclaration), ou encore le blanchiment fondé sur les échanges commerciaux (TBML), souvent observé dans les flux import-export. L'ANRF utilise à cette fin des outils performants tels que goAML, système d'information intégré de traitement et de messagerie sécurisé, développé par l'Office des Nations Unies contre la Drogue et le Crime (ONUDC).

Mme BENMADANI a également insisté sur l'importance des sources d'information. En plus des déclarations de soupçon émanant des entités assujetties, l'ANRF exploite les communications d'organismes publics, les données issues d'autorités étrangères (via 24 accords de coopération bilatérale/MOU), les échanges d'informations facilités par le Groupe Egmont, qui regroupe 177 Cellules de Renseignement Financier (CRF) à travers le monde, ainsi que les sources ouvertes (OSINT), notamment les bases de données accessibles au public, les réseaux sociaux et les informations commerciales.

La présentation s'est conclue par deux cas pratiques, illustrant les capacités de l'ANRF à intervenir efficacement. Le premier cas portait sur la détection d'une tentative de financement

du terrorisme par les actifs virtuels, et qui a été l'occasion de coordonner le travail entre l'ensemble des acteurs nationaux concernés par la LBC/FT au Maroc. Le second concernait un montage de blanchiment de capitaux via des transactions transfrontalières. Ces cas ont permis de mettre en lumière le rôle crucial du croisement d'informations, de la reconstitution de schémas transactionnels et de la traçabilité des fonds pour étayer des poursuites judiciaires. Mme BENMADANI a conclu en appelant à une coopération renforcée entre les institutions financières, les autorités publiques et les partenaires internationaux, afin de répondre efficacement aux menaces en constante évolution posées par les flux numériques.

Les discussions ont mis en évidence les défis majeurs auxquels les Banques Centrales africaines sont confrontées face à l'accélération de la digitalisation des services financiers, en particulier des transactions transfrontalières. Cette évolution soulève des enjeux critiques de conformité technique et d'efficacité en matière de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme. L'exemple du Zimbabwe a illustré les efforts en cours pour structurer un cadre institutionnel clair, à travers la collaboration entre la Banque Centrale, les unités de renseignement financier et les régulateurs des systèmes de paiement. La mise en œuvre de règles telles que la "Travel Rule", l'amélioration des systèmes de collecte et de traitement de données et les évaluations de risques constituent des étapes essentielles vers une meilleure maîtrise des menaces financières liées aux cryptomonnaies et aux nouveaux instruments numériques.

Par ailleurs, les échanges ont insisté sur la nécessité d'une coordination régionale et d'une harmonisation des cadres réglementaires, en particulier au sein des Communautés Économiques Régionales (CER) comme la Communauté de Développement d'Afrique Australe (SADC) où des écarts réglementaires entre pays (l'Afrique du Sud et ses voisins) créent des failles exploitables par les criminels, traduisant l'importance de mettre en place des mécanismes de coopération, de partage d'expériences et d'assistance technique mutuelle. L'initiative du Maroc, qui accueille régulièrement des délégations africaines pour partager son expérience en matière de conformité LBC/FT, a été saluée comme une bonne pratique à pérenniser et à structurer davantage via un répertoire humain des compétences disponibles sur le continent.

Enfin, les discussions ont souligné que la lutte contre la cybercriminalité et la protection des données personnelles sont des piliers incontournables de la résilience du secteur financier. Les régulateurs sont appelés à renforcer la sécurité des applications mobiles, à assurer la conformité des opérateurs FinTech et à mieux sensibiliser les consommateurs aux risques numériques. Le recours à des sandboxes réglementaires a été évoqué comme levier de promotion d'une innovation responsable. Une proposition a été faite pour créer un mécanisme continental de coordination des sandboxes et des unités de renseignement financier à l'effet de renforcer les réponses communes face aux menaces numériques et financières transnationales.

3.2. Session plénière 2 : Expériences des Banques Centrales de l'ABCA

Quatre Banques Centrales de l'ABCA ont partagé leurs expériences concernant le thème principal du Séminaire.

3.2.1. Central Bank of Egypt (CBE)

Avec un âge médian d'environ 24 ans, l'Égypte possède une démographie jeune et encline au numérique, prête à l'adoption rapide des technologies. Associé aux efforts nationaux visant à renforcer l'inclusion financière, en particulier pour les personnes non bancarisées et mal desservies, cet élan axé sur la jeunesse alimente une transformation du système financier égyptien.

Le Conseil National des Paiements[1], créé en 2017, a introduit le « Less-Cash Transformation Framework » pour mener la transition de l'Égypte vers une économie numérique. La FinTech et l'Innovation et la Cybersécurité sont toutes deux d'importants catalyseurs de ce cadre. La technologie financière joue également un rôle clé dans le Cadre d'Inclusion Financière lancé en 2022.

En 2019, la Central Bank of Egypt (CBE) a lancé sa stratégie FinTech et Innovation, s'alignant sur la Vision 2030 de l'Égypte et les besoins et aspirations évolutifs du marché. L'Égypte vise à se positionner comme un pôle FinTech de premier plan dans la région arabe et en Afrique, favorisant l'innovation, les talents et les services financiers de nouvelle génération.

Les initiatives de la CBE sont soutenues par un cadre juridique solide qui rend obligatoires les paiements numériques pour les transactions gouvernementales et établit la base législative de la transformation numérique dans les secteurs financier et bancaire, et promeut l'utilisation des technologies modernes dans tous les domaines fournissant des services financiers, bancaires ou réglementaires.

Pour renforcer la coordination réglementaire, le Comité FinTech et Innovation a été créé en juillet 2019, réunissant tous les régulateurs pertinents pour assurer une surveillance et un soutien efficaces à l'industrie FinTech en pleine croissance.

Le Sandbox réglementaire, lancé en juillet 2019, offre un environnement contrôlé où les startups et les innovateurs FinTech peuvent tester des solutions en temps réel sous la supervision de la Banque Centrale, mais sans exposer le système financier au risque.

L'une des innovations clés, actuellement à l'étude, est le prêt numérique via le scoring comportemental, qui exploite les données d'utilisation mobile et de paiements de services publics pour permettre les nano-prêts. Cette approche vise à faire progresser l'inclusion financière, en particulier pour la population égyptienne non bancarisée.

La Central Bank of Egypt a élaboré des objectifs stratégiques et opérationnels complets en matière de cybersécurité, visant à relever les défis de la cybersécurité de manière fiable et cohérente. Ces objectifs soutiennent l'exécution des politiques et initiatives organisationnelles dans le cadre d'un plan stratégique intégré. Ils contribuent également au renforcement des compétences nationales capables d'atténuer et de répondre efficacement aux cybermenaces tout en tirant parti de leur centre de veille sur les menaces.

Le Département Central de Surveillance de la Préparation à la Cybersécurité, au sein du Secteur de la Cybersécurité de la CBE, a dirigé les efforts visant à unifier les contrôles de

[1] National Payments Council (NPC)

cybersécurité dans l'ensemble du secteur financier et bancaire égyptien. Les réalisations clés comprennent :

- Élaboration du premier cadre réglementaire sectoriel de cybersécurité : EG-FinCSF ;
- Intégration des meilleures pratiques et normes internationales dans les réglementations et circulaires de la CBE ;
- Soutien aux institutions financières pour l'alignement des initiatives de cybersécurité avec les objectifs commerciaux et les innovations technologiques émergentes ;
- Établissement d'un mécanisme d'évaluation comparative indépendante de la préparation à la cybersécurité pour toutes les entités agréées sous la supervision de la CBE.

Le Secteur Cybersécurité de la CBE a lancé le Programme de Vigilance et de Surveillance des Risques, permettant à la fois des auto-évaluations et des évaluations indépendantes de la conformité des institutions en matière de cybersécurité. Ce programme se concentre sur :

- Le suivi de la maturité, des risques, des capacités, de la résilience et de la préparation des banques, des institutions financières et des entreprises FinTech ;
- La validation de la conformité avec l'EG-FinCSF ;
- L'amélioration des stratégies de cybersécurité par l'identification préventive des risques ;
- La promotion de l'amélioration continue et des pratiques de conformité durables dans l'ensemble du secteur.

La Central Bank of Egypt a créé l'EG-FinCIRT (Équipe d'Intervention en Cas d'Incidents Informatiques du Secteur Financier Égyptien), responsable de la gestion des incidents et de la réponse d'urgence pour les banques et les entités FinTech. Les fonctions clés comprennent :

- Déploiement de technologies avancées de surveillance de la sécurité et de détection non conventionnelles ;
- Analyse des preuves numériques et identification des vulnérabilités de cybersécurité ;
- Exécution d'analyses de logiciels malveillants et de procédures de rétro-ingénierie pour renforcer la cyber-résilience à l'échelle du secteur ;
- Amélioration des compétences techniques du personnel du secteur financier par des initiatives de sensibilisation professionnelle et des programmes spécialisés de formation et de sensibilisation, dispensés par des experts qualifiés en collaboration avec des entités internationales spécialisées dans la cybersécurité.

Ce modèle sert de référence pour les autres Banques Centrales qui cherchent à favoriser l'innovation tout en abordant de manière proactive les risques cybernétiques en rapide évolution.

3.2.2. Central Bank of Kenya (CBK)

La Central Bank of Kenya joue un rôle de premier plan dans la transformation du secteur financier du pays, marquée par une forte digitalisation et une adoption accélérée des technologies financières. Cette présentation met en lumière l’évolution du paysage bancaire kényan, l’essor des innovations FinTech et les risques croissants liés à la cybersécurité.

Le système bancaire formel du Kenya repose sur un ensemble d'institutions financières supervisées, notamment les banques commerciales, les institutions de microfinance et les prestataires de services de paiement. Le Kenya s'est imposé comme un des leaders continentaux de l'innovation FinTech. La révolution des services financiers numériques repose sur des avancées majeures en matière de mobile money, de crédit digital et de paiements instantanés. Des plateformes emblématiques telles que M-Pesa ont non seulement amélioré l'expérience client, mais également favorisé l'inclusion financière, en touchant des segments de population jusque-là exclus du système bancaire. Ce développement est porté par un écosystème mixte associant entreprises technologiques, opérateurs télécoms et cadre réglementaire favorable à l'innovation.

Bien que les innovations FinTech apportent des gains en efficacité, en accessibilité et en rapidité, elles introduisent également de nouvelles vulnérabilités opérationnelles et sécuritaires. Le secteur est confronté à des défis tels que les cyberattaques, les atteintes à la protection des données et une dépendance croissante vis-à-vis de prestataires technologiques tiers, notamment les plateformes cloud. Ces risques exigent des stratégies de gestion adaptées et une amélioration continue des dispositifs de cybersécurité. Parmi les vecteurs d'attaque les plus fréquents figurent le phishing, les malwares, la fraude par le SIM swapping et les ransomwares. Ces menaces visent aussi bien les infrastructures des établissements que les clients finaux, soulignant la nécessité d'un dispositif de défense global et intégré.

Pour faire face à ces menaces, le Kenya a mis en place un cadre juridique et réglementaire proactif. La Loi sur la cybercriminalité et les abus informatiques adoptée en 2018 constitue la base législative pour la poursuite des infractions numériques. Parallèlement, la CBK a élaboré des règlements et des lignes directrices spécifiques pour le secteur financier, fixant des normes minimales de conformité et renforçant les capacités de détection et de réaction face aux incidents de sécurité. La CBK adopte une approche de supervision basée sur les risques, axée sur la résilience, la gestion proactive des menaces et le respect des obligations réglementaires. Elle réalise des évaluations régulières, impose la notification des incidents et entretient un dialogue constant avec les acteurs du secteur pour adapter ses pratiques aux nouvelles technologies. Ce modèle souple permet à la CBK de concilier innovation et sécurité.

Une enquête menée sur l'application des lignes directrices de la CBK de 2017 en matière de cybersécurité révèle une pratique inégale au niveau des structures financières. Des avancées notables ont été enregistrées dans la gouvernance et les contrôles internes, mais des lacunes persistent, notamment dans la gestion des incidents, la formation des employés et le suivi des risques liés aux prestataires tiers. Ces constats mettent en évidence le besoin de renforcer les capacités à tous les niveaux.

La CBK s'engage à renforcer durablement la cybersécurité du secteur financier kényan à travers un ensemble d'initiatives à court et long terme. Les priorités incluent l'actualisation du cadre réglementaire, la promotion de la coopération sectorielle, le développement de programmes de sensibilisation et de formation, ainsi que l'amélioration des outils de surveillance et de réponse aux menaces en temps réel. L'objectif est de garantir que l'innovation aille de pair avec la résilience, dans un environnement financier sûr et digne de confiance.

3.2.3 Banque Centrale du Congo (BCC)

La Banque Centrale du Congo a exposé son expérience institutionnelle en matière de gestion des cybermenaces dans un écosystème financier en pleine transformation numérique. Forte de son rôle de régulateur et de catalyseur, la BCC veille à préserver la stabilité du système financier national, composé de plus de 112 établissements de crédit dont 15 banques commerciales et 183 sociétés financières non bancaires dont quatre émetteurs de monnaie électronique et plusieurs agrégateurs FinTech. Cette vigilance est essentielle pour éviter tout dysfonctionnement systémique pouvant avoir des effets en cascade.

Pour la BCC, la transformation digitale, bien qu'elle favorise l'inclusion financière et la modernisation des paiements, expose également le secteur à des risques cyber accrus tels que les attaques ciblant les plateformes monétiques, les cartes prépayées, les services mobiles, le cloud, ou encore les solutions FinTech émergentes. Consciente du caractère interconnecté du secteur, la Banque privilégie une approche collective et collaborative, estimant qu'aucune institution ne peut, isolément, contenir efficacement ces menaces. La stratégie de réponse de la BCC repose donc sur la mobilisation de tous les acteurs, appuyée par un dispositif de supervision progressif articulé autour de la réglementation, de la surveillance des risques, de la coordination, du partage d'informations et du renforcement des capacités.

En tant qu'institution stratégique, la BCC s'applique les mêmes exigences imposées aux acteurs du secteur. Lors d'incidents cyber, elle adopte une posture proactive en faisant une intervention immédiate en soutien aux institutions affectées et un suivi personnalisé du traitement de l'incident. Elle procède également à une évaluation a posteriori. Ce processus crée un partage d'expériences sécurisé avec l'ensemble du secteur afin de diffuser les bonnes pratiques. Par ailleurs, la BCC élabore actuellement une stratégie nationale des systèmes de paiement 2025-2030 qui intègre un volet sur la cybersécurité.

3.2.4 South African Reserve Bank (SARB)

L'Afrique du Sud dispose d'un secteur bancaire et financier développé, avec des services de paiement numérique largement accessibles et un taux élevé d'inclusion financière. Dans le cadre de sa Vision 2025, des améliorations ont été apportées au système national de paiement, notamment le lancement d'un système de paiement rapide (PayShap) en mars 2023 et l'introduction des paiements sans contact et des codes QR. Cependant, malgré la numérisation croissante, les espèces restent dominantes (cash is king) et l'adoption des paiements digitaux reste limitée parmi les ménages à faible niveau de vie. Pour y remédier, la SARB a lancé sa feuille de route pour les paiements numériques (Project Stimela), visant à élargir l'accès au système national de paiement, à proposer des solutions innovantes à faible coût et à moderniser les infrastructures de paiement.

Le pays fait face à une augmentation des cas de fraude, comme le relève la Southern African Fraud Prevention Service (SAFPS), notamment en matière de détournement de comptes, de falsification de documents et d'usurpation d'identité. Cette dernière catégorie enregistre la plus forte progression. Pour renforcer la lutte contre ces risques, la SARB s'appuie sur plusieurs entités spécialisées, notamment l'Autorité prudentielle (régulation prudentielle, risques cyber

et LBC/FT), le Département des Systèmes de Paiement Nationaux (paiements domestiques), la Direction de la Surveillance Financière (contrôle des changes et paiements transfrontaliers), la Direction de la Stabilité Financière (gestion des risques systémiques, y compris cyber), la Division FinTech (innovation) et l'Unité Cybersécurité et Sécurité de l'Information (gestion des risques cyber).

L'Unité de Cybersécurité et de Sécurité de l'Information (CISU) de la SARB collabore avec le secteur financier sud-africain, régional (SADC) et international (Banque des Règlements Internationaux - BRI), pour renforcer la résilience face aux cybermenaces. Elle préside notamment un Sous-comité sur la cyber-résilience et travaille à la mise en place d'une équipe de réponse aux incidents (CSIRT) dédiée au secteur financier. Par ailleurs, les deux composantes du Programme de Modernisation des Écosystèmes de Paiement (PEM) de la SARB ont été mises en avant, à savoir la composante 4 (interopérabilité, lutte contre la fraude et harmonisation réglementaire) et la composante 1 (facilitateurs fondamentaux y compris l'identité financière numérique – DFID), la DFID étant développée en partenariat avec le gouvernement.

Enfin, la SARB s'engage activement dans l'innovation FinTech, notamment via son partenariat avec le BIS Innovation Hub, et, sous la Présidence du G20, elle a initié le TechSprint 2025 centré sur l'identité numérique, la portabilité des données de crédit et la lutte contre la fraude. Elle est également membre fondateur du Groupe de Travail Intergouvernemental sur les FinTechs (IFWG), qui vise à garantir une transparence réglementaire des diverses innovations du secteur financier à travers son sandbox réglementaire.

À l'issue des partages d'expériences, les discussions ont porté sur la manière dont les Banques Centrales africaines, notamment celles d'Égypte, du Kenya, du Congo et d'Afrique du Sud, adaptent leurs politiques et infrastructures pour encadrer l'innovation financière tout en assurant la protection des consommateurs. Des outils tels que les sandboxes réglementaires, la notation comportementale (behavioral scoring), les initiatives d'intégration avec les parties prenantes (FinTechs, institutions de microfinance et opérateurs mobiles), ainsi que la réglementation sur la protection des données, ont été mis en exergue pour encadrer les nouveaux acteurs du système financier. Le cas égyptien a été particulièrement illustratif avec un cadre réglementaire évolutif et des mécanismes de concertation avec les parties prenantes pour améliorer la conformité des FinTechs à chaque cohorte.

Les intervenants ont soulevé la problématique des menaces croissantes, complexes et transfrontalières qui nécessitent des réponses concertées. Des exemples ont été donnés sur la mise en œuvre de centres de surveillance 24/7, de simulations régulières d'incidents (cyber drills), de politiques de sécurité dès la conception (security by design), ainsi que sur la nécessité d'avoir des contrôles intégrés à tous les niveaux des systèmes d'information. La formation continue et la sensibilisation du public, y compris dans les zones rurales, sont également apparues comme essentielles pour renforcer la résilience.

Un point saillant a concerné la coopération entre institutions financières nationales et internationales et les Autorités de régulation. Les Banques Centrales reconnaissent l'importance d'une coordination efficace, à la fois entre les unités internes (cybersécurité, réglementation et supervision) et avec d'autres agences nationales (protection des données, télécommunications et justice) mais aussi avec les partenaires internationaux (par exemple,

BRI, G20 et autres Banques Centrales). Les Protocoles d'Accord (PA) ont été mentionnés comme outils indispensables pour institutionnaliser cette collaboration. L'exemple du Congo avec la mise en place d'un FinCERT national illustre l'engagement pour un dispositif national coordonné.

Enfin, les intervenants ont souligné la nécessité de développer des cadres réglementaires flexibles, proportionnés aux risques et capables de s'adapter rapidement à l'évolution des technologies. Les politiques doivent être inscrites dans une stratégie nationale claire, inclusive et évolutive. Une attention particulière a été portée aux institutions non réglementées ou opérant dans l'informel, souvent à l'origine de pratiques abusives. Dans ce contexte, la transparence, la responsabilisation des acteurs et l'éducation financière sont des priorités pour garantir un développement sain et sécurisé de l'inclusion financière à travers l'Afrique. L'enjeu pour les Banques Centrales serait de concilier souveraineté numérique, interopérabilité régionale et inclusion effective, tout en maintenant la confiance et la stabilité dans leurs systèmes financiers. La mise en réseau des expertises et des pratiques pourrait nourrir une véritable collaboration continentale et internationale en matière de cybersécurité financière.

4. SESSIONS DE GROUPE

Groupe I : « Adoption des Monnaies Numériques de Banque Centrale (MNBC) en Afrique : défis et opportunités »

I. Contexte

L'adoption des Monnaies Numériques de Banque Centrale (MNBC) prend de l'ampleur en Afrique, les pays explorant des solutions innovantes pour renforcer l'inclusion financière, améliorer les systèmes de paiement et consolider la souveraineté monétaire. Poussées par la transformation numérique rapide des économies et la demande croissante de services financiers sécurisés, rentables et accessibles, plusieurs Banques Centrales africaines mènent activement des recherches et des projets pilotes sur les MNBC. Cependant, le processus de mise en œuvre est complexe et présente un ensemble unique de défis, notamment les contraintes d'infrastructure, les risques de cybersécurité, les incertitudes réglementaires et la confiance du public. Dans le même temps, les MNBC offrent des opportunités significatives pour combler les lacunes financières, moderniser les outils de politique monétaire et favoriser une plus grande résilience économique.

À l'heure actuelle, les statistiques ci-dessous mettent en évidence le déploiement des MNBC à différents stades :

- 134 pays (couvrant plus de 98% du PIB mondial) explorent les MNBC ;
- 39 pays sont à un stade avancé (pilote et lancement) ;
- 11 pays ont entièrement lancé une MNBC ;
- 53 pays sont en phase de développement ou en phase pilote ;
- Seuls deux pays ont abandonné leur projet de MNBC après l'avoir piloté.

Statistiques de déploiement des MNBC spécifiques à l'Afrique (en 2025)

Pays	Statut	Type de MNBC	Domaine d'intérêt clé
Nigéria	Lancé	Détail	Inclusion financière et coût des espèces.
Ghana	En pilote	Hybride	Utilisation hors ligne, intégration de l'argent mobile.
Afrique du Sud	Pilote (gros)	Gros	Règlement interbancaire (Projet Khokha).
Namibie	Étude de faisabilité	À déterminer	Efficacité des paiements.
Rwanda	Recherche	À déterminer	Conception de la MNBC et analyse d'impact.
Kenya	Suivi du développement	À déterminer	Suivi du développement – suite à la publication du document de discussion sur les MNBC et le rapport des commentaires du public relatifs au document de discussion.
UEMOA (BCEAO)	Recherche	À déterminer	Exploration d'une MNBC régionale.
Région SADC	Exploratoire	Mixte	Potentiel de projet pilote transfrontalier.

Points saillants de l'enquête de la Banque des Règlements Internationaux (BRI) (Focus sur l'Afrique en 2024/2025)

- 80% des Banques Centrales africaines étudient activement ou planifient des MNBC ;
- 63% citent l'interopérabilité avec la monnaie mobile comme un objectif de conception clé ;
- Plus de 70% ont exprimé des inquiétudes quant aux impacts potentiels sur l'intermédiation des banques commerciales ;
- Moins de 40% disposent aujourd'hui d'un cadre juridique adéquat pour émettre une MNBC.

L'ARCHITECTURE

Lors de la conception et de la mise en œuvre des MNBC, un ensemble de décisions clés doivent être évaluées à différentes étapes concernant la technologie et l'accès, la confidentialité et le modèle de distribution. Les MNBC nécessitent également la création d'une infrastructure de paiement couvrant tout, de la base de données sur laquelle les MNBC sont enregistrées aux applications et aux dispositifs de point de vente utilisés pour initier les paiements. Les considérations clés pour la construction de la solution MNBC ainsi que de la plateforme ont été évaluées en détail. Les Banques Centrales ont le choix de décider si elles doivent adopter une approche basée sur le jeton ou sur le compte.

Approche basée sur le jeton : dans le cas d'une MNBC basée sur le jeton, la distribution de la devise impliquera le transfert d'un objet de valeur d'un portefeuille à un autre. Les MNBC basées sur le jeton garantissent que la transaction est approuvée par des paires de clés publiques-privées et des signatures numériques basées sur l'émetteur et le bénéficiaire. Ainsi, le système offre un niveau élevé de confidentialité, mais ajoute plus de difficultés à tracer le blanchiment d'argent et les transactions frauduleuses. De plus, les clients doivent se souvenir de leurs clés d'accès, sinon ils perdraient l'accès aux fonds.

Approche basée sur le compte : dans une MNBC basée sur le compte, la distribution de la devise impliquera un transfert d'un compte à un autre. Le modèle assurerait la garantie que la transaction est approuvée par l'émetteur et le bénéficiaire sur la base de la vérification de l'identité de l'utilisateur. En émettant de tels comptes, les Banques Centrales devraient s'assurer de l'existence d'un compte numérique pour chaque utilisateur.

En comparant les avantages et les inconvénients de chacune des deux technologies d'accès, l'approche basée sur le jeton a généralement été préférée par les régulateurs pour les transactions transfrontalières où les deux entités n'ont besoin que de portefeuilles pour faciliter les transactions. L'approche basée sur le jeton facilite également les objectifs d'inclusion financière car seule une connexion Internet est requise pour que les deux utilisateurs puissent effectuer le paiement. De plus, l'approche basée sur le jeton offre un degré élevé d'anonymat aux utilisateurs. D'un autre côté, une approche basée sur le compte permet aux régulateurs de surveiller les transactions de plus près et d'avoir un degré d'implication relativement plus élevé dans le processus de paiement de bout en bout.

L'approche directe comparée à l'approche indirecte :

	Mécanisme	**Contrôle**	**Exemples**
MNBC Directe	La Banque Centrale agit en tant que fournisseur direct de la monnaie numérique au public, potentiellement via un portefeuille numérique ou un autre système de paiement.	La Banque Centrale maintient un degré élevé de contrôle sur la MNBC, y compris son émission, sa distribution et sa gestion.	Cela pourrait impliquer que la Banque Centrale crée des comptes directement pour les citoyens ou utilise un système basé sur des jetons où les individus détiennent la monnaie numérique dans un portefeuille.
MNBC Indirecte	La Banque Centrale émet la MNBC aux banques commerciales ou à d'autres institutions financières, qui gèrent ensuite la distribution et l'accès pour leurs clients.	Le contrôle de la Banque Centrale est moins direct, car elle s'appuie sur les institutions intermédiaires pour gérer les aspects de la MNBC en contact avec le public.	Cela pourrait impliquer que la Banque Centrale fournisse de la monnaie numérique aux banques commerciales, qui l'offrent ensuite à leurs clients via leur infrastructure bancaire existante.

Cette session met en exergue le paysage évolutif de l'adoption des MNBC en Afrique, en soulignant les principales opportunités et les défis qui façonnent cet avenir monétaire numérique avec les pays ayant des objectifs différents.

II. Opportunités :

- Sécurité, les MNBC offrent une garantie, car elles sont adossées à l'autorité monétaire ;
- Facilité d'accès / Inclusion financière – les MNBC peuvent servir de vecteur d'accès aux services financiers pour les populations exclues du système bancaire traditionnel, notamment dans les pays en développement ou les zones reculées dépourvues d'infrastructures bancaires adéquates ;
- Traitement rapide des paiements – elles permettent potentiellement de réduire les délais et les coûts des transactions par rapport aux systèmes existants, y compris pour les paiements transfrontaliers ;
- Réduction de la dépendance aux intermédiaires – ce qui peut entraîner une baisse des frais de transaction et une accélération des paiements ;
- Interopérabilité – possibilité d'interagir avec d'autres plateformes de paiement et de bénéficier de la rapidité des moyens de paiement alternatifs ;
- Innovation technologique – notamment via la programmabilité et l'intégration avec d'autres plateformes numériques requérant des paiements digitaux ;
- Réduction des risques – les MNBC, en tant que créance directe sur la Banque Centrale, peuvent atténuer certains risques, en particulier le risque de contrepartie, en représentant le moyen de paiement le plus sûr ;
- Réduction des coûts pour les Banques Centrales – en diminuant les dépenses liées à l'émission de billets, l'adoption des MNBC pourrait réduire la circulation fiduciaire et les coûts afférents ;
- Flexibilité pour les usagers – les utilisateurs pourraient facilement basculer entre les MNBC et d'autres formes de finance comme la monnaie fiduciaire ou les plateformes numériques.

III. Défis :

- Infrastructures numériques limitées : dans plusieurs pays africains, les lacunes en matière d'infrastructure numérique freinent l'adoption des MNBC. Dans les zones rurales, l'accès à Internet est instable et l'approvisionnement en électricité irrégulier. Le coût élevé des smartphones et des équipements compatibles limite également l'accessibilité, surtout pour les populations à faibles revenus ;
- Faible culture financière et numérique : le faible niveau de littératie financière et numérique constitue un obstacle majeur à la compréhension et à l'utilisation des

MNBC. Une méfiance généralisée, nourrie par des antécédents de fraude ou d'instabilité des systèmes, peut aggraver cette situation ;

- Risques liés à la cybersécurité et à la fraude : les MNBC sont exposées aux menaces cybernétiques (piratage, hameçonnage et fraude). De nombreux pays africains manquent d'infrastructures et de compétences spécialisées nécessaires pour sécuriser les plateformes numériques, exposant ainsi les utilisateurs, notamment les moins technophiles, à des pertes financières ;

- Capacité des Banques Centrales et gouvernance : le déploiement réussi d'une MNBC requiert une expertise technique et institutionnelle que certaines Banques Centrales africaines peuvent ne pas maîtriser pleinement. La conformité réglementaire avec les lois existantes (bancaires, monétiques et mobile money) complexifie davantage l'implémentation ;

- Risque de désintermédiation bancaire : une adoption directe de MNBC par les usagers pourrait entraîner une diminution des dépôts dans les banques commerciales, affectant leur capacité de prêt et leur liquidité, et perturbant leur rôle traditionnel. La transmission de la politique monétaire pourrait également être impactée ;

- Interopérabilité avec les systèmes existants : dans de nombreux pays africains, les services de mobile money (comme M-Pesa au Kenya) sont déjà bien implantés. Assurer une intégration harmonieuse des MNBC dans ces écosystèmes nécessite des efforts techniques et institutionnels considérables ;

- Préoccupations liées à la vie privée et à la surveillance : sans lois solides sur la protection des données, les citoyens pourraient craindre une surveillance étatique de leurs transactions, ce qui compromettrait la confiance dans les MNBC ;

- Coûts d'implémentation élevés : la conception et la maintenance d'une infrastructure MNBC sécurisée et évolutive nécessitent des investissements importants, alors que certains pays font face à un manque de ressources qu'ils ne peuvent assumer sans recours à des partenaires extérieurs ou à des bailleurs internationaux ;

- Complexité des paiements transfrontaliers : les MNBC peuvent faciliter le commerce intrarégional, mais cela requiert des cadres harmonisés, l'interopérabilité entre systèmes nationaux et une coopération renforcée entre Banques Centrales. L'état actuel de coordination régionale reste insuffisant ;

- Problèmes de convertibilité des devises : l'absence de convertibilité libre de certaines monnaies africaines peut compliquer l'usage des MNBC à l'international. Sans mécanismes de change adéquats, leur portée transfrontalière reste limitée ;

- Identification et vérification (KYC) : des protocoles KYC solides sont essentiels pour prévenir les usages illicites. Or, une grande partie de la population ne dispose pas de pièces d'identité formelles, ce qui pourrait exclure les populations vulnérables, notamment dans les zones rurales ;

- Stabilité du système financier : une migration massive des dépôts vers les MNBC pourrait affaiblir la capacité de crédit des banques, accroître les risques de liquidité et perturber l'intermédiation financière traditionnelle ;
- Coordination et mobilisation du public : le succès des MNBC dépend d'une coordination efficace entre les autorités publiques, les régulateurs, les institutions financières, les opérateurs télécoms et les usagers. Un déficit de concertation ou de communication claire peut entraîner une mauvaise conception et une adoption limitée.

IV. Recommandations

Pour réussir l'adoption des MNBC en Afrique, des stratégies multidimensionnelles ont été proposées :

1. Renforcement des infrastructures numériques et financières : les États doivent investir dans l'extension de la connectivité internet, l'amélioration de la fiabilité électrique et l'accès à des équipements numériques abordables, en particulier dans les zones rurales. Ces actions doivent s'appuyer sur des partenariats public-privé ciblés ;
2. Promotion de la littératie financière et numérique : des campagnes de sensibilisation doivent être menées pour expliquer le fonctionnement des MNBC, leurs avantages et leur complémentarité vis-à-vis d'autres instruments de paiement numériques. Un effort particulier doit être porté vers les groupes marginalisés tels que les femmes, les personnes âgées et les personnes défavorisées, ainsi que la lutte contre la méfiance liée à la surveillance et à la fraude. Le développement des MNBC devrait s'accompagner d'une campagne de sensibilisation du public afin d'éviter les malentendus et la faible utilisation par le public ;
3. Mise en place de cadres juridiques et réglementaires solides : les MNBC doivent bénéficier d'un statut clair de monnaie légale, être conformes aux réglementations LBC/FT, intégrer des mesures strictes de protection des données et prévoir l'interopérabilité transfrontalière. Une cohérence réglementaire entre les Banques Centrales, les institutions financières et les régulateurs des télécoms est cruciale pour une gestion efficace. Afin d'assurer la coexistence des MNBC avec les systèmes financiers existants, il est nécessaire de veiller à ce que toutes les parties prenantes concernées fassent partie du processus d'élaboration de la politique ;
4. Cybersécurité et supervision des risques : les MNBC doivent être conçues avec des standards de sécurité élevés pour prévenir les cyberattaques, le vol d'identité et les défaillances système. Cela implique des investissements dans des infrastructures sécurisées, le renforcement des capacités IT des Banques Centrales et l'adoption de standards internationaux en matière de cybersécurité. Les cadres de supervision doivent évoluer pour intégrer les risques opérationnels, cybernétiques et systémiques, via des outils de surveillance en temps réel, d'analytique avancée et d'Intelligence Artificielle ;

   Les mécanismes de surveillance traditionnels peuvent ne pas tenir compte de la complexité, de la nature en temps réel et des risques technologiques associés aux

monnaies numériques. Par conséquent, les cadres de surveillance doivent être modernisés pour refléter les risques opérationnels, cybernétiques et systémiques introduits par les MNBC. Les Banques Centrales devraient adopter des outils de surveillance en temps réel, des analyses de données et des systèmes basés sur l'Intelligence Artificielle pour améliorer les capacités d'alerte précoce, la détection des fraudes et le suivi des anomalies dans les transactions de MNBC. Ces outils sont essentiels pour identifier les menaces émergentes, assurer la conformité avec les réglementations en matière de Lutte contre le Blanchiment des Capitaux et le Financement du Terrorisme (LBC/FT) et maintenir la confiance du public ;

5. Interopérabilité avec les systèmes financiers existants : l'intégration fluide avec les plateformes de mobile money, les systèmes bancaires et les réseaux de paiement régionaux est essentielle pour limiter les perturbations, encourager l'adoption et faciliter les transactions transfrontalières ;

6. Adoption progressive, inclusive et collaborative : il convient de démarrer par des projets pilotes ou des bacs à sable réglementaires, impliquant dès le départ les parties prenantes publiques et privées, tout en assurant une boucle de rétroaction continue. Cette démarche favorisera une adaptation aux contextes locaux et une meilleure appropriation par les usagers ;

7. Dans le contexte d'une union monétaire, il devrait y avoir une coordination claire entre tous les pays concernés à l'effet de de limiter les perturbations transfrontalières, y compris mais sans s'y limiter, les échanges commerciaux et la fuite des capitaux.

Groupe II : « Politiques et cadres réglementaires pour les solutions technologiques financières (FinTechs) émergentes »

I. Contexte

La croissance rapide des technologies financières (FinTechs) remodèle le système financier mondial, offrant à la fois des opportunités et des défis, en particulier pour les Marchés Émergents et les Économies en Développement (MEED). En Afrique, les innovations FinTech favorisent une plus grande inclusion financière, accélérant ainsi la digitalisation des paiements, du crédit, de l'assurance et permettant d'autres services. La pandémie de COVID-19 a considérablement catalysé cette transformation, poussant davantage d'utilisateurs et d'institutions vers des solutions financières numériques qui représentent la limite de l'infrastructure traditionnelle.

Toutefois, le rythme de l'innovation pose également des défis en matière de réglementation et de surveillance. Les acteurs FinTech, qu'il s'agisse d'émetteurs de monnaie électronique par le biais des télécommunications, d'agrégateurs de paiements, de prêteurs numériques, de technologies d'assurance ou de plateformes basées sur l'IA, se situent souvent en dehors des périmètres réglementaires traditionnels. Ainsi, de nombreuses juridictions se demandent comment classer correctement ces nouveaux acteurs, comprendre leur profil de risque et évaluer leur impact systémique.

Un cadre réglementaire et politique solide doit commencer par une compréhension claire de la notion de FinTech, y compris de ses acteurs, de ses risques et de ses insuffisances. Cela nécessite d'adapter la supervision grâce à des approches proportionnelles qui équilibrent l'innovation et l'atténuation des risques. L'essor des modèles financiers pilotés par l'IA complique encore la surveillance, ce qui nécessite des politiques flexibles et tournées vers l'avenir. Des outils réglementaires tels que les sandboxes sont apparus pour soutenir l'innovation, mais des questions subsistent quant à leur efficacité et à leur évolutivité.

Cette session a permis aux Banques Centrales de partager leurs expériences, d'examiner comment favoriser l'innovation tout en préservant la stabilité financière et de débattre de la question de savoir si le cadre réglementaire existant, conçu à l'origine pour des établissements physiques traditionnels, est adapté à l'ère de la finance numérique.

II. Problématiques clés

Les questions importantes qui ont été discutées sont les suivantes :

1. Définitions et champ d'application : les participants ont convenu que les définitions actuelles des FinTechs contenues dans le Conseil de stabilité financière[2] sont trop génériques. Bien que nous utilisions cette définition aux fins du présent rapport, il est nécessaire de l'améliorer pour l'adapter au contexte du pays. L'objectif devrait identifier la valeur ajoutée des FinTechs et d'adapter les réglementations en conséquence. Et la définition devrait prendre en compte à la fois les FinTechs et les solutions financières basées sur les FinTechs ;

2. Réglementation proportionnelle et approches fondées sur le risque : les régulateurs ont souligné l'importance de la proportionnalité dans la réglementation, en passant d'une approche sectorielle à une approche basée sur l'activité. Les technologies devraient être considérées comme des outils, la supervision étant axée sur la nature des activités financières (par exemple, l'émission de crédits), quel que soit le fournisseur. Cette distinction est essentielle pour garantir que les acteurs innovants soient réglementés de manière appropriée sans étouffer le développement ;

3. Protection des consommateurs et éducation financière : le débat a porté sur la vulnérabilité des consommateurs. Les participants ont souligné l'importance de l'éducation financière, mais surtout de la sensibilisation, de la divulgation claire et de la protection des consommateurs contre la fraude et les pratiques prédatrices.

4. Capacité de surveillance et collaboration : l'évolution rapide de l'espace FinTech exige des capacités de surveillance renforcées, en particulier en matière d'audit informatique et de cyber-risque ;

5. Protection des données et risques systémiques : des préoccupations croissantes ont été partagées au sujet de l'utilisation abusive des données et de son potentiel à perturber la continuité des activités, la stabilité financière et même l'ordre social ;

6. Outils d'innovation réglementaire : les pays adoptent divers outils tels que les sandboxes réglementaires pour tester et apprendre avant de procéder à la réglementation ;

[2] La FinTech englobe les nouveaux produits et services financiers numériques rendus possibles par les nouvelles technologies et stratégies.

7. Sensibilisation à l'infrastructure et à l'architecture : la compréhension de l'architecture technologique sous-jacente, à la fois fonctionnelle et non fonctionnelle, est considérée comme essentielle pour une surveillance efficace. Les régulateurs doivent comprendre comment les flux de données et les systèmes interagissent afin d'élaborer des politiques pertinentes ;

8. Nécessité d'une coordination intersectorielle : l'implication des télécommunications et d'autres acteurs non traditionnels (en particulier dans les paiements et les canaux numériques) soulève des questions en ce qui concerne le périmètre réglementaire. Il est nécessaire de clarifier les responsabilités et de renforcer la coopération entre les secteurs.

III. Recommandations

À la lumière des diverses discussions et expériences partagées par les Banques Centrales participantes et les acteurs du secteur financier, plusieurs recommandations clés ont été formulées pour guider l'élaboration de politiques et de réglementations efficaces.

1. Adopter des politiques et des réglementations fondées sur des principes : adapter les normes mondiales telles que celles de Bâle et les Principes pour les Infrastructures de Marchés Financiers aux contextes locaux plutôt que d'appliquer une approche unique ;

2. Envisager l'introduction de cadres financiers ouverts : veiller à ce que les lois existantes sur la protection des données soient prises en compte et que les régulateurs compétents soient consultés au cours du processus ;

3. Envisager d'élaborer des stratégies FinTech alignées sur celles nationales ou régionales et de mettre en place une fonction FinTech : il peut s'agir de réaliser des évaluations diagnostiques et de s'assurer qu'il existe un besoin et que celui-ci n'est pas couvert par d'autres stratégies ou fonctions respectivement ;

4. Simplifier l'octroi de licences et promouvoir le passporting : créer des processus d'autorisation rationalisés et étudier la possibilité d'une reconnaissance bilatérale ou régionale des autorisations ;

5. Pour les Banques Centrales qui n’en disposent pas sandboxes réglementaires, étudier la possibilité d'introduire des sandboxes réglementaires afin d'encourager les essais d'innovation dans des environnements contrôlés ;

6. Mettre à jour les cadres juridiques adaptés aux modèles émergents : les lois devraient être révisées pour reconnaître et réglementer la finance alternative (comme le crowdfunding et les prêts P2P) et les banques exclusivement digitales, en garantissant la clarté sur l'octroi de licences, la gouvernance et la protection des consommateurs tout en permettant l'innovation dans un cadre supervisé ;

7. Envisager la collaboration des régulateurs pour les produits FinTechs hybrides par le biais de lois ou de lignes directrices nouvelles ou révisées. Par exemple, travailler avec l'Autorité des Marchés Financiers pour le crowdfunding ;

8. Renforcer la protection des consommateurs : donner la priorité à la sensibilisation des consommateurs, à l'éducation financière, à des mécanismes de plainte efficaces et à une conception responsable des produits ;

9. Soutenir les écosystèmes d'innovation pour les petites FinTechs : investir dans des programmes d'incubation et d'accélération et créer des plateformes pour un dialogue continu sur l'innovation ;

10. Élargir l'engagement : collaborer avec les banques commerciales, les entreprises de télécommunication et d'autres acteurs pour assurer un développement inclusif et équilibré des FinTechs et une bonne compréhension des risques de la part des acteurs ;
11. Les régulateurs devraient à la fois adopter et superviser l'utilisation responsable de l'IA dans le secteur financier en déployant des outils d'apprentissage artificiel et automatique à des fins de surveillance - comme la détection de la fraude, du blanchiment d'argent et du financement du terrorisme (FT) - tout en établissant des orientations réglementaires pour régir la façon dont les entités agréées utilisent l'IA, y compris des normes d'explicabilité, de limitation des préjugés et de responsabilisation dans les algorithmes de prise de décision.
12. Les pays devraient adopter une stratégie nationale de souveraineté en matière d'utilisation de cloud pour assurer la gestion sécurisée des données du secteur financier, maintenir la surveillance réglementaire et la continuité des activités et réduire progressivement la dépendance à l'égard des fournisseurs de cloud étrangers ou tiers.

Groupe III : « Coopération transfrontalière en matière de renseignement et de réponse face aux cybermenaces »

I. Contexte

Avec le développement de la digitalisation en Afrique, le risque cyber devient une composante intégrée des activités économiques, constituant ainsi un élément permanent de l'univers des risques. La rapidité et l'ampleur avec lesquelles un incident peut survenir et s'aggraver diffèrent des autres risques opérationnels et commerciaux, nécessitant une bonne compréhension du paysage des menaces ainsi qu'une solide capacité de détection et de réponse aux menaces émergentes.

Les avancées technologiques peuvent engendrer de nouveaux risques tout en exacerbant les risques existants. L'utilisation de l'Intelligence Artificielle Générative (AGI) a accru la vitesse à laquelle les attaques par usurpation d'identité peuvent être menées. L'interconnexion des systèmes mondiaux et la dépendance aux tiers ont été illustrées, par exemple, lors de l'incident CrowdStrike où une défaillance opérationnelle a paralysé des systèmes à l'échelle mondiale.

Les évolutions récentes telles que les rançongiciels ciblant les institutions financières, les fraudes sophistiquées par SIM-swap, les attaques sur les chaînes d'approvisionnement et l'armement du renseignement en sources ouvertes (OSINT) ont mis en évidence les limites des réponses isolées au niveau national.

En s'appuyant sur le Cadre de cybersécurité du National Institute of Standards and Technology (NIST), la gouvernance et la protection restent essentielles. Toutefois, la capacité à détecter, à répondre et à se rétablir est désormais primordiale. Autrement dit, dans un monde où il ne s'agit plus de savoir si une attaque aura lieu, mais quand, la résilience devient cruciale. Le partage de renseignements sur les menaces et la mise en place de capacités de réponse aux incidents telles que les équipes de réponse aux incidents de cybersécurité (CSIRT) sont devenus impératifs.

La montée des cybermenaces ciblant les systèmes financiers africains souligne l'urgence d'une action régionale coordonnée. Cette session a porté sur la nécessité de renforcer la coopération transfrontalière en matière de partage de renseignements sur les cyberattaques et de réponse aux incidents, en particulier dans le contexte de la digitalisation croissante, de l'adoption de la monnaie mobile et de l'interconnexion des services financiers à travers le continent. Étant donné que les pays africains présentent des niveaux de maturité différents en cybersécurité, les participants ont convenu qu'une approche harmonisée et coopérative est essentielle pour protéger la stabilité financière régionale et renforcer la confiance des consommateurs.

II. Problématiques clés :

- Absence de cadres transfrontaliers de résilience cyber, de partage de renseignements sur les menaces et de réponses aux incidents permettant une coopération efficace. L'adoption conjointe des attentes de surveillance en matière de résilience cyber (CROE) de la Banque Centrale Européenne, qui visent à renforcer la résilience des systèmes de paiement est, pour le moment, un exemple de bonne pratique manquante ;
- Les capacités en cybersécurité sont fragmentées entre juridictions. Certaines Banques Centrales disposent de centres des opérations de sécurité (SOC) ou de CSIRT, tandis que d'autres ne disposent même pas d'une infrastructure de détection des menaces de base ;
- Certains pays ne disposent pas de lois adaptées à la cybersécurité permettant le partage transfrontalier d'informations et la réponse aux incidents, ou bien sont freinés par des contraintes liées à la protection des données ;
- Il y a un manque de renseignements sur les menaces, de partage des incidents cybernétiques et de plateformes de laboratoires médico-légaux à travers les frontières africaines.

III. Défis identifiés :

- Certaines juridictions peuvent ne pas avoir de mandat clair pour traiter la réponse aux incidents et le partage des menaces dans le domaine de la cybersécurité, d'un point de vue opérationnel et sectoriel ;
- Il y a une mauvaise intégration des parties prenantes : par exemple, des entités non réglementées peuvent représenter un risque pour le secteur financier réglementé, sans être légalement tenues de participer aux structures de partage de renseignement ou de réponse aux incidents ;
- Insuffisance des compétences, ressources et capacités humaines dans certains pays en matière de renseignement sur les menaces, de réponse aux incidents et de criminalistique numérique. Quand elles existent, leur rétention du personnel qualifié reste un défi ;
- La dépendance excessive à des tiers en cybersécurité peut poser des problèmes, ces derniers étant parfois réticents à partager l'information ou à participer aux efforts de réponse ;
- Le reporting en cybersécurité est complexe : il est difficile de savoir quels indicateurs reflètent à la fois les risques encourus et l'efficacité des mesures défensives ;

- Pour obtenir leur adhésion, les conseils d'administration et la haute direction doivent bénéficier de formations sur la cybersécurité et la sensibilisation ;
- L'analyse des menaces est une tâche lourde, nécessitant le traitement de quantité importante de données, ce qui augmente le risque d'omission des signaux d'incidents critiques. Certaines juridictions n'exploitent pas efficacement l'automatisation pour détecter les menaces et anomalies.

IV. Recommandations :

- Cadres pour la résilience cyber, le partage d'informations et la réponse aux incidents à l'échelle transfrontalière :
    - Le Sous-groupe de Travail sur la cybersécurité de l'ABCA devrait envisager la mise en place de trois cadres pour les pays membres de l'ABCA, à savoir la cyber-résilience, l'échange de renseignements sur les menaces et la réponse aux incidents ;
    - Résilience cyber :

      Les pays membres de l'ABCA doivent travailler à l'alignement des cadres de cybersécurité et de résilience, en adoptant éventuellement, les meilleures pratiques internationales afin de soutenir l'harmonisation des normes à travers les frontières ;
    - Partage de renseignement : il conviendrait d'envisager la création d'une plateforme panafricaine de renseignement sur les menaces, une fois que les cadres et les normes pertinents auront été mis en place. Cette plateforme pourrait être développée en collaboration avec l'Union Africaine. En plus, un cadre pour le partage des données entre les membres de l'ABCA doit prendre en compte le respect de la législation sur la protection des données dans toutes les juridictions. De même, les membres individuels doivent examiner comment leurs entités réglementées sont autorisées à partager des données en vertu des cadres législatifs de leurs juridictions respectives ;
    - Réponse aux incidents – SOC, CERT, CSIRT :
        - Le cadre de réponse doit préciser les procédures de gestion et de déclaration des incidents ;
        - Il doit prévoir le développement de plans d'intervention opérationnelle (playbooks), adaptés à chaque juridiction, mais harmonisés au niveau régional ;
        - L'efficacité de ces playbooks doit être testée via des exercices simulés (tabletop) ou des exercices sur cyber-range ;
        - La structure organisationnelle doit être réfléchie : par exemple, un CSIRT national relevant d'un CSIRT régional.
    - Les cadres doivent identifier les structures requises (SOC, CSIRT et ISAC) et définir explicitement les rôles et responsabilités. Des rôles et des responsabilités clairs doivent être définis pour chaque structure, qui doit en fin de compte être établie et rendue possible par les cadres législatifs nationaux. L'intégration des Banques Centrales dans les structures nationales de cybersécurité (partage d'informations

et réponse aux incidents) doit être clarifiée. L'exemple de la Communauté de développement de l'Afrique australe (SADC) peut servir de référence utile.

- Capacités fragmentées et niveaux de maturité différents :
    - Un plan de montée en maturité doit être défini, avec pour point de départ un « produit minimum viable » des structures essentielles et une feuille de route vers une maturité avancée ;
    - Utiliser des référentiels internationaux, comme le C2M2 (Cybersecurity Capability Maturity Model), pour évaluer et améliorer les capacités ;
- Formation, sensibilisation et renforcement des capacités humaines :
    - Les pays membres de l'ABCA doivent adopter une stratégie de développement des compétences autour du renseignement sur les menaces et de la réponse aux incidents. Les conseils d'administration et la haute direction doivent suivre une formation en cybersécurité et sensibilisation pour garantir leur implication et une prise de décision éclairée. Les institutions financières doivent veiller à organiser régulièrement des programmes de sensibilisation à l'intention de leurs employés, des tiers, des clients et d'autres parties prenantes concernées.
- Meilleure utilisation des technologies
    - Il convient également d'envisager l'utilisation des technologies émergentes, notamment l'Intelligence Artificielle, pour renforcer la détection automatisée et rapide des menaces et incidents.

Fait à Rabat, le 23 juillet 2025

LISTE DES PARTICIPANTS

N°	Institution	Nom et prénoms	Fonction	Email
1	Attijariwafa Bank	Mr Mohamed Tazi	Director of Information Systems Security	moh.tazi@attijariwafa.com
2	Attijariwafa Bank	Mrs Fatima Zahra Essami	Staff	
3	Autorité Nationale du Renseignement Financier	Mrs. Najwa Benmadani	Director of the Investigations and Financial Intelligence Division	benmadani@anrf.gov.ma
4	Autorité Nationale du Renseignement Financier	Mr Badr Taiabi	Staff	taiabi@anrf.gov.ma
5	Autorité Nationale du Renseignement Financier	Mr Alae Laachoub	Staff	laachoub@anrf.gov.ma
6	Banco de Moçambique	Mr Jamal Luis Abacar Omar	Executive Director and Board Member	Micaela.Pascoal@bancomoc.mz
7	Banco de Moçambique	Mr Turay Filipe De Melo	Assistant Manager	turay.melo@bancomoc.mz
8	Banco Nacional de Angola	Mr Luis Vieira	Engineer	lvieira@bna.ao

N°	Institution	Nom et prénoms	Fonction	Email
9	Bank of Ghana	Mr Elhanan Owureku Asare	Director	elhanan.asare@bog.gov.gh
10	Bank of Mauritius	Mrs Kaajal Seebaluck-Beerbul	Senior Analyst	kaajal.beerbul@bom.mu
11	Bank of Sierra Leone	Mrs Adama Aduadjoe	IT EXAMINER	aaduadjoe@bsl.gov.sl
12	Bank of Sierra Leone	Mr Edmund Tamuke	Economic Adviser to the Governor	etamuke@bsl.gov.sl
13	Bank of Uganda	Mr Alfred Labu Kurong	Team Leader/Acting Deputy Director	akurong@bou.or.ug
14	Bank of Zambia	Mr Musonda Mathew Mbalazi	Assistant Manager Payment Systems Fintech and Research	mmbalazi@boz.zm
15	Bank of Zambia	Mr Daniel Chibesakunda	Acting Assistant Director - IT Security	dchibesakunda@boz.zm
16	Banque Centrale de la République de Guinée	Mr Kerfalla Sylla	Directeur Adjoint des Systèmes et Moyens de Paiement	kerfalla.sylla@bcrg-guinee.org
17	Banque Centrale de Tunisie	Mr Riadh Mejri	Directeur du Développement et de la Surveillance des Systèmes et des moyens de Paiement	riadh.mejri@bct.gov.tn

N°	Institution	Nom et prénoms	Fonction	Email
18	Banque Centrale de Tunisie	Mr Aymen Rejeb	Head of IT Networks Department	aymen.rejeb@bct.gov.tn
19	Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO)	Miss Fatou Ndiaye	IT Risk Analyst	fndiaye@bceao.int
20	Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO)	Mr Hidja Serge Eric Bama	Adjoint au Directeur des Systèmes d'Information	hsebama@bceao.int
21	Banque Centrale du Congo	Mr Willy Luboa Ngovo	Directeur	luboa@bcc.cd
22	Banque Centrale du Congo	Mr Jimmy Mpongo	Acting IT Director	mpongo@bcc.cd
23	Banque des Etats de l'Afrique Centrale (BEAC)	Mr Wilner Junior Boussougou	Chef de Service en Charge des Opérations Financières et Activités Bancaires	boussougou@beac.int
24	Banque des Etats de l'Afrique Centrale (BEAC)	Mr Mankololo Yebas Pierre Ariel Roger	Chef de Service SMP	arielmankololo@gmail.com

N°	Institution	Nom et prénoms	Fonction	Email
25	Central Bank of Egypt	Mrs Mary Safwat Hanna	Head of Fintech Enablement Office	mary.safwat@cbe.org.eg
26	Central Bank of Egypt	Dr. Mohamed Elsheshtawy	Head of Readiness & Risk Oversight	mohamed.shishtawy@cbe.org.eg
27	Central Bank of Eswatini	Mr Sipho Skosana	Deputy Director Research, BOP and International Economics	Siphos@centralbank.org.sz
28	Central Bank of Kenya	Mr James Yogo	Deputy Director – Cyber Security	yogojo@centralbank.go.ke
29	Central Bank of Kenya	Mr Mike Ombuna	Information Systems Auditor	OmbunaMG@centralbank.go.ke
30	Central Bank of Lesotho	Mr Bafokeng Martin Noosi	Director of Other Financial Institutions Supervision	bnoosi@centralbank.org.ls
31	Central Bank of Liberia	Mr Collins W. Teah Jr.	Senior Technical Advisor	cwteah@cbl.org.lr
32	Central Bank of Liberia	Mr Bouleigh D. Cooper	Deputy Director	bdcooper@cbl.org.lr
33	Central Bank of Libya	Dr. Salem Jebriel	Director of Information Security Department	salsewi@cbl.gov.ly
34	Central Bank of Nigeria	Mr Amarachukwu Nelson Nwosu	Economist/Researcher	annwosu@cbn.gov.ng

N°	Institution	Nom et prénoms	Fonction	Email
35	Central Bank of Nigeria	Mr Waiyeola Itanola Ajakaiye	Assistant Director	wajakaiye@cbn.gov.ng
36	Central Bank of Nigeria	Miss Nafisat Gaffar Olajide	Cybersecurity Operations	ngolajide@cbn.gov.ng
37	Central Bank of Seychelles	Mr Yanick Sauzier	Senior Systems Administrator	yanick.sauzier@cbs.sc
38	Central Bank of Seychelles	Miss Tisha Constance	Financial Surveillance Analyst	tisha.constance@cbs.sc
39	COMESA Clearing House	Mr Brighton Dube	Payments and Transition Officer	bdube@comesach.org
40	COMESA Monetary Institute	Dr. Thomas Bwire	Deputy Director	tbwire@comesa.int
41	COMESA Monetary Institute	Dr. Lucas Njoroge	Director	LNJOROGE@COMESA.INT
42	Commission de l'UEMOA	Mr Kouakou Hyppolite Konan	Chef de la Division du Suivi de la Politique Monétaire	khkonan@uemoa.int
43	East Africa Community (EAC)	Mr Julius Kilonzi Mutemi	Payment Systems Expert	jmutemi@eachq.org

N°	Institution	Nom et prénoms	Fonction	Email
44	Federal Reserve Bank of New York (FRBNY)	Mrs Susmitha Thomas	Associate Director	susmitha.thomas@ny.frb.org
45	IOX Labs 34 Ventures Talaty	Mr Soulaimane Lahrech	Founder of Talaty	soulaimane@talatypay.com
46	National Bank of Rwanda	Mr Songa Chris Musonera	Ag. Manager, Offsite surveillance, Payment Systems	csonga@bnr.rw
47	National Bank of Rwanda	Mr Olivier Mugwaneza	Manager, Financial Sector Policy	omugwaneza@bnr.rw
48	Reserve Bank of Malawi	Dr. Wytone Jombo	Principal Economist	jombowytone@gmail.com
49	Reserve Bank of Zimbabwe	Mrs Julia Njobo	Chief - Digital Financial Services & Licensing	jnjobo@rbz.co.zw
50	South African Reserve Bank	Mr Gerhard Van Deventer	Financial Sector Cybersecurity Consultant	gerhard.vandeventer@resbank.co.za
51	United Nations Economic Commission for Africa (UNECA)	Dr. Adam Elhiraika	Director	elhiraika@un.org
52	West African Monetary Agency (WAMA)	Mr Boima S. Kamara	Director General	bskamara@amao-wama.org

N°	Institution	Nom et prénoms	Fonction	Email
53	West African Monetary Institute (WAMI)	Dr. Sikiru Abdulsalam	Director	saabdulsalam@wami-amao.org
54	World Bank	Mr Mazen Bouri	Lead Financial Sector Specialist	mbouri@worldbank.org
55	Bank Al-Maghrib	Mr Abdouahed Rhiat	Head - Cooperation & Institutional Relations Division	a.rhiat@bkam.ma
56	Bank Al-Maghrib	Miss Ghita Faddi	Deputy Head - Cooperation & Institutional Relations Division	g.faddi@bkam.ma
57	Bank Al-Maghrib	Mr Mohamed Ait Ali	Head of the Protocol and Events Unit	m.aitali@bkam.ma
58	Bank Al-Maghrib	Miss Rabab Akaaboune	Officer in charge of Protocol and Events	r.akaaboune@bkam.ma
59	Bank Al-Maghrib	Mr Zakaria Hasnaoui	Officer in charge of Protocol and Events	z.hasnaoui@bkam.ma
60	Bank Al-Maghrib	Mr. Youssef Maazouzi	Foreign Organization Relations Officer	y.maazouzi@bkam.ma
61	Bank Al-Maghrib	Mr Chihab Saadi	Lab Innovation Department	c.saadi@bkam.ma

N°	Institution	Nom et prénoms	Fonction	Email
62	Bank Al-Maghrib	Mr Nabil Badr	Deputy Head – Banking Supervision Department	n.badr@bkam.ma
63	Bank Al-Maghrib	Mrs Ilham Zainane	Deputy Head – Banking Supervision Department	i.zainane@bkam.ma
64	Bank Al-Maghrib	Mrs Asmaa Hajar Essaid	Responsable du Service Statistiques Monétaires	as.essaid@bkam.ma
65	Bank Al-Maghrib	Mrs. Hiba Afailal	Ingénieur Etudes et Développement	h.afailal@bkam.ma
66	Bank Al-Maghrib	Mrs Dounia Tahri	Adjoint du Responsable de la Direction Statistiques et Gestion des Données	d.tahiri@bkam.ma
67	Bank Al-Maghrib	Mr Yassine El Bada	Ingénieur Data	y.elbada@bkam.ma
68	Bank Al-Maghrib	Mr Lhoussaine Derouich	Responsable du Département Régulation de la Finance Digitale	l.derouich@bkam.ma
69	Bank Al-Maghrib	Mr Nour Dine Hajjami	Responsable de la Direction Système d'Information	n.hajjami@bkam.ma
70	Bank Al-Maghrib	Mr Nassim El Hayani	Expert en Cybersecurité	n.elhayani@bkam.ma
71	Bank Al-Maghrib	Mr Yassine Abane	Responsable du Département Sécurité de l'Information	y.abane@bkam.ma

N°	Institution	Nom et prénoms	Fonction	Email
72	Bank Al-Maghrib	Mr Halim Jadi	Responsable de la Direction Risques, Conformité et Cybersécurité	h.jadi@bkam.ma
73	Bank Al-Maghrib	Mrs Siham Halim	Spécialiste Réglementation SMP Senior	s.halim@bkam.ma
74	Bank Al-Maghrib	Mme Sana Ghafour	Responsable du Service Gestion des Fraudes et Risques Technologiques	s.ghaffour@bkam.ma
75	Bank Al-Maghrib	Mr Mohamed Bazzi El Idrissi	Adjoint du Responsable du Département Stratégie, Transformation	m.bazzi@bkam.ma
76	Bank Al-Maghrib	Mme Sarah Belkasmi	Responsable du Département Communication	s.belkasmi@bkam.ma
77	Bank Al-Maghrib	Chahrazade El Alaoui	Spécialiste Inclusion Financière Senior	c.elalaoui@bkam.ma
78	Bank Al-Maghrib	Mrs Sara Zitouni	Chef de Projet Innovation	s.zitouni@bkam.ma
79	Bank Al-Maghrib	Mr Ilias Dekkoun	Chargé d'organisation	i.dekkoun@bkam.ma
80	AACB Secretariat	Dr. Djoulassi Kokou Oloufade	AACB Executive Secretary	dkoloufade@bceao.int
81	AACB Secretariat	Mr Thierno Mountaga Mbow	Accountant	tmbow@bceao.int
82	AACB Secretariat	Mr Konan Yao Arthur Koffi	Website Manager	kyakoffi@bceao.int
83	AACB Secretariat	Mr Abdourahimoune Amadou Abdoul Aziz	Research Officer	aamadouabdoulaziz@bceao.int

N°	Institution	Nom et prénoms	Fonction	Email
84	AACB Secretariat	Mr Wend-Panga Justin Ouedraogo	Research Officer	jwpouedraogo@bceao.int
85	AACB Secretariat	Mrs Confort Freda Ansayi Akouvi Djamie Amessoudji	Assistant	cfaadeamessoudji@bceao.int