DATAPROTECT
Security is our commitment

# LA CYBER-RÉSILIENCE DU SECTEUR BANCAIRE EN AFRIQUE

## NOUVEAUX DÉFIS POUR LE RÉGULATEUR

Livre Blanc

# LA CYBER-RÉSILIENCE DU SECTEUR BANCAIRE EN AFRIQUE

Une étude DATAPROTECT
Casablanca, 2023

# TABLE DES MATIERES


TABLE DES MATIÈRES....03
TABLE DES ILLUSTRATIONS....05
SIGLES ET ACRONYMES....06
EXECUTIVE SUMMARY....07
PRÉFACE....09
1. PANORAMA DU SECTEUR BANCAIRE AFRICAIN....11
*1.1 - Régulation du secteur bancaire africain....12*
*1.2 - La banque africaine est rentable....12*
*1.3 - Les services bancaires se diversifient....13*
*1.4 - Une spécificité africaine : l'appropriation financière du téléphone mobile....14*
*1.5 - Internationalisation de la banque africaine....14*
*1.6 - Premier essai de coopération financière interafricaine....15*
*1.7 - La recherche en cybersécurité financière....17*
2. LES GRANDS ENJEUX DU SECTEUR BANCAIRE AFRICAIN....18
*2.1 - Numérisation du secteur bancaire....19*
*2.2 - Naissance des néobanques....19*
*2.3 - La déferlante des fintechs....20*
*2.4 - Popularité des solutions infonuagiques....21*
*2.5 - La question de l'argent numérique....22*
Nature des cryptomonnaies....22
Intérêt de l'Afrique pour les cryptomonnaies....22
Du bitcoin au stablecoin....23
Naissance de la monnaie numérique de banque centrale....23
Le Nigeria ouvre la marche....23
Les essais pilotes d'Afrique du Sud et du Ghana....24
Le cas de la Centrafrique....24
3. LE CYBERCRIME COMME CONTREPARTIE DE LA TRANSFORMATION DIGITALE....25
*3.1 - La cybersécurité se transforme en cyber-résilience....26*
*3.2 - La cybercriminalité en Afrique....27*
Benchmark de l'état de la cybercriminalité en Afrique....27
Aperçu sur la cybercriminalité générale....28
Aperçu sur la cybercriminalité dans le secteur bancaire....29
*3.3 - Le coût de la cybercriminalité dans le secteur bancaire....30*
*3.4 - Les outils du cybercrime....31*
• Les escroqueries en ligne et l'hameçonnage....32
• Fraude au président....33
• Botnets et chevaux de Troie....35
• Rançongiciels....36
• RaaS....36
*3.5 - La menace s'étend à la périphérie du secteur bancaire....37*
Le cas de la fintech....37
Quand la menace vient du ciel....37
Les cryptomonnaies et l'anarchie de la finance décentralisée....38
Le cas de la monnaie numérique....38

# TABLE DES MATIERES


4. COMMENT LE SECTEUR FINANCIER LUTTE CONTRE LA CYBERCRIMINALITÉ.....39
*4.1 - L'approche politique*.....40
Stratégie nationale de cybersécurité.....40
Concertation panafricaine.....41
Concertation régionale.....42
Le cas particulier d'AFRIPOL.....42
Traités internationaux.....43
*4.2 - L'approche réglementaire*.....43
Réglementation nationale.....43
Approche associative.....44
Réglementation internationale.....45
5. DISCUSSION SUR DEUX EXEMPLES DE RÉGLEMENTATION NATIONALE.....46
*5.1 - Cas de Bank Al-Maghrib : Innovation et renforcement de la cyber-résilience*.....47
La réglementation.....48
Coordination et échange d'information.....49
Surveillance des risques.....50
Pilier renforcement des capacités.....51
*5.2 - Cas de la Banque du Canada : Réduire les risques et renforcer la résilience*.....51
Le parcours de la Banque du Canada en matière de cybersécurité.....52
Stratégie de cybersécurité de la Banque du Canada.....52
Rôle de l'autorité de réglementation.....54
6. CONCLUSIONS ET MEILLEURES PRATIQUES.....55
*6.1 - Pilier Réglementation*.....56
Principe 1 : Cyber-résilience du secteur financier.....56
Principe 2 : Nécessité de garantir la cyber-résilience.....56
Principe 3 : Convergence panafricaine des réglementations.....56
*6.2 - Pilier Surveillance des Risques*.....57
Principe 4 : Surveillance et mise en place d'un SOC.....57
Principe 5 : Plan d'intervention en cas de cyberincident.....57
Principe 6 : Notification obligatoire des incidents.....58
Principe 7 : Cartographie et quantification des risques.....58
Principe 8 : Produire un référentiel sur l'utilisation du nuage (cloud).....59
Principe 9 : Effectuer un cyber stress test.....59
Principe 10 : Unité interne de fintech.....60
*6.3 - Pilier Coordination et échange d'information*.....60
Principe 11 : Création d'un CERT financier.....60
Principe 12 : Groupe de partage d'information financière.....62
*6.4 - Pilier Renforcement des Capacités*.....63
Principe 13 : Sensibilisation continue.....63
Principe 14 : Recrutement des talents internes.....64
Principe 15 : Nécessité d'une cyber-gouvernance.....64
Principe 16 : Enregistrement des fintechs.....65
Principe 17 : Sandbox réglementaire.....65
ANNEXE 1 : BIBLIOGRAPHIE CHOISIE.....67
ANNEXE 2 : EFFORTS DES NATIONS UNIES EN MATIÈRE DE CYBERSÉCURITÉ.....69

# TABLE DES ILLUSTRATIONS


***Figure 1*** – *Population adulte possédant un compte bancaire en Afrique subsaharienne*.....12
***Figure 2*** – *Dynamisme du secteur bancaire africain (pré-Covid)*.....13
***Figure 3*** – *Services financiers numériques d'Afrique*.....13
***Figure 4*** – *Les dix plus grands groupes bancaires africains*.....15
***Figure 5*** – *Comment fonctionnent les paiements instantanés*.....16
***Figure 6*** – *Les 12 pays africains les plus mûrs en cybersécurité*.....27
***Figure 7*** – *Bilan récapitulatif de la cybermenace*.....28
***Figure 8*** – *Proportion des banques à risque en Afrique subsaharienne*.....29
***Figure 9*** – *Principaux types d'outils du cybercrime*.....31
***Figure 10*** – *Impact sectoriel du hameçonnage*.....32
***Figure 11*** – *Carte des acteurs africains de la fraude au président*.....34
***Figure 12*** – *L'état de la législation sur la cybercriminalité en Afrique*.....41
***Figure 13*** – *Pays ayant signé ou ratifié la convention de Malabo*.....42
***Figure 14*** – *Banques centrales ayant un cadre d'analyse des cyber-risques*.....44
***Figure 15*** – *Les banques centrales africaines sont favorables au partage d'information*.....44
***Figure 16*** – *... mais elles ne partagent pas l'information sur les cyber-incidents*.....45
***Figure 17*** – *Les quatre piliers d'action de la banque centrale du Maroc*.....47
***Figure 18*** – *Objectifs internes de la stratégie de cybersécurité de la Banque du Canada*.....52
***Figure 19*** – *Objectifs externes de la stratégie de cybersécurité de la Banque du Canada*.....53
***Figure 20*** – *Test d'intrusion traditionnel et TCFR*.....54
***Figure 21*** – *Les grands vecteurs d'action des banques centrales*.....55
***Figure 22*** – *Cycle d'intervention en cas d'incident*.....57
***Figure 23*** – *Modèle de référentiel sur le recours au nuage*.....59
***Figure 24*** – *Objectifs de l'unité interne de fintech de la banque centrale d'Afrique du Sud*.....60
***Figure 25*** – *Place du CERT dans la cybersécurité*.....61

# SIGLES ET ACRONYMES

| | |
|---|---|
| ABCA | Association des Banques Centrales Africaines |
| ACRC | Centre africain de ressources sur la cybersécurité pour l'inclusion financière |
| ADD | Agence de Développement du Digital |
| ADFI | Africa Digital Financial Inclusion facility |
| ANRT | Agence Nationale de Réglementation des Télécommunications |
| API | Application Programming Interface |
| ASIS | American Society for Industrial Security |
| BCEAO | Banque Centrale des États de l'Afrique de l'Ouest |
| BEAC | Banque des États de l'Afrique Centrale |
| BIS | Bank for International Settlements (en français BRI) |
| BRI | Banque des Règlements Internationaux (en anglais BIS) |
| BSA | Business Software Alliance |
| CBDC | Central Bank Digital Currency (en français MNBC) |
| CEMAC | Communauté Économique et Monétaire en Afrique Centrale |
| CERT | Computer Emergency Response Team |
| CIRT | Computer Incident Response Team |
| CSIRT | Computer Security Incident Response Team |
| CSP | Customer Security Programme (norme de SWIFT) |
| DLT | Distributed Ledger Technology (en français: technologie du registre distribué) |
| DSI | Directeur des Systèmes d'Information |
| GAFA | Google, Amazon, Facebook, Apple (on ajoute parfois Microsoft, ce qui donne GAFAM) |
| GSM | Global System for Mobile Communications |
| IMF | Infrastructures de Marchés Financiers |
| ISO | International Organization for Standardization |
| ISP | Information Systems Professional |
| ISPA | INTERPOL's Support Programme for the African Union |
| ITCP | Information Technology Certified Professional |
| MNBC | Monnaie Numérique de Banque Centrale (en anglais CDBC) |
| NIST-CSF | National Institute of Standards and Technology-Cybersecurity Framework |
| PAPSS | Panafrican Payment and Settlement System |
| PKI | Public Key Infrastructure |
| PME | Petites et Moyennes Entreprises |
| PMP | Project Management Professional |
| R-D | Recherche et Développement |
| RFID | Radio Frequency Identification |
| RGPD | Règlement Général sur la Protection des Données |
| RSSI | Responsable de la Sécurité des Systèmes d'Information |
| RVP | Réseau Virtuel Privé |
| SIEM | Security Information and Event Management |
| SOC | Security Operations Center |
| SSCP | Systems Security Certified Practitioner |
| SWIFT | Society for Worldwide Interbank Financial Telecommunication |
| TIC | Technologies de l'Information et Communications |
| TSCP | Transglobal Secure Collaboration Program |
| UEMOA | Union Économique et Monétaire Ouest-Africaine |
| UIT | Union Internationale des Télécommunications |
| USSD | Unstructured Supplementary Service Data |
| ZLECAf | Zone de Libre-Échange Continentale Africaine |

# EXECUTIVE SUMMARY

L'Afrique enregistre depuis quelques années des taux de croissance supérieurs à ceux du reste du monde. La croissance économique du continent devrait dépasser celle du reste du monde au cours des deux prochaines années, avec un produit intérieur brut réel d'environ 4 % en moyenne en 2023 et 2024.[1] L'Afrique est aujourd'hui synonyme de croissance économique, d'intégration rapide des nouvelles technologies, de moindre dépendance des revenus des matières premières et d'émergence d'une classe moyenne de plus en plus importante.

Le secteur bancaire africain est un contributeur de premier ordre à cet essor. En effet, le dynamisme remarquable dont fait preuve le secteur témoigne de son expansion et de sa résilience face aux défis économiques et politiques. La régulation du secteur bancaire africain s'est inscrite dans un process d'amélioration continue, offrant un cadre propice à la croissance et à la stabilité financière. Les banques africaines sont devenues des acteurs clés du développement économique en fournissant des services financiers adaptés aux besoins locaux, favorisant ainsi l'inclusion financière et la réduction de la pauvreté.

Si la transformation digitale amorcée par les banques africaines a permis l'émergence de solutions innovantes favorisant l'inclusion financière et l'accès aux services bancaires, celle-ci a considérablement accrut les surfaces d'expositions aux risques cyber. L'étude **DATAPROTECT "La cyber-résilience du secteur bancaire en Afrique : nouveaux défis pour le régulateur"** se propose d'examiner les différents aspects de cette problématique complexe pour présenter, en fin d'ouvrage, une série de recommandations à l'adresse des banques centrales africaines pour renforcer la sécurité et la cyber résilience dans ce domaine crucial. Nous sommes convaincus qu'au fur et à mesure que le monde se transforme et se consolide, que les modes de travail évoluent, les frontières de la cybersécurité s'étendent. Avec chaque nouvel appareil connecté, découverte numérique ou processus automatisé, de nouvelles vulnérabilités et des préoccupations en cybersécurité émergent.

Le premier pan de l'étude propose un panorama du secteur bancaire africain, mettant en évidence la régulation en place, la rentabilité des banques africaines, la diversification des services bancaires et l'adoption croissante de la finance mobile en tant que spécificité africaine. Nous y abordons également le processus d'internationalisation des banques africaines et les premières tentatives de coopérations financières interafricaines. Dans un second temps, nous avons choisi de braquer les projecteurs sur les grands enjeux auxquels est confronté le secteur bancaire africain en explorant la numérisation du secteur bancaire, l'émergence des néo-banques, l'essor des fintechs et la popularité croissante des solutions infonuagiques (Cloud). Nous analysons également la question de l'argent numérique, en mettant en évidence les aspects liés aux cryptomonnaies, du bitcoin aux stable coins, ainsi que les initiatives de monnaie numérique de banque centrale dans certains pays africains.

**Le cœur de l'étude commence au troisième volet.**
Nous y examinons le cybercrime comme contrepartie inévitable de la numérisation et comment le concept de cybersécurité devrait entamer sa transformation pour devenir **cyber-résilience**. Nous définissons la cyber-résilience comme '' la capacité d'une organisation à continuer à remplir sa mission en anticipant et en s'adaptant aux cybermenaces et à d'autres changements pertinents dans l'environnement, ainsi qu'en résistant, en réduisant et en se relevant rapidement des cyber-incidents."[2]. Cela signifie qu'en mesurant son niveau de compétence et de résilience en matière de cyber sécurité, une organisation sera plus à même de poursuivre ses activités avec peu ou pas de temps d'indisponibilité.

Il nous est apparu structurant d'apporter des éléments d'analyse quant au coût de la cybercriminalité pour les banques et des outils utilisés par les cybercriminels. Ces techniques étant en perpétuel changement, nous avons néanmoins tenu à lister les différents types d'attaques les plus fréquents pour servir de cadre de référence et savoir reconnaitre les symptômes d'une attaque DDoS ou d'un logiciel malveillant.

*1 https://www.afdb.org/fr/news-and-events/press-releases/la-croissance-economique-de-lafrique-depassera-les-previsions-mondiales-en-2023-2024-selon-le-rapport-semestriel-de-la-banque-africaine-de-developpement-58301*
*2 "Annual report 2020-21", Bank for International Settlements (BIS), 219 pages. Cf. p. 87.*

# EXECUTIVE SUMMARY

Dans son quatrième volet, l'étude se penche sur le volet réglementaire et les mesures prises par le secteur bancaire africain pour lutter contre la cybercriminalité. Nous examinons les approches politiques, les stratégies nationales de cybersécurité, la coopération panafricaine et les réglementations internationales. Nous nous sommes particulièrement penchés sur trois formes de lutte contre le cybercrime pour les banques centrales : **politique, réglementaire et compétences (Skills).**

Convaincus qu'il faille agrémenter notre étude avec des ''business cases''(ou cas pratiques) concrets, nous avons tenu des discussions approfondies avec les responsables de la réglementation de deux banques centrales : **Bank Al Maghrib (Royaume du Maroc) et Banque du Canada (Canada)** pour examiner les mesures prises par ces institutions pour innover, renforcer la cyber-résilience et réduire les risques. Les témoignages des responsables de ces institutions nous ont permis de documenter différentes facettes de la lutte contre le risque cyber selon 4 axes structurants portant sur : **le volet réglementaire, la surveillance des risques, la coordination et l'échange d'information et le renforcement des capacités** pour le cas marocain et 2 volets stratégiques pour le cas canadien à savoir : **interne et externe.**

Enfin, dans la dernière partie, nous présentons une série de conclusions clés et des meilleures pratiques à l'adresse des banques centrales. Nous proposons des principes et des recommandations pour chaque pilier clé en suivant la typologie de Bank Al Maghrib. Cette étude vise essentiellement à sensibiliser les acteurs du secteur bancaire, les régulateurs et les décideurs aux défis croissants de la cyber-résilience en Afrique. Elle offre des perspectives et des recommandations concrètes pour renforcer la sécurité et la résilience dans ce domaine critique, afin de garantir la stabilité et la confiance dans le secteur bancaire africain face à l'évolution des menaces et des technologies.

A travers cette étude, Dataprotect ambitionne de donner aux Gouverneurs, Directeurs généraux et aux Responsables de la Sécurité des Systèmes d'Information des banques centrales et commerciales africaines, des éléments d'information et des sources d'inspiration.

Nous souhaitons, à travers cette étude, apporter notre contribution au renforcement de la cybersécurité et la cyber résilience dans les banques africaines et rappeler que DATAPROTECT est bien plus qu'une société de conseil en cybersécurité. Nous sommes un partenaire capable d'accompagner les régulateurs dans leur processus de transformation digitale. En plus de l'apport technologique, aussi sophistiqué soit-il, nous sommes capables de déployer une stratégie qui englobe l'ensemble de l'écosystème bancaire, y compris les fintechs tout en respectant l'ensemble des exigences légales et réglementaires pertinentes relatives à la protection et à la confidentialité des données.

# PREFACE

Par **Ali El Azzouzi**,
*CEO de DATAPROTECT*

***Ce qui arrive en fin de compte, ce n'est pas l'inévitable mais l'imprévisible***

*John Maynard Keynes*[3]

La fraude bancaire en Afrique subsaharienne n'a cessé de faire de nouvelles victimes. Non seulement la cybercriminalité augmente en nombre d'attaques, mais elle gagne en sophistication. L'évolution technologique contribue à cette évolution de tous les dangers. Il va de soi que la transformation digitale des banques accroît la surface d'exposition au risque cyber. Mais il y a plus. La nature de l'institution financière change.

Tous les services financiers sont en passe d'être offerts en ligne. L'Afrique est en tête de ce mouvement mondial grâce à l'adoption massive de l'argent mobile. Les banques ont réagi en recourant au cloud qui offre des solutions à la fois élégantes et peu coûteuses pour offrir des services en ligne de haute qualité. Les fintechs ont saisi la balle au vol et lancent des applications mobiles de toutes sortes.

Signe irréfutable du succès: six fintechs africaines sont d'ores et déjà considérées comme des licornes. Les investisseurs internationaux ne s'y trompent pas et investissent massivement. On parle d'un milliard et demi USD seulement pour l'an passé.[4] Cependant, cette expansion rapide à l'ère post covid a trop souvent relégué les exigences de cybersécurité au second plan sous prétexte de « time to market ».

La cybercriminalité attaque le ventre mou du secteur bancaire: les services mobiles, le cloud et les fintechs. Toute cette périphérie est en ébullition constante: les innovations se succèdent à un

rythme effréné. Or, la réglementation ne suit pas toujours. Les modèles traditionnels de cybersécurité ne suffisent plus ou sont inadaptés à un environnement où les frontières entre le monde physique et le monde virtuel sont devenues poreuses.

La notion même de périmètre à défendre a disparu. L'origine des vulnérabilités est aussi bien interne qu'externe. On parle alors de "confiance zéro", ce qui signifie de ne jamais faire confiance à quiconque et de toujours vérifier. Cette approche nouvelle, qui multiplie les contrôles sur les flux d'information, exclut toute improvisation en matière de cybersécurité. L'heure des interventions brillantes d'un expert de talent est finie.

Déjà dans notre étude de 2019 sur "La fraude bancaire en Afrique subsaharienne" nous évoquions cette course technologique avec le crime organisé. Voilà pourquoi, nous préconisions l'intelligence artificielle (IA) comme "arme de choix de cette concurrence". Impossible de tout vérifier à la main. Il faut que nos "solutions de cybersécurité intègrent des moteurs d'IA" pour "effectuer de l'analyse comportementale".

**3** *Citation originale: "The inevitable never happens. It is the unexpected always."*
**4** *"Fintech Dominates Africa Startup Funding and Unicorn Club", Fintech Africa, 1er mars 2023.*

Aujourd'hui plus encore qu'hier, le recours à l'IA est incontournable. Les modes opératoires des cybercriminels ont explosé. Depuis les attaques ciblant les plateformes monétiques, notamment les cartes prépayées, jusqu'aux virements frauduleux, en passant par les plateformes SWIFT et de transfert d'argent, rien n'y échappe. Derrière ces attaques, tout un écosystème cybercriminel bien rodé tire profit de l'absence de contrôles élémentaires qui caractérise la périphérie bancaire.

Ce n'est pas parce qu'une banque externalise ses services dans le cloud que ceux-ci sont à l'abri. Les malfaiteurs sont capables de pénétrer dans les clouds les mieux protégés si les services hébergés ne le sont pas. Le résultat de cette explosion des modes opératoires est la création d'un knowledge malveillant accessible dans le dark web et permettant à des personnes motivées par l'appât du gain de franchir le pas et de passer à l'acte.

Sur les décombres du périmètre disparu, il faut inventer un nouveau paradigme axé sur l'utilisateur, son exigence de convivialité alliée à la volonté de protéger la confidentialité de ses données personnelles. Pour cela, il faut que l'intégrité de l'établissement de crédit couvre la gouvernance, le risque opérationnel, la gestion des relations avec les fournisseurs, la continuité des activités en cas d'incident, y compris le plan de relève.

La combinaison de tous ces facteurs dépasse le cadre trop étroitement technologique de la cybersécurité pour se transformer en cyber-résilience. C'est ici qu'intervient la présente étude basée sur l'actualité la plus brûlante et sur l'expérience de terrain de Dataprotect. Pour répondre à une cybercriminalité plus diversifiée et plus sophistiquée que jamais, une banque isolée, aussi bien équipée soit-elle, ne suffit pas.

La réponse au cybercrime doit mobiliser le secteur bancaire organisé. C'est la conviction des experts Dataprotect. Or, seule la banque centrale ou, quand il est distinct, l'organisme de régulation, a la capacité de structurer une telle réponse, par son pouvoir réglementaire justement, mais aussi par son rôle de leader du secteur financier. Outre son mandat principal qui est de conduire la politique monétaire du pays concerné, la banque centrale a aussi la responsabilité de veiller au risque opérationnel.

Dans l'étude qui suit, Dataprotect évoque brièvement le nouvel écosystème bancaire, décrit la prolifération des formes de cybercriminalité, met en valeur la riposte du secteur financier qui effectue sa transition vers la cyber-résilience et, enfin, élabore une ébauche de définition du défi qui attend les banques centrales sous forme de recommandations. Loin d'être des injonctions, ces recommandations doivent plutôt être considérées comme des pistes exploratoires.

Délibérément placées sous le signe de la cyber-résilience, nos recommandations sont articulées autour de quatre grands axes d'intervention: la réglementation proprement dite, la surveillance des risques, la coordination et l'échange d'information, le renforcement des capacités. De par sa nature réseautée, le secteur bancaire est particulièrement vulnérable, il est vrai, mais en même temps, il est mieux armé que tout autre secteur économique pour affronter le risque cyber.

# 1

# PANORAMA DU SECTEUR BANCAIRE AFRICAIN

Le secteur bancaire est un des plus régulé de l'économie. Aussi est-il opportun de commencer ce panorama par un bref rappel de la situation réglementaire de l'Afrique en la matière.

# 1 PANORAMA DU SECTEUR BANCAIRE AFRICAIN

## 1.1 - Régulation du secteur bancaire africain

Chaque pays ou zone économique dispose de sa propre banque centrale, dont l'actionnaire est l'État. La banque centrale assure la stabilité monétaire d'un pays. À cette fin, elle doit éviter tout dysfonctionnement lié à un ou plusieurs risques, en particulier le cyber-risque, qui peut avoir des effets en cascade et mettre en danger l'ensemble du système financier national.

Au total, l'Afrique compte 41 banques centrales qui sont réunies au sein de l'Association des banques centrales africaines (ABCA), dont le siège est à Dakar. Il y a une banque centrale par pays, sauf dans deux exceptions :

- Les huit pays membres de l'Union économique et monétaire ouest-africaine (UEMOA) - Bénin, Burkina Faso, Côte d'Ivoire, Guinée-Bissau, Mali, Niger, Sénégal et Togo - se sont regroupés pour confier leur politique monétaire à la Banque centrale des États de l'Afrique de l'Ouest (BCEAO). Son siège social est à Dakar (Sénégal).
- Les six pays membres de la Communauté économique et monétaire de l'Afrique centrale (CEMAC) - Cameroun, République centrafricaine, République du Congo, Gabon, Guinée équatoriale et Tchad - ont fait de même au profit de la Banque des États de l'Afrique centrale (BEAC). Son siège est à Yaoundé (Cameroun).

Le secteur bancaire est régulé au niveau international par toute une série d'instances dont la principale est la Banque des règlements internationaux (BRI) dont le siège social est à Bâle (le rôle de la BRI est abordé au point 4.2 - L'approche réglementaire, section Réglementation internationale).

Sur le plan national, la fonction de réglementation est généralement assurée par la banque centrale en Afrique. Deux exceptions majeures, toutefois, l'UEMOA et la CEMAC où il existe une autorité de réglementation distincte de la banque centrale, respectivement la Commission Bancaire de l'Union Monétaire Ouest Africaine (BC-UMOA) basée à Abidjan et la Commission bancaire de l'Afrique centrale (COBAC) dont le siège est à Libreville.

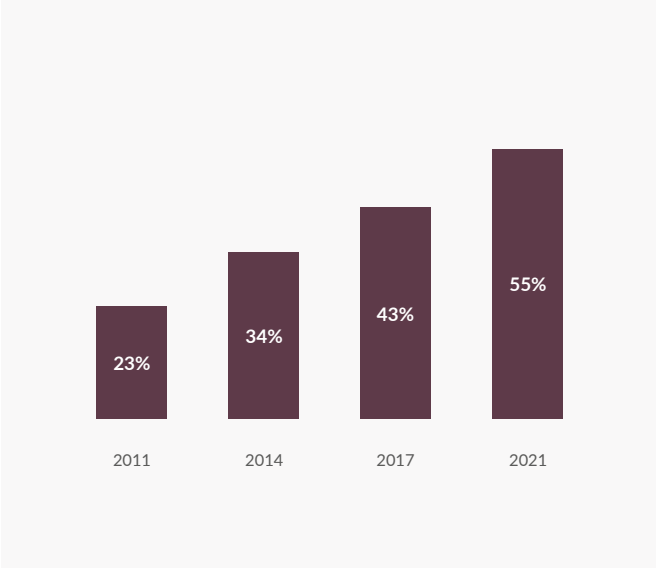
Que ce soit par le truchement de la banque centrale ou d'une autorité distincte, le régulateur national joue un rôle clé. D'une part, il a pour mission de réglementer directement ainsi que d'accompagner en continu les banques commerciales. D'autre part, il établit la liaison entre les instances internationales et les banques commerciales. D'une manière générale, on peut dire que la réglementation internationale est appliquée sur le terrain par le régulateur national.

## 1.2 - La banque africaine est rentable

La bancarisation de l'Afrique a enfin décollé. Il y a une raison structurelle à ce nouveau boom : l'Afrique est le continent qui connaît la plus forte expansion démographique au monde. Sa population est très jeune, c'est surtout le cas en Afrique subsaharienne où 40% des habitants avaient moins de 15 ans en 2021 – la moyenne mondiale est de 25% (Statista). L'éducation y croît rapidement : aujourd'hui, 83% des enfants terminent leurs études primaires, contre 65% en 2000.[5]

Pour les banques africaines, cela signifie que le taux de nouveaux comptes augmente rapidement: au sud du Sahara, il représentait 43% de la population adulte en 2017, il est passé à 55% en 2022. Il ne faut donc pas s'étonner si le secteur bancaire africain est devenu à la fin des années 2010 un des plus dynamique au monde : le deuxième en termes de croissance et de profitabilité – derrière l'Amérique latine.

**FIGURE 1 -** POPULATION ADULTE POSSÉDANT UN COMPTE BANCAIRE EN AFRIQUE SUBSAHARIENNE

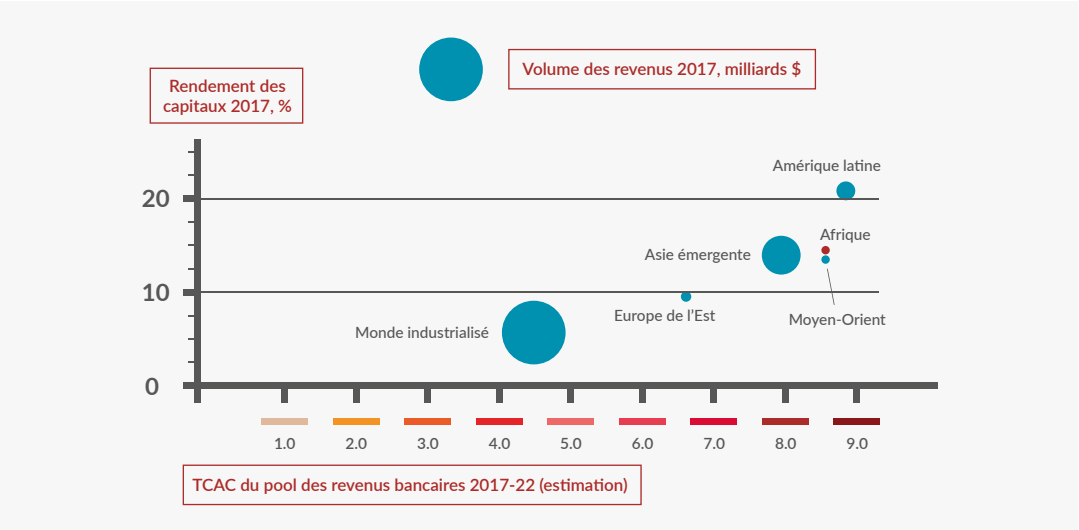



*Source : Global Findex Database, World Bank, 2021.*

Telle du moins était la situation jusqu'à ce que le Covid ne fasse chuter le taux de rendement moyen de moitié, passant de 14 % en 2019 à 7 % en 2020 – suivi il est vrai d'une forte reprise. Aujourd'hui, le taux de rendement demeure encore un ou deux points au-dessous de la période pré-Covid, même si les revenus sont plus élevés que jamais auparavant.[6]

*5 "Transformer l'éducation en Afrique", UNICEF, septembre 2021, pp. 11 et 12.*
*6 Omar Dayi, François Jurd de Girancourt, Ahmed Fjer et Zandile Makgatho, "African banking: The productivity opportunity", McKinsey & Company, 6 décembre 2022.*
*- François Jurd de Girancourt, Aalind Gupta, Shikha Gupta et Uzayr Jeenah, "African banking in the new reality", McKinsey, 25 mars 2021.*

**FIGURE 2 -** DYNAMISME DU SECTEUR BANCAIRE AFRICAIN (PRÉ-COVID)



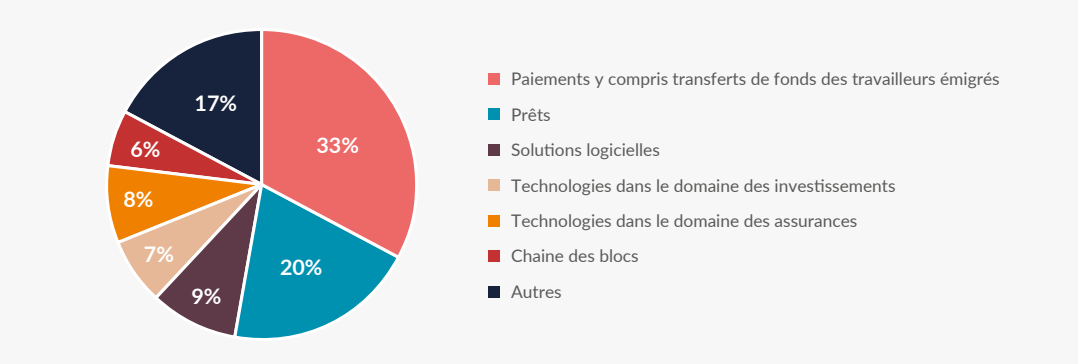

*Source : McKinsey Global Banking Pools, 2017*

L'Afrique compte environ 760 banques commerciales - ce qui est relativement peu comparé aux 4 000 banques des États-Unis ou aux 6 000 banques d'Europe (Statista). En Afrique même, le nombre de banques varie beaucoup d'un pays à l'autre, mais le nombre de banques n'est en rien indicatif de la performance du système bancaire.[7]

## 1.3 - Les services bancaires se diversifient

Les services de paiement (y compris les transferts de fonds des travailleurs émigrés) et de prêt constituent toujours les produits phares de la banque africaine, mais leur proportion diminue année après année. En effet, la numérisation favorise la diversification. Les domaines de croissance sont les solutions logicielles et l'utilisation de la technologie de la chaîne de blocs. Les réponses regroupées dans la catégorie "Autres" comprennent une gamme variée de domaines en forte croissance, en particulier la cybersécurité et les technologies réglementaires.[8]

**FIGURE 3 -** SERVICES FINANCIERS NUMÉRIQUES D'AFRIQUE




*Source : Banque européenne d'investissement, 2022.*

*7 Emmanuel Abara Benson, "These 7 African countries have the highest number of commercial banks", Business Insider Africa, 25 juillet 2022. Le nombre de banques est sujet à variation quotidienne en raison des créations et fusions-acquisitions. Ce chiffre est cité à titre indicatif.*
*8 "La finance en Afrique : naviguer en eaux troubles", Banque européenne d'investissement (BEI), 2022, 148 pages. Cf. pp. 99-100.*

# 1 PANORAMA DU SECTEUR BANCAIRE AFRICAIN

## 1.4 - Une spécificité africaine : l'appropriation financière du téléphone mobile

L'autre phénomène qui contribue à dynamiser le secteur financier africain est technologique. L'adoption massive du téléphone mobile est en passe de faire de l'Afrique le continent numérique du XXIe siècle. Nous avons vu que 55 % des adultes d'Afrique subsaharienne disposent d'un compte bancaire (voir figure 4 - Taux de la population adulte possédant un compte bancaire en Afrique subsaharienne). Encore faut-il préciser que sur ce montant, 33 % de ces comptes sont mobiles.[9]

Le téléphone est devenu un outil financier. Il y a un « miracle » africain. À la faveur d'un phénomène d'appropriation, une population largement rurale et sans accès au système financier, a détourné le téléphone mobile de sa fonction initiale pour en faire un moyen de paiement de personne à personne. Il suffit d'utiliser une partie des montants versés pour la recharge de la carte SIM. La simplicité du système est telle que son succès a été immédiat.

Pour permettre aux utilisateurs d'effectuer cette opération, les opérateurs de télécommunications utilisent une fonctionnalité peu connue de la technologie GSM appelée Unstructured Supplementary Service Data (USSD). Ce protocole permet de déclencher un service par envoi d'un message. Contrairement à un SMS, il n'y a aucun stockage en USSD, les informations sont disponibles seulement durant l'ouverture de la session et disparaissent ensuite. C'est une fonctionnalité basique qui ne nécessite pas le recours à une infrastructure lourde.[10]

Le protocole USSD est donc un véritable outil de démocratisation des usages numériques. Toutefois, les applications de paiement en ligne demeurent rudimentaires et ne transforment pas pour autant le téléphone mobile en véritable compte bancaire : les opérateurs de télécommunications ne sont pas autorisés à consentir de crédit à leurs clients. Même ceux d'entre eux qui ont obtenu une licence d'émetteur de monnaie électronique demeurent limités par la réglementation en vigueur.

Ces services sont offerts par les opérateurs ou par des start-ups spécialisées en développement des technologies financières – les fintechs. Au total, des milliers d'applications pour téléphones intelligents sont nées qui réinventent la nature du secteur financier et lui permettent de mieux coller à la réalité africaine.

Dans bien des cas, les détenteurs d'un compte mobile ont d'ailleurs été incités à ouvrir un véritable compte bancaire. Pour leur part, les banques classiques passent souvent des accords avec les compagnies de téléphone pour desservir les régions rurales où elles n'ont pas de succursales. Les deux industries sont tour à tour concurrentes et partenaires.

## 1.5 - Internationalisation de la banque africaine

Auparavant, le secteur bancaire africain relevait d'une ancienne structure postcoloniale: maison mère située en Europe ou plus rarement en Amérique du Nord et seules les succursales se trouvaient en Afrique. Aujourd'hui, tout change. Non seulement la banque africaine prend son autonomie, mais elle commence à essaimer à la grandeur du continent et parfois même au-delà.

Ce mouvement s'articule autour de trois pôles: au premier rang se trouve l'Afrique du Sud qui compte cinq des 10 plus grandes banques du continent. Les banques sud-africaines représentent près de 40 % du total des actifs du continent. À fins de comparaison, il faut quand même noter que la première banque sud-africaine, la Standard Bank, occupe seulement la 152e position dans le Top 1000 des institutions mondiales.

Deuxième pôle: l'Égypte bénéficie d'une culture bancaire qui remonte à la fin du XIXe siècle ainsi que d'un secteur financier éprouvé. Depuis quelques années, trois banques, à savoir National Bank of Egypt, Banque Misr et Commercial International Bank, ont multiplié les investissements dans la Corne de l'Afrique, pays où la pénétration bancaire est faible et où les acteurs locaux sont peu nombreux. Les banques égyptiennes semblent ainsi privilégier les marchés africains les moins développés.

Enfin, le Maroc a commencé dès les années 1990 le processus d'internationalisation de son secteur bancaire. Les banques marocaines détiennent une part de marché de près de 30 % des comptes bancaires dans des pays tels que le Bénin, le Nigéria, la Côte d'Ivoire, le Togo, le Sénégal, le Mali, le Niger et la Guinée. Signalons, en particulier, BCP qui a maintenant des succursales ou des filiales dans 28 pays dont 14 en Afrique et Attijariwafa Bank qui a essaimé dans 21 pays dont 16 en Afrique.[11]

*__9__ "The Global Findex Database », World Bank, 2021, 184 pages. Cf. p. 2.*
*__10__ "En Afrique, 62% des systèmes de paiement instantané utilisent les protocoles USSD", Agence Ecofin, 8 mars 2023.*
*- Joyce Imiegha, "The History and Importance of USSD in Africa's Digital Landscape", Blog USSD, 24 février 2023. - Jacqueline Jumah et Sabine Mensah, "All Eyes on Instant Payments for Greater Financial Inclusion in Africa", Digital Banker Africa Magazine, 2 juin 2022.*
*__11__ GBO Specialist, "List of largest African Banks in the world", MoneyGate, 1er janvier 2023. - Chloe Domat, "Egyptian And Moroccan Banks Spread Across Africa", Global Finance, 6 octobre 2022. - Emmanuel Abara Benson, "10 largest banks in Africa based on asset size", Business Insider Africa, 10 septembre 2022.*

Hors de ces trois pôles dominants, le reste de l'Afrique compte également plusieurs banques de grande valeur, au premier rang desquelles on peut citer la nouvelle génération de banques nigérianes, emmenées par Access Bank et First Bank. Autre "success story", le groupe togolais Ecobank qui a déjà essaimé dans 35 pays africains et a déjà ouvert des bureaux à Paris, Londres, Dubaï et Beijing.

Toutefois, les institutions européennes contrôlent encore 43% du secteur bancaire africain, même si ces institutions sont généralement en train de réduire leur présence – à l'instar de BNP Paribas et BPC. Même la Société Générale, qui a longtemps joué la carte du développement africain, entame en 2023 un mouvement de retrait.[12]

**FIGURE 4 -** LES DIX PLUS GRANDS GROUPES BANCAIRES AFRICAINS

| Classement | Banque | Pays | Actifs (millions USD) |
|---|---|---|---|
| 1 | **Standard Bank Group (Stanbank)** | Afrique du Sud | 161,9 |
| 2 | **National Bank of Egypt** | Égypte | 96,7 |
| 3 | **FirstRand** | Afrique du Sud | 91,7 |
| 4 | **Absa Bank** | Afrique du Sud | 82,5 |
| 5 | **Nedbank Group** | Afrique du Sud | 75,9 |
| 6 | **Banque Misr** | Égypte | 58,1 |
| 7 | **Attijariwafa Bank** | Maroc | 55,6 |
| 8 | **Banque Centrale Populaire** | Maroc | 45,1 |
| 9 | **BMCE Bank Group** | Maroc | 32,9 |
| 10 | **Investec Bank** | Afrique du Sud | 29,9 |

*Source : List of largest African Banks in the world, MoneyGate, 1er janvier 2023.*

## 1.6 - Premier essai de coopération financière interafricaine

Un nouvel enjeu est né pour les banques centrales africaines: la création de la Zone de Libre-Échange Continentale Africaine (ZLECAf) qui est entrée dans sa phase opérationnelle en janvier 2021. En effet, le commerce en Afrique reste confronté à de nombreuses barrières tarifaires et non tarifaires, parmi lesquelles se trouve bien évidemment l'infrastructure financière.

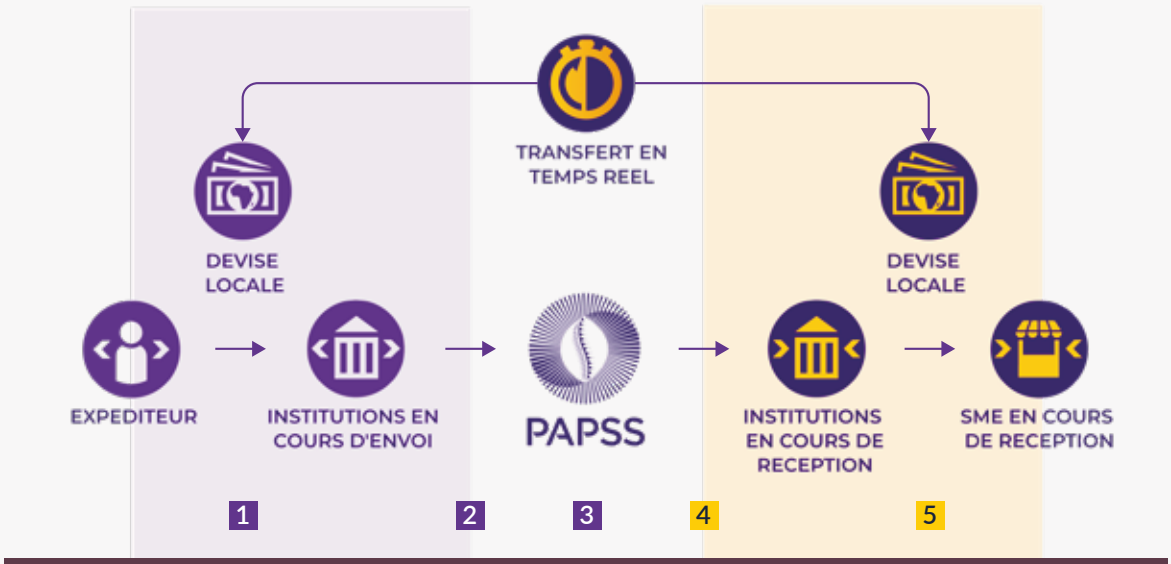
Les entreprises africaines sont confrontées à des coûts d'importation et d'exportation élevés, ainsi qu'à des retards liés au manque de relations directes entre les banques continentales et au manque de disponibilité en devises étrangères. Plus de 80 % des transactions transfrontalières effectuées entre des banques africaines sont compensées et réglées à l'étranger. Cela crée des inefficacités et augmente le coût des paiements transfrontaliers africains.

*12 Danièle Guinot, "Les banques françaises se replient du continent africain", Le Figaro, 9 juin 2023. - Geoff Lyatse, "In search of Africa's financial system sovereignty", The Guardian, 3 avril 2023 . - "Africa Payments: Insights into African transaction flows", SWIFT, 2018, 40 pages.*

# 1 PANORAMA DU SECTEUR BANCAIRE AFRICAIN

Voilà pourquoi, le Système de Paiement et de Règlement Panafricain (PAPSS) a été créé par l'Union Africaine, le Secrétariat de la Zone de libre-échange continentale africaine (ZLECAf), la Banque Africaine d'Import-Export (AfreximBank) et un groupe de banques centrales africaines. Ces dernières ont mis leurs ressources en commun pour créer une infrastructure centralisée de paiement et de règlement, à laquelle les banques commerciales africaines, les prestataires de services de paiement et les fintechs peuvent se joindre en tant que participants.

**FIGURE 5 -** COMMENT FONCTIONNENT LES PAIEMENTS INSTANTANÉS




1 Un donneur d'ordre émet un ordre de paiement dans sa devise locale auprès de sa banque ou de son prestataire de services de paiement.
2 L'ordre de paiement est envoyé au PAPSS.
3 Le PAPSS effectue tous les contrôles de validation nécessaires sur l'ordre de paiement.
4 L'ordre de paiement est transmis à la banque ou au prestataire de services de paiement du bénéficiaire.
5 La banque du bénéficiaire libère les fonds au bénéficiaire dans sa devise locale.

*Source : Site du PAPSS - https://papss.com/fr/comment-ca-fonctionne/*

Lancé en janvier 2022, le PAPSS sert de plateforme continentale pour régler de manière quasi-instantanée - 120 secondes - les paiements transfrontaliers en monnaie locale. Les usagers n'ont plus besoin de convertir les monnaies locales en devises de référence (dollar, euro ou livre sterling). Le système facilite ainsi les transactions transfrontalières entre les pays africains membres de la ZLECAf, tout en réduisant la dépendance à l'égard des devises étrangères.

Comme l'interconnexion des réseaux financiers à l'échelle continentale accroît le risque cyber, les responsables du PAPSS ont mis un accent spécial sur la cybersécurité. La plateforme a été certifiée ISO 27001 en septembre 2022 et quatre mois plus tard, ISO/IEC 27701:2019. Cette double certification démontre le sérieux des dirigeants du PAPSS en matière de de sécurité des données et de protection de la vie privée.

Sur la scène extérieure, le PAPPS a conclu en avril 2022 un protocole d'accord avec BUNA, le système de paiement transfrontalier et multidevises appartenant au Fonds monétaire arabe (FMA). À terme, cette collaboration devrait favoriser une meilleure intégration commerciale de la région du Moyen-Orient et de l'Afrique.[13] Le secrétariat du PAPSS est basé au Caire.

*13 Alain Kiyindou, "Numérique et technologies financières en Afrique", Agence française de développement éd., L'économie africaine 2023. La Découverte, 2023, pp. 95-108. - Aboubacar Fall, "Le système panafricain de paiement et de règlement (PAPSS)", Financial Afrik, 22 novembre 2022. - Richie Santosdiaz, "Overview of The Pan-African Payment and Settlement System PAPSS", The Fintech Times, 25 juin 2022.*

## 1.7 - La recherche en cybersécurité financière

Le problème numéro un de la cybersécurité en Afrique est le manque de ressources humaines qualifiées. Une étude qui date déjà de plusieurs années évaluait à 10 000 le nombre de professionnels certifiés cybersécurité sur l'ensemble du continent, alors qu'il en faudrait quatre fois plus.[14] Pourtant, le secteur éducatif s'est emparé de l'enjeu de longue date et des institutions sont créées chaque année pour pallier cette carence.

Parmi les universités de pointe en matière de cybersécurité, il faut accorder une place spéciale à Carnegie Mellon University Africa qui est un centre d'excellence régional spécialisé dans les TIC. Basée à Kigali, CMU-Africa a été créée en 2011 par la célèbre université américaine qui, avec 20 lauréats du prix Nobel et surtout 13 lauréats du prix Turing parmi ses enseignants ou anciens élèves, est un des leaders mondiaux de la recherche informatique.

CMU-Africa a lancé l'initiative CyLab-Africa en octobre 2022. Ce laboratoire vise à améliorer la cybersécurité des systèmes financiers en Afrique. Plus précisément, il évalue le paysage de la cybersécurité parmi les opérateurs de fintechs et leurs utilisateurs à l'échelle du continent. À cet effet, le laboratoire effectue des enquêtes auprès des opérateurs de fintechs afin de mieux comprendre leur niveau de préparation ainsi que d'investissements en matière de cybersécurité. L'équipe de CyLab-Africa effectue aussi des tests contrôlés d'intrusion dans l'infrastructure informatique des organisations.

**14** *"Africa Cybersecurity Report", Serianu, 2017, 86 pages. Cf. p. 11.*

# 2

# LES GRANDS ENJEUX DU SECTEUR BANCAIRE AFRICAIN

La banque africaine s'inscrit dans un tissu serré de tendances internationales. En effet, le secteur financier est entré dans une période de transformations profondes partout sur le globe. L'Afrique participe pleinement au mouvement et, pour des raisons qui lui sont propres, a commencé comme nous l'avons vu, par miser sur l'argent mobile, ce qui l'expose à certains risques qui lui sont spécifiques.

# 2 LES GRANDS ENJEUX DU SECTEUR BANCAIRE AFRICAIN

## 2.1 - Numérisation du secteur bancaire

Partout dans le monde, le secteur bancaire connaît une mutation radicale. Les banques se livrent une course effrénée pour offrir leurs services en ligne – pas quelques services : tous les produits financiers sont concernés. La tendance est irréversible car la technologie le permet et que le client l'exige : il ne veut pas se déplacer, parfois loin de chez lui, pour faire la queue. Il veut avoir une vue globale de ses actifs financiers instantanément, où qu'il se trouve et, surtout, faire des transactions en ligne.

La banque d'aujourd'hui ressemble de plus en plus à une firme de technologie de l'information. La convergence est si forte que les institutions financières se retrouvent en concurrence avec des nouveaux venus en provenance directe du monde des TI.

> Nous voulons créer la banque 100% numérique. Voilà pourquoi, nous avons priorisé le commerce électronique et la cybersécurité. Il nous faut seulement dégager des budgets suffisants.
>
> Gestionnaire de banque, Tunisie, 2019

## 2.2 - Naissance des néobanques

C'est ainsi qu'au début des années 2000, surviennent les néobanques qui misent sur le numérique et la téléphonie mobile pour réinventer les services financiers et faciliter la vie des clients via une offre simplifiée. Elles réduisent drastiquement les frais bancaires en renonçant à exploiter un réseau d'agences classiques. Il n'y a pas de modèle unique de néobanque. Certaines sont des établissements 100% numériques, d'autres sont des filiales de banques étrangères, d'autres encore sont des extensions d'un réseau de télécommunications. Il faut enfin compter avec les GAFA qui touchent désormais tous les domaines d'activités y compris les services financiers.

L'essor des néobanques en Afrique a été quelque peu freiné par la présence de l'argent mobile en tant que moyen privilégié d'effectuer des opérations bancaires sur le continent. Toutefois, alors que l'argent mobile est principalement axé sur les paiements et les transferts d'argent, les néobanques offrent toute la gamme des services bancaires en ligne, ainsi que des cartes de crédit et de débit prépayées. Les néobanques permettent aussi d'effectuer des transferts d'argent internationaux à des taux de change compétitifs et elles proposent des services d'investissement dans les cryptomonnaies.

Examinons quelques exemples de néobanques qui ont connu un certain succès sur le marché africain. Parmi les principales néobanques qui ont fait leur apparition à l'échelle continentale, la sud-africaine **TymeBank** vient en tête avec 123 millions USD de financement, suivie par **Kuda** au Nigéria avec 92 millions USD. Les deux néobanques dominent cet espace en tant que pionniers de la fintech sous licence, avec respectivement plus de six millions et cinq millions d'utilisateurs :

- **TymeBank** vient de passer le cap des six millions de clients au début de l'année grâce à l'introduction de services centrés sur le client, de nouveaux produits d'avance sur salaire et d'une nouvelle plateforme bancaire virtuelle aux Philippines, GOTyme, en collaboration avec le groupe philippin Gokongwei.
- **Kuda** est unique parmi les néobanques car elle déploie ses services en bénéficiant de sa propre licence bancaire. Avec le lancement récent de son produit et l'obtention d'un financement de 55 millions USD, la banque est en pleine progression et, contrairement à la majorité des néobanques, dès ses premiers pas, elle se peut se lancer dans le crédit par le biais d'une autorisation de découvert.[15]

Parmi les autres noms significatifs, mentionnons certaines entreprises prometteuses :

- **Lemonade Finance** qui a été créée en 2020 pour permettre aux diasporas africaines d'envoyer des fonds dans leur pays d'origine. La start-up nigériane, qui revendique plus de 100 000 utilisateurs, leur propose de conserver leur solde dans les devises qui leur conviennent, en les convertissant facilement de l'une à l'autre.
- **Payday**, une néobanque rwandaise qui a levé 3 millions de dollars dans le cadre d'un tour d'investissement d'amorçage en 2021 et a depuis reçu un appui financier international dans le cadre du programme Techstars (bureau de Toronto).[16]
- Enfin, il faut citer la principale néobanque francophone créée en 2020 en Côte d'Ivoire sous le nom de **Djamo** qui revendique actuellement 500 000 clients. La firme cible l'élite ivoirienne digitalisée et a levé 14 millions de dollars – le tour de table le plus important de Côte d'Ivoire – pour étendre ses services en Afrique francophone.[17]

---

***15*** *Tage Kene-Okafor, "Kuda takes digital banking play to the UK with its remittance product", Tech Crunch, 9 novembre 2022. - Londiwe Buthelezi, "TymeBank is now signing up over 200 000 customers a month accreditation", News 24, 9 décembre 2022. - Kshitija Kaur, "African Neobanking: A Stellar And Steady Rise", Whitesight, 21 septembre 2021.*
***16*** *Tage Kene-Okafor, "Payday wants to power the future of work for Africa with $3M seed led by Moniepoint", Tech Crunch, 29 mars 2023.*
***17*** *Antonin Gouze et Quentin Velluet, "Néobanques, mobile money… Les futurs leaders africains de la fintech", Jeune Afrique, 27 avril 2023.*

> Les banques numériques ont de plus en plus d'importance systémique sur leurs marchés locaux. Également désignées sous le nom de néobanques, elles sont plus exposées que leurs homologues traditionnelles…
>
> Antonio Garcia Pascual, Fabio Natalucci, Blogue FMI, 2022

## 2.3 - La déferlante des fintechs

À partir des années 2010 survient un autre phénomène : les fintechs – contraction de « finance » et de « technologie ». Comme les néobanques dont elles sont souvent les pourvoyeuses, les fintechs exploitent des canaux non traditionnels comme les smartphones et les technologies mobiles en général. Elles offrent une grande simplicité de gestion des comptes bancaires, une utilisation plus conviviale et des tarifs plus attrayants.

Toutefois, à la différence des néobanques qui sont des banques entièrement en ligne, les fintechs sont des entreprises technologiques qui proposent des solutions financières innovantes ponctuelles - un service ou une fonction unique. Les fintechs commercialisent parfois directement leurs services ou par le truchement des banques (leur offre est alors intégrée à celle de la banque). On estime que plus de 79% des institutions financières ont déjà noué des partenariats avec les fintechs ou envisagent de le faire.[18]

> Dans le secteur bancaire, les fintechs bouleversent les services financiers de base et poussent les banques à innover pour ne pas se laisser distancer. Pour les consommateurs, elles ouvrent la possibilité d'un accès plus large à de meilleurs services. Cette évolution fait monter les enjeux pour les organismes de réglementation et de contrôle.
>
> Antonio Garcia Pascual, Fabio Natalucci, Blogue FMI, 2022

Il y avait au début de l'année 2022, plus de 1000 fintechs actives en Afrique, contre 450 deux ans plus tôt. La grande majorité sont des entreprises africaines (80%) mais leur répartition demeure très inégale. Quatre pays ( Nigéria, Afrique du Sud, Kenya, Égypte) regroupent 70 % des fintechs africaines.[19] L'Afrique du Sud occupe une place prépondérante dans ce marché, mais la croissance la plus forte se situe en Afrique de l'Ouest. Pas moins de six fintechs africaines sont déjà valorisées à plus d'un milliard USD, méritant ainsi l'appellation d'unicornes: Interswitch (Nigéria), Flutterwave (Nigéria), Wave (Sénégal), OPay (Nigéria), Chipper Cash (Ouganda-Ghana) et MNT-Halan (Égypte).[20]

Dès le début, les fintechs africaines ont utilisé la plateforme du téléphone mobile pour prolonger et faciliter les paiements en ligne (y compris les transferts de fonds des travailleurs émigrés). Aujourd'hui, les paiements en ligne occupent 45 % des transactions et 24 % du capital-risque total des fintechs.[21] Les revenus des paiements mobiles qui s'élèvent à 3,5 milliards USD en 2020 et les observateurs estiment que ces montants pourraient être multipliés par quatre ou même cinq d'ici 2025.[22]

Qui plus est, les fintechs africaines diversifient leurs services. Elles font exploser le cadre restrictif du paiement en ligne pour étendre leur offre aux prêts et aux assurances. Il s'agit généralement de services très ciblés comme le crowdfunding, le microcrédit et le prêt interpersonnel ou encore la liquidité B2B, la cybersécurité et les technologies réglementaires : lutte contre le blanchiment d'argent (AML) ou la conformité à la connaissance du client (KYC), etc.[23]

Un autre champ d'application aux activités des fintechs est la gestion du risque. En effet, les banques africaines ont un des plus hauts taux de risque au monde. L'emblématique fintech sud-africaine JUMO a mis au point un système d'agrégation des données au moyen d'algorithmes spécialisés qui permet à sa clientèle d'emprunter de petits montants en temps réel tout en abaissant le taux de défaut de paiement. Des institutions internationales comme Goldman Sachs, Visa et Fidelity travaillent désormais avec JUMO pour améliorer leurs services de prêts[24].

---

***18*** *"Baromètre de l'industrie financière africaine", Deloitte, avril 2023, 59 pages. Cf. p. 39.*
***19*** *"La finance en Afrique : naviguer en eaux troubles", Banque européenne d'investissement, 2022, 148 pages. Cf. p. 99. "FinTechs in Sub-Saharan Africa", Ernst and Young (EY), 2019, 21 pages.*
***20*** *Chipper Cash a été fondé par un Ougandais et un Ghanéen et son marché est africain, mais son siège social est en Californie. "Fintech in Africa: The end of the beginning", McKinsey & Company, août 2022, 46 pages. Cf. pp. 3 et 14. - "Six out of seven African unicorns are fintechs", Fintech Pad, 22 février 2023.*
***21*** *"Blueprint for e-Payments for the Facilitation of Digital Trade across Africa", Smart Africa, 2020.*
***22*** *Alain Kiyindou, « VI / Numérique et technologies financières en Afrique », Agence française de développement éd., L'économie africaine 2023. La Découverte, 2023, pp. 95-108. - "Fintech in Africa: The end of the beginning", McKinsey & Company, 30 août 2022, 47 pages.*
***23*** *"La finance en Afrique", idem, p. 100, "Fintech in Africa", idem, p. 18.*
***24*** *David Whitehouse, "Goldman Sachs-backed fintech Jumo set to expand in Cameroon, Nigeria, Benin", The African Report, 12 décembre 2022. - "Roaring to life: Growth and innovation in African retail banking", McKinsey & Company, 2018, 54 pages. Cf. p. 4.*

# 2 LES GRANDS ENJEUX DU SECTEUR BANCAIRE AFRICAIN

À la faveur de la gestion du risque, les fintechs débordent même du monde bancaire et se glissent peu à peu dans celui de l'assurance où elles mettent au point des offres très concrètes, en prise directe avec les préoccupations de leurs clientèles comme une couverture sur la récolte ou sur les frais funéraires. On parle désormais d'insurtechs et celles-ci sont maintenant actives dans des domaines aussi variés que la santé ou l'emploi.[25]

## 2.4 - Popularité des solutions infonuagiques

Les services infonuagiques peuvent être offerts par les GAFAM ou encore des fintechs. En effet, la plupart des applications mises au point par des fintechs sont hébergées dans le nuage. D'une manière comme de l'autre, cela signifie que les données les plus sensibles des banques résident de plus en plus au-dehors de leurs réseaux internes, ce qui pose des problèmes de souveraineté numérique. En effet, la plupart des grands opérateurs de services infonuagiques sont américains. Or, en mars 2018, le Congrès américain a adopté le CLOUD Act qui permet expressément au Département de la Justice d'avoir accès aux données des opérateurs de cloud, quel que soit l'endroit où les serveurs infonuagiques sont situés.[26]

**Qu'est-ce que le nuage ?**

**Le cloud, pour être plus précis, consiste à externaliser son infrastructure informatique dans un nuage, en profitant de la mutualisation d'infrastructures tierces tout en cloisonnant son système d'information. Les leaders en la matière sont outre-Atlantique : Azure de Microsoft, AWS d'Amazon, GCP de Google ou Bluemix pour IBM.**

"La cyber-résilience dans le secteur bancaire de demain",
École de guerre économique (EGE), février 2023.

Face à la menace que font peser les États-Unis sur la confidentialité et la sécurité des données, pas moins de 25 pays africains ont adopté des lois qui interdisent ou limitent l'usage des services infonuagiques. L'interdiction consiste le plus souvent à exiger que les données soient stockées localement et porte uniquement sur les transferts transfrontaliers, sauf autorisation ponctuelle des autorités de régulation. Quinze pays sont dans ce cas. Il est plus difficile de trouver une ligne directrice chez les pays qui limitent l'accès au nuage. Chacun utilise une approche différente: législation sur la protection des données personnelles, les services financiers, la cybersécurité ou encore les télécommunications.[27]

Malgré ces obstacles, les banques africaines recourent de plus en plus aux services infonuagiques. En effet, c'est un moyen élégant d'automatiser les processus internes et d'offrir de nouveaux services tout en minimisant les coûts de développement et d'exploitation. En outre, le recours au nuage est une réponse à la pénurie chronique de main-d'œuvre qualifiée en informatique et en cybersécurité. Enfin, durant la crise du Covid-19, le nuage a permis d'offrir des solutions de télétravail au pied levé.

Cette transition infonuagique supprime certaines vulnérabilités informatiques, en particulier sur les infrastructures du réseau interne. Par contre, il en crée de nouvelles. Ainsi, une panne prolongée chez un grand opérateur de services en nuage engendrerait un problème immédiat pour les institutions financières. Non seulement l'accès à leur services en ligne serait compromis, mais l'ensemble de leurs opérations serait perturbé, avec tout ce que cela signifie en termes d'image pour la banque et de perte de confiance.

L'autre grande vulnérabilité est le changement de paradigme de la cybercriminalité qui privilégie de plus en plus les utilisateurs finaux, leurs appareils mobiles et leurs identités, en s'appuyant généralement sur des techniques d'ingénierie sociale comme l'hameçonnage (phishing).

***25*** *Brian Yu, "Forget about Mobile Money, Invest in Insurtech Instead: The Untapped Triple Bottom Line Opportunity in Nigeria", NextBillion, 14 avril 2023.*
*"Fintech in Sub-Saharan African Countries", Fonds monétaire international (FMI), 2019, 51 pages. Cf. pp. 10-1.*
*"Disrupting Africa: Riding the wave of the digital revolution", PwC, 2016, 53 pages. Cf. p. 15.*
***26*** *Dataprotect prépare une étude en profondeur sur les questions de souveraineté numérique en Afrique*
***27*** *Pays qui interdisent l'accès au nuage: Algérie, Angola, Bénin, Burkina Faso, Cap-Vert, Côte d'Ivoire, Congo Brazzaville, Gabon, Guinée Conakry, Maroc, Madagascar, Maurice, Niger, Sao Tomé & Principe, Togo. Pays qui en limitent l'accès: Afrique du Sud, Cameroun, Éthiopie, Kenya, Nigéria, Ouganda, Rwanda, Tunisie, Zambie, Zimbabwe. "Which Way for Data Localisation in Africa", Collaboration on International ICT Policy for East and Southern Africa (CIPESA), novembre 2022.*

## 2.5 - La question de l'argent numérique

### • *Nature des cryptomonnaies*

Bons vieux carnets de chèques, cartes bancaires et argent mobile: il s'agit dans tous les cas de la représentation symbolique de la monnaie traditionnelle que nous utilisons tous les jours. Le chèque, la carte ou le paiement mobile tirent leur valeur du montant d'argent dont dispose l'utilisateur.

Avec les cryptomonnaies, on change de registre. Un jeton de bitcoin ou de toute autre cryptomonnaie a une valeur propre. Il ne renvoie à rien d'autre que sa propre valeur. La valeur du bitcoin n'est pas indexée sur le cours de l'or ni sur celle des devises classiques et elle n'est pas garantie par une banque centrale.

> **La cryptomonnaie (...) est une forme de monnaie qui existe sous forme numérique ou virtuelle et qui utilise la cryptographie pour sécuriser les transactions. Les cryptomonnaies n'ont pas d'autorité centrale d'émission ni de régulation, mais elles utilisent un système décentralisé pour enregistrer les transactions et émettre de nouvelles unités.**
>
> "Qu'est-ce que la cryptomonnaie et comment fonctionne-t-elle ?", Kaspersky, 2023.

Le grand inconvénient des cryptomonnaies est précisément cette absence de garantie ainsi que la décentralisation de leur gestion qui entraîne une volatilité extrême. Voilà pourquoi de nombreux économistes demeurent méfiants devant le phénomène. Deux chercheurs de l'Université John Hopkins vont même jusqu'à contester leur nature financière: "Contrairement à ce que nous disent les experts en marketing, la crypto-monnaie n'est ni de l'argent ni un véhicule financier. Il s'agit d'une simulation élaborée de la finance qui produit des gains et des pertes."[28]

> **Ma très humble opinion est que les crypto-actifs ne valent rien. Ils ne sont basés sur rien, ils ne se rattachent à aucun actif sous-jacent qui pourrait apporter de la sécurité.**
>
> Christine Lagarde, présidente de la Banque centrale européenne, 2022[29]

Il existe, en outre, des obstacles typiquement africains, en premier lieu celui des infrastructures: perte d'accès à Internet et coupures de courant. Cela a imposé aux opérateurs de cryptomonnaie des investissements additionnels en infrastructures. En outre, plusieurs pays ont interdit purement et simplement l'usage de la cryptomonnaie: Algérie, Égypte, Libye, Maroc, Namibie, Nigéria, Zambie et Zimbabwe. D'autres en ont limité l'usage selon des modalités diverses.

### • *Intérêt de l'Afrique pour les cryptomonnaies*

Malgré ces inconvénients, le continent africain a rapidement vu l'intérêt des cryptomonnaies pour régler le problème des envois de fonds internationaux. Dans ses transferts, la diaspora africaine peut perdre jusqu'à 20% en frais d'intermédiaire - la Banque mondiale a calculé qu'il est plus coûteux d'envoyer des fonds en Afrique subsaharienne que dans n'importe quelle autre région du monde.

C'est ainsi que plusieurs plateformes de cryptomonnaies africaines de type bitcoin ont vu le jour: Kobocoin (Nigéria), Digital Shilling (Kenya), Safcoin (Afrique du Sud), Awehcash (Namibie), Dala (Ouganda), etc.[30] Ces cryptomonnaies africaines ont dû affronter les mêmes problèmes de volatilité des marchés que leurs consoeurs du monde industriel.

Malgré toutes ces difficultés structurelles ou politiques, les cryptomonnaies sont relativement populaires en Afrique. La firme singapourienne Triple A estime qu'avec 38 millions de détenteurs de cryptomonnaies en 2023, l'Afrique arrive en troisième position dans le monde - derrière l'Asie et l'Amérique du Nord, mais devant l'Europe. Trois pays africains figurent parmi les 20 premiers utilisateurs de cryptomonnaies : Nigéria, Afrique du Sud et Éthiopie.[31] Encore faut-il préciser que la cryptomonnaie la plus utilisée en Afrique est de loin le bitcoin, non une plateforme locale.

*28 Steve Hanke et Matt Sekerke, cités in "Des économistes comparent les cryptomonnaies à la cocaïne", Investing.Com, 10 mars 2023.*
*29 Johanna Treeck, "Crypto assets are 'worth nothing,' says ECB's Christine Lagarde", Politico, 21 mai 2022.*
*30 Ines Aissani, "Les 8 meilleures cryptomonnaies africaines à découvrir", Zone bitcoin, 7 mars 2023.*
*31 "Global crypto adoption", Triple A, 5 avril 2023.*

# 2 LES GRANDS ENJEUX DU SECTEUR BANCAIRE AFRICAIN

## • *Du bitcoin au stablecoin*

Pour préserver la fluidité de la monnaie numérique tout en lui conférant une valeur réelle, il faut l'adosser à une devise généralement reconnue, l'étalon-or ou encore une matière première comme le pétrole. On parle alors de "stablecoin" pour insister sur le côté stable et fiable du nouveau type de monnaie.

C'est ce qu'a voulu faire Facebook en mai 2019 quand l'entreprise a annoncé le lancement de sa propre cryptomonnaie – la Libra. Brièvement rebaptisé Diem, le projet Libra a finalement été abandonné en janvier 2022 en raison des oppositions multiples qu'il a rencontrées tant dans le milieu financier qu'auprès des gouvernements et des défenseurs du respect de la vie privée.

## • *Naissance de la monnaie numérique de banque centrale*

Le grand mérite du projet avorté de Facebook aura été d'envoyer des ondes de choc un peu partout sur la terre. C'est ainsi qu'on a vu surgir une nouvelle métamorphose de la cryptomonnaie qui est la monnaie numérique de banque centrale (MNBC). Contrairement aux stablecoins qui sont indexés sur la valeur du dollar ou de toute autre devise reconnue, les MNBC ont vocation à être émises par les banques centrales elles-mêmes.

L'intérêt pour les MNBC s'est alors répandu comme un feu de paille si bien que le Fonds monétaire international estime qu'en 2022 près de 100 banques centrales conduisent un projet de MNBC. Sans surprise, la Chine, les États-Unis et, dans une moindre mesure, l'Union européenne, sont sur les rangs.[32]

Ici encore, l'Afrique est sur les rangs des cryptomonnaies d'État que sont les MNBC. Quinze pays ont lancé des projets en matière de MNBC. Il est vrai que la plupart en sont au stade des études préliminaires, mais il n'en reste pas moins que trois pays ont lancé des essais pilotes (Afrique du Sud, Ghana et Centrafrique) et un a même atteint la phase commerciale (Nigéria).[33]

## • *Le Nigeria ouvre la marche*

Le premier pays d'Afrique à s'engager dans l'adoption à la grandeur du pays d'une monnaie numérique de banque centrale (MNBC) est le Nigéria. Lancée en octobre 2021 par la Central Bank of Nigeria (CBN), l'eNaira est la troisième MNBC au monde derrière le Sand Dollar des Bahamas (octobre 2020) et le DCash des Caraïbes orientales (mars 2021).[34]

Pour distribuer l'eNaira, la banque centrale du Nigéria s'est associée aux établissements de dépôt. La CBN administre l'eNaira par le biais d'une plateforme basée sur la blockchain pour émettre et frapper la MNBC, tandis que les institutions financières créent un portefeuille de trésorerie eNaira pour suivre les mouvements de la monnaie numérique sur la plateforme.

Il existe deux types de portefeuilles: le Merchant Speed Wallet est réservé aux entreprises, tandis que le Speed Wallet de base est destiné aux consommateurs. Même les personnes qui n'ont pas de compte bancaire peuvent ouvrir un compte eNaira: il suffit de se prévaloir d'un numéro de téléphone mobile. Le système a été configuré pour servir principalement aux petits paiements de détail.

L'autre application visée par la CBN est le transfert de fonds transfrontaliers. À cette fin, l'eNaira a été conçu de façon à respecter l'interopérabilité internationale. L'eNaira pourrait donc permettre de réduire le coût des transferts de fonds transfrontières. Cette disposition vise deux objectifs: faciliter les envois d'argent de la diaspora ainsi que conférer un avantage concurrentiel aux échanges commerciaux des entreprises nigérianes.[35]

Disons tout de suite que les premiers résultats de l'eNaira sont décevants. Fin novembre 2022, le nombre de portefeuilles était inférieur à un million, ce qui représente moins d'un pour cent des titulaires de comptes bancaires au Nigéria. Même les consommateurs qui possèdent des portefeuilles eNaira ne les utilisent pas. En outre, seulement dix pour cent des commerçants équipés de terminaux de point de vente soutiennent la MNBC.[36]

---

***32*** *Andrew Stanley, "Les MNBC ont le vent en poupe", Fonds monétaire international, septembre 2022. - "Central bank digital currencies in Africa", Bank for International Settlements (BIS), novembre 2022, 22 pages. Cf. p. 4.*
***33*** *Zachary Kazzaz, "The Rise and Stall of CBDCs and Cryptocurrencies in Africa: What's Next?" AfricaNenda, 29 mars 2023.*
***34*** *La Banque centrale des Caraïbes orientales dessert huit États indépendants des Caraïbes, à savoir Antigua-et-Barbuda, Montserrat, le Commonwealth de Dominique, la Grenade, Saint-Kitts-et-Nevis, Sainte-Lucie, Saint-Vincent-et-les-Grenadines et Anguilla. "Here's a list of countries to officially launch digital currencies", Telangana Today, 10 décembre 2022.*
***35*** *"Central bank digital currencies in Africa", Bank for International Settlements (BIS), novembre 2022, 22 pages. Cf. p. 5.*
***36*** *"Nigeria talking to new CBDC eNaira providers", Ledger Insight, 21 février 2023.*

## • *Les essais pilotes d'Afrique du Sud et du Ghana*

Pendant ce temps, l'Afrique du Sud et le Ghana ont procédé à des projets pilotes (de gros et de détail, respectivement). L'Afrique du Sud a également participé au projet multidevises Dunbar (mCBDC) coordonné par le Centre d'innovation de la BRI. Ce projet réunit les banques centrales d'Australie, de Malaisie et d'Afrique du Sud qui utilisent une plateforme commune à plusieurs monnaies numériques.[37]

- **Le projet Khokha 2 en Afrique du Sud**. Dès janvier 2018, l'Afrique du Sud procédait à une démonstration de faisabilité d'un mécanisme électronique de gestion des paiements de gros basé sur la technologie du registre distribué (en anglais Distributed Ledger Technology) qui est une forme simplifiée de blockchain. Baptisé Khokha, le projet visait à accélérer le traitement des transferts de fonds. Pour mener à bien ce test d'une durée de 14 semaines, la South African Reserve Bank (SARB) avait créé une fintech au sein de sa propre structure. Forte de l'expérience acquise, la SARB testait en février 2022 une véritable MNBC toujours pour les paiements de gros. Pour le projet Khokha 2, l'unité interne de fintech de la banque centrale fut à nouveau mise à contribution ainsi que les firmes Accenture et Block Markets Africa (BMA) en tant que prestataires de services techniques, et Deloitte en tant que partenaire de soutien. Khokha 2 visait à émettre, compenser et régler des emprunts sur la technologie du registre distribué en utilisant deux options de règlement :
  - Une MNBC de gros comme équivalent de monnaie émise par la banque centrale,
  - Un jeton de règlement de gros comme forme de monnaie privée émise par les banques commerciales.

  Cette nouvelle démonstration de faisabilité visait à tester les paramètres technologiques et à vérifier les dispositions politiques, juridiques et réglementaires qui devront être mises en place pour commercialiser une MNBC. Khokha 2 comme Khokha 1 a fait l'objet d'un rapport détaillé qui passe pour un guide des meilleures pratiques en matière d'essai pilote de monnaie numérique.[38]

- **Le projet eCedi au Ghana.** La MNBC du Ghana est testée depuis septembre 2021 et comprend deux niveaux d'utilisation : avec une application de portefeuille numérique téléchargeable sur un téléphone mobile et gérée par une institution financière ou, pour les consommateurs non bancarisés, avec un portefeuille matériel physique tel qu'une carte à puce sans contact, qui peut être utilisée hors ligne. L'essai pilote est organisé par la Bank of Ghana (BoG) en partenariat avec le fournisseur allemand de solutions de paiement Giesecke+Devrient (G+D). Le remboursement de l'eCedi en devise nationale est possible à tout moment.[39]

## • *Le cas de la Centrafrique*

Toute autre situation en République centrafricaine. En avril 2022, ce pays a créé la surprise en adoptant le bitcoin comme monnaie légale, au côté du FCFA. C'était alors le deuxième pays au monde après le Salvador à adopter le bitcoin comme devise officielle et le tout premier du continent africain. Or, la République centrafricaine est un des pays les plus pauvres de la planète et se trouve complètement dépourvue des infrastructures de base.

Pourtant, en juillet 2022, le pays récidive et annonce la création d'une cryptomonnaie nationale, le Sango Coin. À l'origine, le Sango Coin avait pour mission d'attirer les investisseurs et de faciliter l'accès aux ressources naturelles du pays. Bangui avait déployé toute une gamme d'incitatifs pour attirer les investisseurs, allant jusqu'à accorder la nationalité centrafricaine à tout étranger achetant pour 60 000 dollars ou plus en Sango Coin - bloqués pendant cinq ans à titre de garantie.[40]

Cette approche hybride mêle l'utilisation du bitcoin, la création d'une MNBC et une campagne de promotion des investissements internationaux. L'opération était sûrement trop disparate pour réussir. Le bitcoin a perdu son statut de monnaie officielle en mars 2023, en raison de l'opposition décidée de la Banque des États de l'Afrique centrale (BEAC) et de la Communauté économique et monétaire en Afrique centrale (CEMAC). La seule monnaie légale en République centrafricaine demeure le FCFA. Quant aux investisseurs, on attend toujours qu'ils se manifestent et, à échéances régulières, le gouvernement est contraint d'annoncer un report de la cotation du Sango Coin.[41]

---

***37*** *"Project Dunbar multi-CBDC: can foreign banks access local CBDC?", Ledger Insights, 22 mars 2022.*
***38*** *Project Khokha, South African Reserve Bank (SARB), 2018, 79 pages. - Project Khokha 2, Intergovernmental Fintech Working Group (IFWG) et South African Reserve Bank (SARB), 2022, 58 pages.*
***39*** *Tom Phillips, "Bank of Ghana lays out core design principles for CBDC pilot", NFCW, 21 mars 2022.*
***40*** *"La Centrafrique lance le projet de sa propre cryptomonnaie et d'un crypto-hub", Le Figaro, 4 septembre 2022. - Brian Quarmby, "Le centre crypto Sango est opérationnel en République centrafricaine", Cointelegraph, 4 juillet 2022.*
***41*** *Ben Canton, "Sango Coin: son lancement en Centrafrique aura un léger retard", Journal du Coin, 4 avril 2023. - Stewart Muhindo, "Le bitcoin n'est plus une monnaie légale en République centrafricaine !" 25 mars 2023.*

# 3

# LE CYBERCRIME COMME CONTREPARTIE DE LA TRANSFORMATION DIGITALE

*La prochaine crise pourrait ne pas être due à un choc financier. Le coupable le plus probable est une cyberattaque qui perturbe les capacités des services financiers, en particulier les systèmes de paiement, dans le monde entier.*

*Harvard Business Review, 2018*[42]

Traditionnellement, la sécurité bancaire était synonyme de sécurité physique: vitres blindées, gardiens privés, coffres-forts, etc. Cette image est en train de s'estomper pour céder la place à des algorithmes d'identification des anomalies et de cryptographie. Le braqueur de banque a été remplacé par un cybercriminel en col blanc, parfois votre respectable voisin, mais souvent aussi un malfaiteur anonyme à l'autre extrémité de la planète.

> Il y a 30 ans, lorsqu'une banque souhaitait ouvrir une succursale dans un quartier à forte criminalité, elle déployait ponctuellement des agents de sécurité et installait une ou deux caméras pour protéger ses actifs. Aujourd'hui, alors que les services financiers sont mis en ligne les uns après les autres, c'est l'organisation dans son ensemble qui est soudain plongée dans un environnement très instable.
>
> Adam Evans, Banque Royale du Canada, 2019

42 *Paul Mee et Til Schuermann, "How a Cyber Attack Could Cause the Next Financial Crisis", Harvard Business Review, 14 septembre 2018.*

# 3 LE CYBERCRIME COMME CONTREPARTIE DE LA TRANSFORMATION DIGITALE

## 3.1 - La cybersécurité se transforme en cyber-résilience

Aujourd'hui, la cybersécurité déborde le cadre technologique de la défense du périmètre bancaire pour englober la bonne hygiène managériale de tout l'écosystème financier. Dans ce contexte, la Banque des règlements internationaux (BRI) définit la cyber-résilience comme la capacité d'une banque centrale à remplir sa mission en **anticipant** et en **s'adaptant** aux cyber-menaces et aux autres changements collatéraux de l'environnement technologique, tout en **résistant** au cyber-incidents et en se **relevant** rapidement de crises qui ne dépassent pas la limite opérationnelle de l'organisation.

**Définition de la cyber-résilience**

**La cyber-résilience est la capacité d'une organisation à continuer à remplir sa mission en anticipant et en s'adaptant aux cyber-menaces et à d'autres changements pertinents dans l'environnement, ainsi qu'en résistant, en réduisant et en se relevant rapidement des cyber-incidents.**

BRI, 2020[43]

À partir de cette définition de la cyber-résilience bancaire, la BRI tire trois conséquences :

- Tout d'abord, la notion de risque a changé. Les approches précédentes étaient axées sur la conformité aux normes ainsi que sur l'ajout continuel de nouvelles technologies. Désormais, on privilégie les contrôles ciblés sur des secteurs clés. Leur robustesse est régulièrement testée à l'aide d'attaques simulées à plusieurs niveaux et de grande envergure.

- Deuxièmement, la gestion de la cybersécurité est intégrée dans la structure de gestion des risques de l'entreprise. L'avantage de cette approche comprend une meilleure hiérarchisation des types de risques. Cela permet de mieux répartir les responsabilités entre les employés de première ligne chargés de gérer les risques cyber dans les processus d'affaires.

- Enfin, la cybersécurité évolue vers la cyber-résilience. On part désormais du principe que le risque zéro n'existe pas. En conséquence, l'accent est mis sur la capacité d'une organisation à anticiper et à résister aux attaques tout en poursuivant ses opérations critiques. D'où la priorité accordée à la gestion de crise.[44]

*43 "Annual report 2020-21", Bank for International Settlements (BIS), 219 pages. Cf. p. 87.*
*44 "Cyber risk in central banking", Bank for International Settlements (BIS), septembre 2022, 22 pages. Cf. p. 11.*

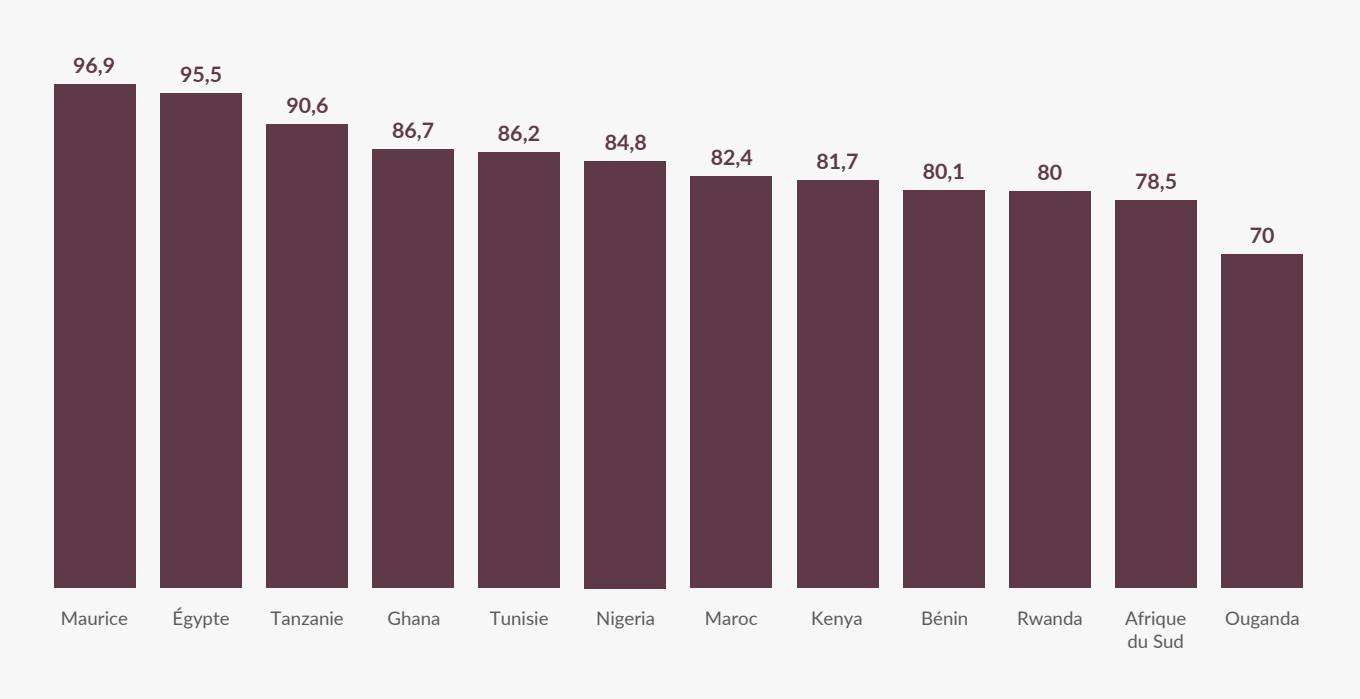
## 3.2 - La cybercriminalité en Afrique

### • *Benchmark de l'état de la cybercriminalité en Afrique*

Chaque deux ans, l'Union international des télécommunications (UIT) évalue la performance des pays en matière de cybersécurité en fonction d'une série d'indicateurs très fins, regroupés en cinq grands piliers: cadre juridique, mesures techniques, structure organisationnelle, renforcement des capacités, coopération. Selon l'évaluation de l'UIT, Maurice est le pays africain le plus performant et arrive au 17e rang mondial de l'index de la cybersécurité globale, il est suivi de l'Égypte (23e rang mondial) puis de la Tanzanie (37e rang mondial).

Dans les trois cas, l'État a servi de locomotive au développement de la cybersécurité : lancement d'un CERT-MU adossé à un projet de dépistage des botnets à Maurice ; création d'un EG-CERT en Égypte dès 2009 puis déploiement d'une stratégie de cybersécurité; création d'un TZ-CERT en Tanzanie dès 2010 suivie d'une législation bien ciblée (Loi sur la cybercriminalité et Loi sur les transactions électroniques, toutes deux en 2015). Ces trois pays encouragent et organisent la coordination entre toutes les entités régionales et nationales, tant privées que publiques, impliquées dans la gestion des incidents de cybersécurité. À bien des égards, ce sont des modèles.

**FIGURE 6 -** LES 12 PAYS AFRICAINS LES PLUS MÛRS EN CYBERSÉCURITÉ




*Source : UIT, Global Cybersecurity Index 2020.*

Aucun des champions africains ne se trouve dans le "Top Ten" mondial, ce qui est un recul relatif puisqu'en 2017, Maurice arrivait en sixième position de l'index global. C'est dire le chemin qui reste à faire. Notons que certains pays améliorent leur position au fil des évaluations de l'UIT, c'est le cas de la Tanzanie qui passe du 87e rang mondial en 2017 au 37e rang en 2020 ou du Ghana qui passe du 86e rang mondial au 43e au cours du même intervalle de temps. La performance la plus spectaculaire demeure celle du Bénin qui occupait le 148e rang mondial en 2017, ce qui en faisait une lanterne rouge de la cybersécurité, et qui fait un bond en avant pour se retrouver à la 56e place.

# 3 LE CYBERCRIME COMME CONTREPARTIE DE LA TRANSFORMATION DIGITALE

## • *Aperçu sur la cybercriminalité générale*

En Afrique, prévient INTERPOL, la plupart des activités malveillantes sont facilitées par des systèmes obsolètes ou encore des solutions de sécurité inefficaces qui laissent subsister des failles que les cybercriminels peuvent exploiter. De son côté, l'association mondiale Business Software Alliance (BSA) estime qu'en Afrique plus de 74% des logiciels sont piratés ou contrefaits (installation sans licence)[45]. Cela signifie que ces logiciels ne peuvent jamais être mis à jour et constituent autant de portes ouvertes pour les cybercriminels.

**FIGURE 7** - BILAN RÉCAPITULATIF DE LA CYBERMENACE

| 4,12 MM$ | 2,32 MM$ | 80% des logiciels | 80% des PC |
|---|---|---|---|
| Représente le coût annuel des cyberattaques pour les entreprises africaines | Constitue le marché annuel de la cybersécurité en Afrique | Africains sont piratés ou contrefaits (installés sans licence) | Africains sont infectés par des virus et autres logiciels malveillants |
| Estimation réalisée par l'entreprise de cybersécurité kényane Serianu, citée par INTERPOL (2021). | PwC Africa Annual Report (2022) | Global Software Survey 2018, Business Software Alliance (BSA), 2018. | Relever les défis juridiques de la Cybersécurité en Afrique, Union Africaine, Ouagadougou, octobre 2018 |

*Source : Dataprotect, 2019 (mis à jour 2023)*

De plus, l'absence ou l'insuffisance de réglementation et de législation en matière de cybercriminalité contribue aussi à l'augmentation des attaques par rançongiciel à l'échelle du continent. En l'absence de règles ou de lignes directrices claires sur la manière de se protéger contre de telles menaces, de nombreuses entreprises se retrouvent en état de vulnérabilité face aux cybercriminels.[46]

*45 "Global Software Survey 2018", Business Software Alliance (BSA), 2018, 20 pages. Cf. p. 11.*
*46 "African Cyberthreat Assessment Report: Cyberthreat Trends", INTERPOL, mars 2023, 31 pages. Cf. p. 20.*

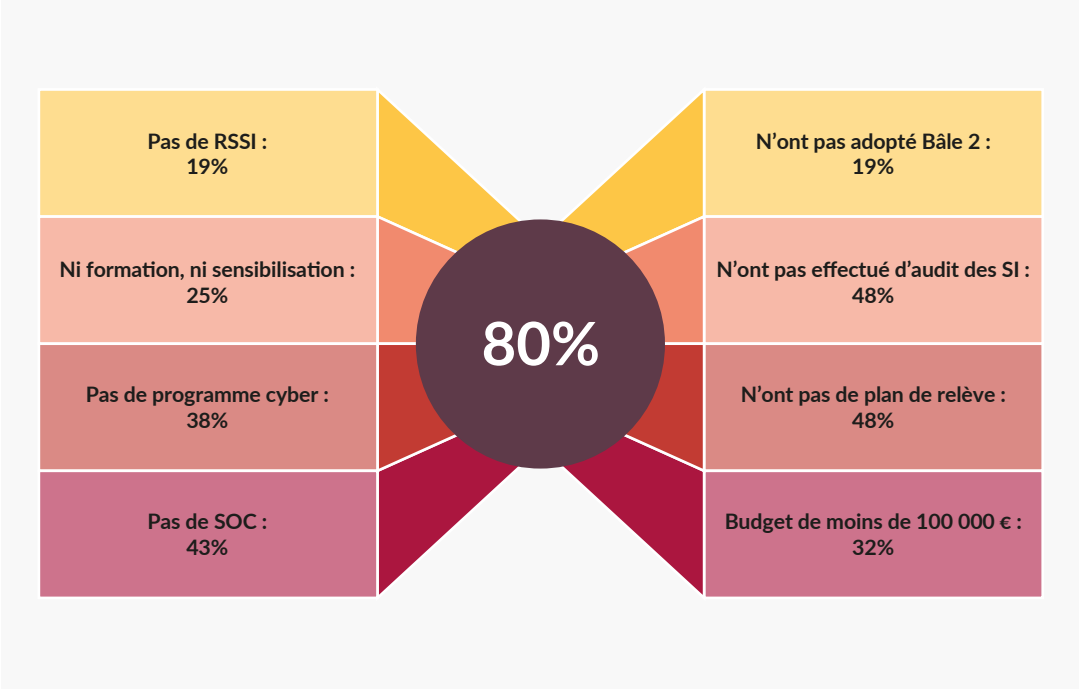
## • *Aperçu sur la cybercriminalité dans le secteur bancaire*

Dans son étude de 2019 sur la fraude bancaire, l'équipe Dataprotect/Sciencetech révélait que 85% des institutions financières d'Afrique de l'ouest et centrale avaient déjà été victimes d'une ou plusieurs cyberattaques – dans certains cas, il s'agit même d'attaques à répétition[47]. La question portait uniquement sur les cyberattaques ayant entraîné des dommages. Nul doute que l'ampleur du problème n'a pas dû s'améliorer depuis lors.

La raison de ce malheureux bilan était clairement démontrée. À peine 20% des banques africaines ayant participé à l'enquête affichaient un taux de cybersécurité relativement satisfaisant, c'est-à-dire qu'elles remplissaient huit conditions jugées comme fondamentales: nomination d'un RSSI, application des principes de Bâle 2, plan de formation ou de sensibilisation, audit régulier, programme de cybersécurité, recours à un SOC et budget annuel supérieur à 100 000 €[48]. Il ne suffit pas de répondre à quelques-uns de ces critères pour être sécuritaire : il faut répondre à tous.

Cela signifie que 80% des banques africaines étaient vulnérables aux cyberattaques. La plupart des banques sont donc incapables de parer aux attaques, elles opèrent les yeux fermés dans une zone à haut risque et, une fois frappées, elles subissent des dommages maximums.

**FIGURE 8 -** PROPORTION DES BANQUES À RISQUE EN AFRIQUE SUBSAHARIENNE




*Source : Étude Dataprotect, 2019.*

**47** *"La fraude bancaire en Afrique subsaharienne", Dataprotect, décembre 2019, 55 pages. Cf. p. 30.*
**48** *"La fraude bancaire en Afrique subsaharienne", idem, cf. p. 41.*

# 3 LE CYBERCRIME COMME CONTREPARTIE DE LA TRANSFORMATION DIGITALE

## 3.3 - Le coût de la cybercriminalité dans le secteur bancaire

Les banques sont conscientes de l'ampleur de la menace. Selon une enquête récente, plus de 74 % des banques africaines considèrent les risques liés à la cybersécurité comme le frein le plus courant à leur développement, et ce pour l'ensemble des régions. C'est leur plus grande préoccupation.[49] Cette crainte est d'autant plus justifiée qu'une cyberattaque dans une banque "coûte" plus cher que dans le reste de l'économie.

Alors que le coût moyen d'une intrusion dans le système d'information d'une entreprise est de 4,35 millions USD, il s'élève à 5,97 millions USD dans une institution financière. Il s'agit bien d'un coût moyen, car il n'y a pour ainsi dire pas de plafond aux pertes que peut encourir une banque sous attaque, comme le démontre l'exemple de la Banque du Bangladesh qui a perdu "seulement" 81 millions USD – mais elle avait failli en perdre un milliard (voir encadré).

À la suite de l'incident survenu au Bangladesh, le think-tank américain Carnegie Endowment for International Peace en coopération avec l'Institut SWIFT et le FMI a mis au point une boîte à outils à l'intention des institutions financières. Lancée en 2019, cette boîte à outils vise à renforcer la cyber-résilience des institutions financières en misant sur une série de mesures techniquement détaillées. Elle est disponible en sept langues dont le français et est accessible en ligne : https://carnegieendowment.org/specialprojects/fincyber/guides

L'importance de ces chiffres a poussé la Banque africaine de développement à accorder, en 2022, un don de deux millions USD pour créer le Centre africain de ressources sur la cybersécurité pour l'inclusion financière (ACRC). Cette nouvelle institution sera chargée d'apporter une réponse à la cybercriminalité et, plus généralement, à la résilience du système numérique africain. Le décaissement des fonds sera fait via la Facilité pour l'inclusion financière numérique en Afrique (ADFI).[51]

**Le vol « manqué » de la Banque du Bangladesh**

Au début de 2016, une organisation cybercriminelle a pénétré les systèmes de sécurité de la Banque du Bangladesh avec un logiciel malveillant qui clonait des transactions légitimes. On estime que l'organisation comptait entre 20 et 40 malfaiteurs aux compétences diverses, dont des experts financiers et bancaires, des pirates informatiques et des ingénieurs en logiciel. Le 4 février, le logiciel malveillant a ainsi expédié 35 demandes de retrait par l'intermédiaire de SWIFT à la Réserve fédérale de New York, où la banque centrale du Bangladesh avait des fonds en dépôt. Un montant de près d'un milliard de dollars américains (très exactement 951 millions) était en cours de transfert quand les cybercriminels ont joué de malchance. L'adresse d'une banque destinataire comportait le mot "Jupiter" qui est le nom d'un pétrolier et d'une compagnie maritime sanctionnée basée à Athènes, ce qui déclencha un examen plus approfondi. En raison des différences de fuseaux horaires, d'horaires de travail et en l'absence de canal de communication entre les deux banques, il a fallu quatre jours pour que l'alarme soit donnée. Trente ordres, d'une valeur de 850 millions de dollars, ont pu alors être bloqués par la Réserve fédérale de New York, mais les malfaiteurs avaient déjà réussi à faire transférer 101 millions de dollars vers des banques du Sri Lanka et des Philippines avant que leurs activités ne soient bloquées. Par la suite, 20 millions de dollars ont été récupérés dans une banque sri-lankaise, mais les 81 millions de dollars restants ont définitivement disparu. Sans le hasard d'une homonymie, cette audacieuse tentative de voler près d'un milliard de dollars aurait probablement réussi - une perspective qui a suscité une grande inquiétude parmi les banques et leurs clients institutionnels, qui conservent d'importantes sommes en dépôt pour payer leur personnel et leurs fournisseurs.

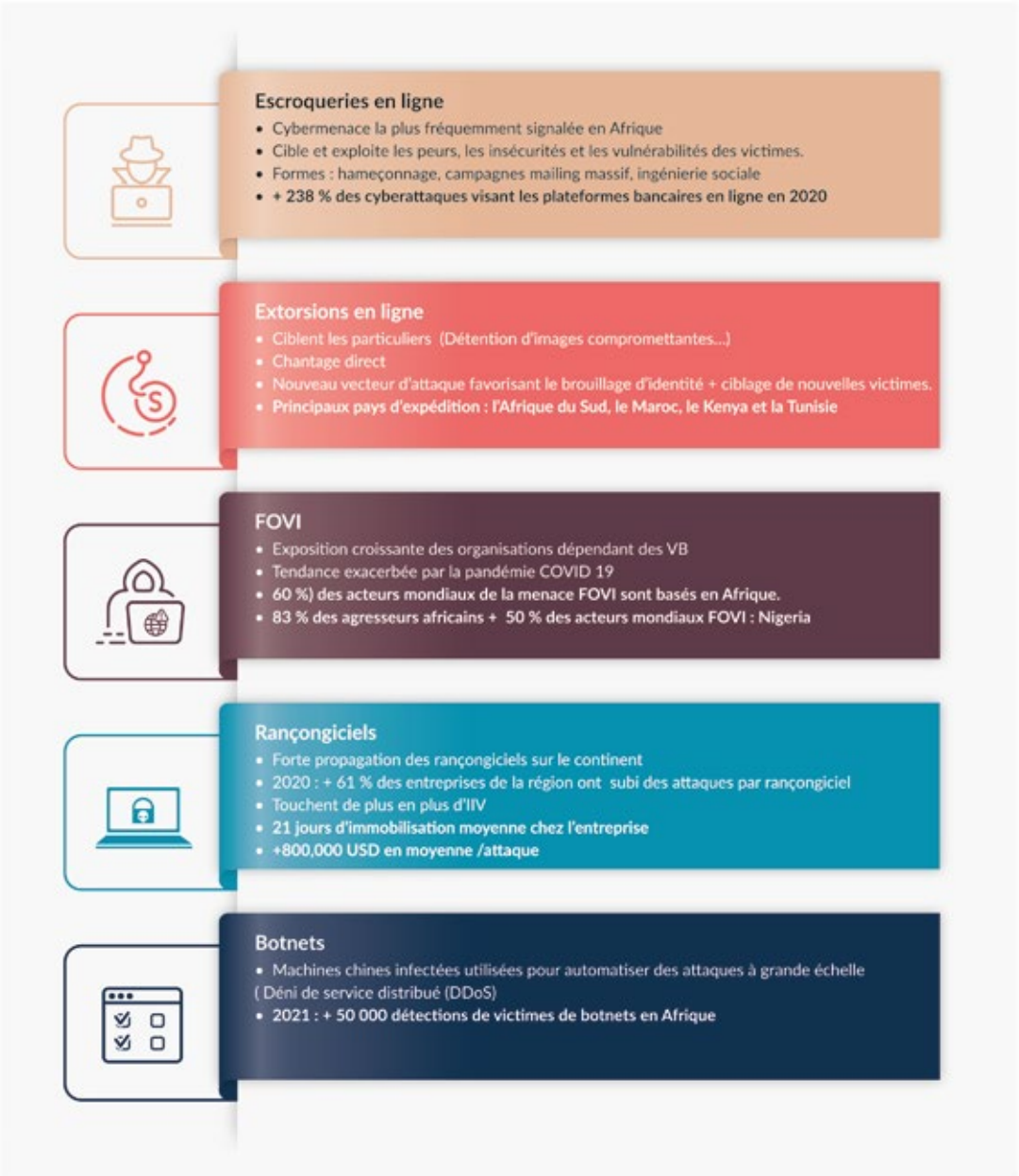
The Atlantic Council of the United States, 2022[50]

*49 "La finance en Afrique : naviguer en eaux troubles", Banque européenne d'investissement, 2022, 148 pages. Cf. p. 98. - "Baromètre de l'industrie financière africaine", Deloitte, avril 2023, 59 pages. Cf. p. 21.*
*50 "DigitalBankingFraud: Best Practice for Technology-Based Prevention", NetGuardians, 2021, 21 pages. Cf. p. 3. "Missing Key: The Challenge of Cybersecurity and Central Bank Digital Currency", The Atlantic Council of the United States, juin 2022, 49 pages. Cf. pp. 43-4.*
*51 En anglais: Africa Digital Financial Inclusion Facility (ADFI). - "Comment muscler la cybersécurité de la finance africaine?", 24 heures au Bénin, 21 avril 2022.*

## 3.4 - Les outils du cybercrime

L'expansion du périmètre numérique du secteur bancaire africain attire toute la gamme de la cybercriminalité au premier rang de laquelle se trouvent les escroqueries en ligne et l'hameçonnage (phishing) qui représentent une menace "élevée" ou "très élevée". Ce ne sont pas les seules comme l'indique le tableau ci-dessous.

**FIGURE 9 -** PRINCIPAUX TYPES D'OUTILS DU CYBERCRIME




*Source : Dataprotect, 2023*

# 3 LE CYBERCRIME COMME CONTREPARTIE DE LA TRANSFORMATION DIGITALE

## • *Les escroqueries en ligne et l'hameçonnage*

Les escroqueries en ligne englobent différents types de fraudes réalisées dans le cyberespace. Il s'agit aussi bien de l'usurpation d'identité, de l'escroquerie à l'avance de frais, de la fraude au paiement à distance que des sextorsions et des escroqueries aux cybermonnaies. Elles cherchent habituellement à exploiter les peurs, les insécurités ou les vulnérabilités des victimes en employant de multiples tactiques, techniques et procédures en ligne. Les escroqueries en ligne constituent une stratégie rentable pour les acteurs des menaces, car elles nécessitent un équipement technique minimal et présentent de faibles coûts de démarrage.[52]

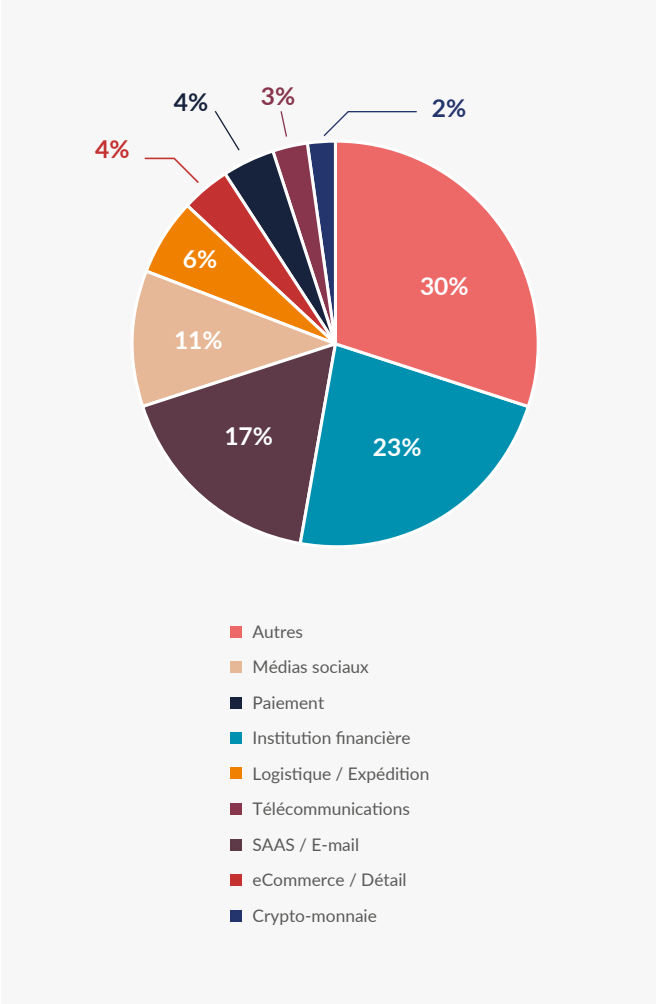
La plupart des escroqueries commencent avec une manœuvre d'hameçonnage exécutée par des acteurs malveillants exploitant leur compréhension des cultures locales. Or, l'hameçonnage est le premier vecteur de cyberattaques réussies en Afrique, nous révèle une étude réalisée par la firme américaine de formation et de sensibilisation KnowBe4[53]. De son côté, le rapport « Spam and Phishing » de Kaspersky évalue que 8,7% des internautes africains ont été victimes d'attaques par voie d'hameçonnage en 2022.[54]

> **Le phishing reste de loin le vecteur d'attaque initial le plus courant. Traditionnellement, les mails d'hameçonnage sont utilisés pour inciter l'utilisateur à exécuter une pièce jointe malveillante afin d'installer un logiciel malveillant qui prend le contrôle de l'appareil de l'utilisateur.**
>
> Banque des règlements internationaux, 2022

La simplicité technologique de l'hameçonnage ne doit pas nous amener à sous-estimer cette menace. C'est la porte d'entrée du cybercrime dans l'organisation et elle est d'autant plus difficile à contrer qu'elle exploite la nature humaine: inattention, fatigue, crédulité, etc. Mais elle vise toujours le même résultat: inciter la personne cible à divulguer une information confidentielle.

Selon le rapport effectué par INTERPOL portant sur l'évaluation des cybermenaces en 2023 en Afrique, les banques sont la principale cible de l'hameçonnage.[55] Or, une attaque par hameçonnage peut déboucher aussi bien sur une banale escroquerie en ligne que sur une opération de rançongiciel (ransomware) hypersophistiquée.

**FIGURE 10 -** IMPACT SECTORIEL DU HAMEÇONNAGE




*Source : INTERPOL, mars 2023.*

**52** *"African Cyberthreat Assessment Report: Cyberthreat Trends", INTERPOL, mars 2023, 31 pages. John Campbell, "Last Month, Over Half-a-Billion Africans Accessed the Internet, Campbell", Council on Foreign Relations, juillet 2019.*
**53** *"African Cybersecurity Research Report", KnowBe4, 2019, 8 pages. Cf. p. 4. Le sondage a été effectué auprès de plus de 800 personnes en Afrique du Sud, au Kenya, au Nigéria, au Ghana, en Égypte, au Maroc, à Maurice et au Botswana.*
**54** *Grace Ashiru, "Kaspersky Exposes Phishing Attack Trend in Africa", Tech In Africa, 23 mars 2023.*
**55** *"African Cyberthreat Assessment Report", idem, cf. p. 17.*

### • *Fraude au président*

Une forme avancée d'escroquerie en ligne appuyée sur de l'hameçonnage est la fraude au président où les cybercriminels usurpent une identité dans le but de tromper un employé et d'obtenir des informations confidentielles ou de l'argent. Le fraudeur se présente comme un des dirigeants de l'organisation ou toute autre figure d'autorité et sollicite l'employé afin qu'un virement soit effectué en urgence sur un compte bancaire, généralement domicilié à l'étranger, en vue de la réalisation d'une opération d'acquisition urgente et confidentielle.

Ce type de délinquance peut revêtir trois formes principales :

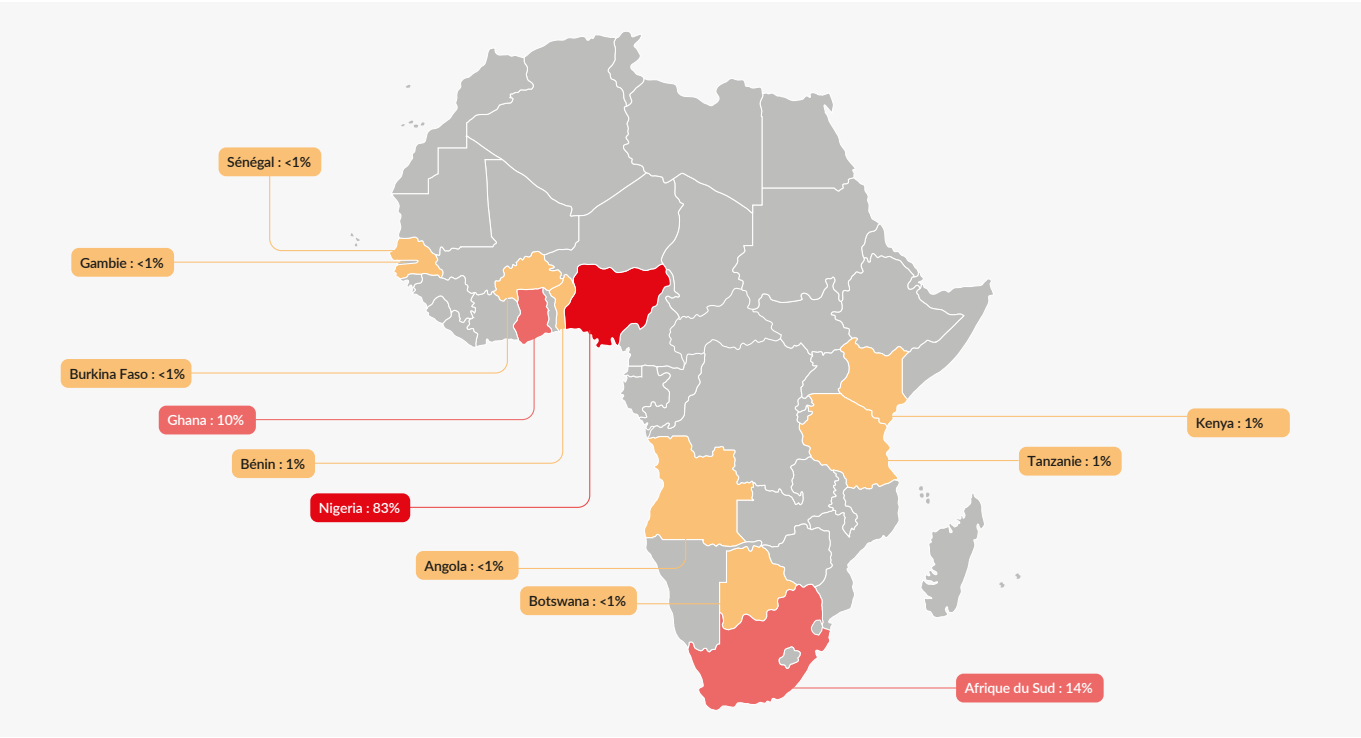
1. Fraude au président proprement dite : le cyber-escroc contacte un employé relevant d'un service où transitent de nombreuses transactions, comme la logistique du groupe ou la direction des opérations de change. Il lui demande d'effectuer en urgence un virement important à un tiers, pour obéir à un prétendu ordre du président ou tout autre membre de la haute direction.
2. Usurpation d'identité : même principe que précédemment, mais cette fois-ci le cyber-escroc se fait passer pour un employé d'un autre service, un fournisseur ou encore en mettant en place un faux affacturage. Il demande que les versements soient dirigés vers un compte bancaire le plus souvent situé dans une néobanque ou à l'étranger.
3. Variante informatique : Le cyber-escroc se fait passer pour l'éditeur du logiciel de trésorerie ou pour tout autre responsable informatique, afin de prendre le contrôle du poste informatique d'un employé et y effectuer des transactions irrégulières.[56]

Dans tous les cas, les escrocs collectent en amont de nombreux renseignements sur le fournisseur, sur la banque et sur leurs liens respectifs. Cette connaissance, associée à des éléments convaincants (ton persuasif au téléphone, utilisation des logos du fournisseur sur les mails, etc.), est la clé de la réussite de la fraude. Pour augmenter ses chances, le fraudeur met toujours son interlocuteur sous pression pour l'empêcher de réfléchir à la situation. Il mise sur l'urgence face à une situation inhabituelle et insiste sur le caractère confidentiel de l'opération.

**56** *Pour plus d'information : "Se prémunir contre les escroqueries aux faux ordres de virement", Collectivités locales, Fr. - https://www.collectivites-locales.gouv.fr/files/Finances%20locales/0.%20dépliants/2022/4_FOVI.pdf*
**57** *"The Geography of BEC", ACID (Agari Cyber Intelligence Division), 2022, 15 pages. Cf. p. 5.*

# 3 LE CYBERCRIME COMME CONTREPARTIE DE LA TRANSFORMATION DIGITALE

**FIGURE 11 -** CARTE DES ACTEURS AFRICAINS DE LA FRAUDE AU PRÉSIDENT




*Source : ACID, 2022.*

**Opérations de type coup de poing au Nigéria**

La fraude au président est appelée en anglais Business Email Compromise (BEC). Selon de récentes statistiques sur les cybercrimes, la fraude du président a permis de dérober plus de 26 milliards USD à des victimes peu méfiantes dans le monde entier. Face à la forte concentration d'acteurs BEC au Nigéria, INTERPOL-Afrique et les forces de police nigérianes (NPF), conjointement avec des acteurs du secteur privés, ont lancé en 2022 deux opérations nommées Delilah et Killer Bee. Ces actions de type coup de poing ont permis de démanteler certains des groupes de cybercriminels les plus actifs au Nigéria.

## • *Botnets et chevaux de Troie*

Un botnet est un ensemble d'ordinateurs connectés automatiquement sans que leurs propriétaires en soient conscients – le mot « botnet » est la contraction des termes « robot » et « network ». Voici comment se passe l'opération de détournement. Un groupe de cybercriminels utilise des chevaux de Troie (Trojans) spéciaux pour contaminer l'ordinateur cible. Un cheval de Troie est un type de logiciel malveillant déguisé en programme légitime et connu.

Dans le cas des botnet, le cheval de Troie infiltré dans l'ordinateur ne provoque aucun dommage et ne se manifeste en rien. On dit qu'il est dormant. Il attend une instruction du groupe de cybercriminels pour agir. L'ordinateur infecté ou zombie est seulement utilisé comme véhicule. Tout au plus son propriétaire notera un ralentissement ou un comportement erratique quand les cybercriminels l'utilisent.

Les ordinateurs zombies sont mis en réseau pour constituer un botnet qui va servir à effectuer des attaques sur des cibles distantes comme, à titre d'exemple, une attaque par dénis de service distribué (DDoS), une campagne de spam, une attaque de rançongiciels, etc. Le botnet n'est pas une fin en soi, c'est une composante de base pour garantir l'anonymat des malfaiteurs.

De nombreux cas médiatisés d'attaques DDoS contre des infrastructures essentielles ont eu lieu en Afrique ces dernières années. Ainsi, le botnet Mirai est devenu célèbre au milieu des années 2010 pour avoir servi à monter toute une série de cyberattaques dans le monde. On estime qu'au sommet de sa malfaisance, Mirai comptait 145 000 zombies (pas seulement des ordinateurs, mais aussi des caméras de surveillance) et avait une capacité de 623 Go/s.[58]

Ainsi, une attaque géante par déni de service (DDoS) menée en octobre 2019 en Afrique du Sud a dans un premier temps paralysé les services destinés au public de plusieurs institutions financières. Les cybercriminels ont ensuite exigé une rançon pour cesser les attaques, via un mail envoyé à des cadres, donc sans précaution pour préserver la confidentialité de l'opération. Aucun rançongiciel n'a été utilisé pour appuyer la demande de rançon. Deux des banques sous attaque, Standard Bank et Capitec, ont déclaré que les données de leurs clients n'avaient pas été compromises.[59]

Aujourd'hui, les descendants de Mirai font infiniment mieux. Le plus nocif est HinataBot qui a surgi en 2022 et peut déjà monter des cyberattaques à plusieurs téraoctets avec un réseau de quelques milliers de zombies seulement. La différence de puissance tient au langage de programmation Goland utilisé dans HinataBot qui est à la fois plus simple et plus puissant que les langages C ou C++ habituellement utilisés dans les logiciels malveillants (Mirai était écrit en C).[60]

***58*** *Nate Nelson, "Mirai Hackers Use Golang to Create a Bigger, Badder DDoS Botnet", Dark Reading, 20 mars 2023.*
***59*** *Grégoire Huvelin, "L'Afrique du Sud frappée de plein fouet par une double cyberattaque DDoS et ransomware", Numérama, 30 octobre 2019.*
***60*** *Nate Nelson, idem.*

# 3 LE CYBERCRIME COMME CONTREPARTIE DE LA TRANSFORMATION DIGITALE

## • *Rançongiciels*

Un rançongiciel (ransomware) est un logiciel malveillant qui bloque l'accès aux fichiers ou aux systèmes d'une organisation jusqu'à ce que celle-ci verse une somme d'argent aux cybercriminels. Il y a deux principaux types de rançongiciels :

- Le cryptorançongiciel (crypto ransomware) remplace les fichiers légitimes entreposés dans le système d'information de l'organisation par des données chiffrées;
- Le rançongiciel cryptoverrouilleur (locker ransomware) empêche les employés de se connecter à leur ordinateur ou téléphone mobile.[61]

La méthode d'attaque passe également par l'hameçonnage. Un mail invite la personne ciblée à cliquer sur un lien conduisant à un site non sécurisé ou à télécharger une pièce jointe qui contient un logiciel malveillant. Les banques encourent des risques importants en termes de réputation, car les données des clients peuvent être rendues publiques ou volées lors de ces incidents, compromettant ainsi leur crédibilité aux yeux du public.

Sans surprise, la Banque des règlements internationaux (BRI) place les attaques par rançongiciels au premier rang des menaces identifiées par les institutions financières des pays émergents (au même rang que les attaques par logiciels malveillants). En termes de coûts également, les attaques de rançongiciels sont celles qui engendrent le plus de pertes.[62]

**Une menace omniprésente**

**INTERPOL estime qu'en Afrique, plus de 61% des entreprises auraient déjà subi des attaques par rançongiciel et la tendance n'est pas prête de disparaître.**

Évaluation des cybermenaces en Afrique", INTERPOL[63]

La principale victime est l'Afrique du Sud suivie de loin par le Maroc. Chaque attaque occasionne un temps d'immobilisation moyen de 21 jours chez l'entreprise qui en est victime. Bien que les entreprises prétendent toujours ne pas payer de rançon, INTERPOL estime que les sommes moyennes versées atteignent désormais plus de 800 000 USD par attaque.[64]

Il s'agit d'une moyenne car, en pratique, les sommes exigées n'ont pas de limite.

## • *RaaS*

Les premiers logiciels malveillants nécessitaient une certaine expertise. Aujourd'hui, le principal danger provient des plateformes de cybercriminalité sur demande. Une quantité de programmes malveillants et de données personnelles (documents d'identité complets, numéros de comptes, mots de passe, etc.) se trouvent en vente libre sur le web invisible (darkweb).

Des outils entièrement préprogrammés sont proposés avec le mode d'emploi, ce qui permet à des malfaiteurs ignorants en informatique de monter des cyberattaques aussi dévastatrices que celles de hackers professionnels. La dernière évolution en date est le développement du Ransomware as a Service (RaaS), qui permet aux cybercriminels de louer à l'heure ou à la journée des versions prédéveloppées de rançongiciel qu'ils peuvent utiliser pour mener leurs attaques.

Avec la disponibilité du RaaS, il est plus facile que jamais de mettre en œuvre des attaques de rançongiciel réussies et les attaquants n'ont plus besoin d'avoir des compétences techniques et une expérience avancée. En outre, les attaquants peuvent rapidement passer d'une version de rançongiciel à l'autre.[65]

*61 "Rançongiciels : comment les prévenir et s'en remettre", Centre canadien pour la cybersécurité, septembre 2021.*
*62 Cyber risk in central banking", BIS Working Papers, septembre 2022, 22 pages. Cf. p. 2 et pp. 11-12.*
*63 Évaluation des cybermenaces en Afrique", INTERPOL, 2021, 34 pages. Cf. p. 7.*
*64 "African Cyberthreat Assessment Report: Cyberthreat Trends", INTERPOL, mars 2023, 31 pages. Cf. p. 19.*
*65 "African Cyberthreat Assessment Report: Cyberthreat Trends", INTERPOL, mars 2023, 31 pages. Cf. p. 21.*

## 3.5 - La menace s'étend à la périphérie du secteur bancaire

Si les banques sont visées et parfois victimes, la nature du risque est relativement bien connue. Il en va tout autrement lorsqu'on gagne la périphérie du secteur bancaire. À la fine pointe de l'innovation, les fintechs explorent des technologies nouvelles, ce qui crée inévitablement des vulnérabilités insoupçonnées. De même, l'adoption croissante du nuage (cloud) par les banques pose des défis supplémentaires en termes de risque cyber et de réglementation.

En parallèle, la mode des cryptomonnaies et de la finance décentralisée en général ont présidé à la création tout un écosystème dans lequel n'importe qui peut agir en qualité d'échangeur, de prêteur ou de fournisseur de liquidités. Enfin, les MNBC remplaceront les innombrables transactions monétaires que nous effectuons tous les jours par des transactions virtuelles, ce qui ne saurait manquer d'accroître encore le périmètre d'attaque des cybercriminels.

### • *Le cas de la fintech*

La réglementation en vigueur dans le secteur bancaire ne convient pas toujours aux fintechs. Contrairement aux banques, il est impossible de prévoir un cadre de cybersécurité unique pour la fintech en raison de la diversité des structures commerciales et opérationnelles. Il est donc essentiel de créer des normes réglementaires spéciales pour les fintechs et surtout de les faire évoluer au même rythme (rapide) que celles-ci.

Dans plusieurs pays, les fintechs ne sont pas aussi strictement régies que les institutions financières traditionnelles. Il convient donc de reconnaître le potentiel perturbateur des fintechs avec les risques que cela entraîne et d'ajouter une couche réglementaire supplémentaire à l'intention des fintechs, a l'instar, par exemple, de la South African Reserve Bank (SARB). Celle-ci a commencé à mettre en place des structures pour monitorer l'écosystème des fintechs et à concevoir des réponses appropriées aux changements technologiques.[66]

Comme les fintechs sont souvent des petites entreprises qui ont l'habitude de prendre des risques, elles n'hésiteront pas à se mettre en non-conformité aux exigences réglementaires, surtout quand celles-ci ne sont pas adaptées. Raison de plus pour le régulateur financier de s'assurer que les fintechs analysent correctement les risques et mettent en œuvre des procédures d'atténuation. Il faut aussi prendre en compte que d'une manière générale ces entités fonctionnent au maximum de leur capacité opérationnelle et qu'elles ont souvent de la difficulté à appliquer les procédures réglementaires.

### • *Quand la menace vient du ciel*

L'analyse du risque cyber ne se limite pas à prendre en compte l'infrastructure traditionnelle de la banque, mais elle doit aussi couvrir l'exposition à l'environnement infonuagique (cloud computing). Par exemple, une panne prolongée chez un grand opérateur de services en nuage engendrerait un problème immédiat pour les institutions financières. Non seulement l'accès à leurs services en ligne serait compromis, mais l'ensemble de leurs opérations serait perturbé.

L'autre grande vulnérabilité est le changement de paradigme de la cybercriminalité qui privilégie de plus en plus les utilisateurs finaux, leurs appareils mobiles et leurs identités, en s'appuyant généralement sur des techniques d'ingénierie sociale comme l'hameçonnage (phishing). Ce faisant, le nouveau périmètre numérique à protéger se dématérialise et il réside désormais dans l'identité des individus.

La Banque des règlements internationaux (BRI) a bien résumé la nouvelle problématique que la popularité du nuage a imposé aux institutions financières :

> *"Tout d'abord, l'estompement des frontières numériques et physiques d'une organisation nécessite de nouvelles stratégies. Une approche courante est le concept dit de "confiance zéro". Elle part du principe qu'il est impossible de faire confiance aux défenses du périmètre ou même au réseau interne."*[67]

Une idée fausse très répandue est que l'opérateur infonuagique est le seul responsable du maintien de la sécurité des services hébergés sur ses infrastructures. La BRI est formelle à ce sujet: "En fait, la sécurité des données, les configurations sécurisées et la gestion des vulnérabilités sont une responsabilité partagée."[68] La stratégie de cybersécurité de l'institution financière doit impérativement tenir compte de cette dimension nouvelle introduite par le nuage.

**66** *"Project Khokha", South African Reserve Bank (SARB), 2018, 79 pages. Cf. p. 18.*
**67** *"Cyber risk in central banking", BIS Working Papers, septembre 2022, 22 pages. Cf. p. 6.*
**68** *"Cyber risk in central banking", idem.*

# 3 LE CYBERCRIME COMME CONTREPARTIE DE LA TRANSFORMATION DIGITALE

## • *Les cryptomonnaies et l'anarchie de la finance décentralisée*

Le bitcoin et autres cryptomonnaies règnent en maître sur le darkweb où leur absence de traçabilité en font le moyen de paiement privilégié de tous les cybercriminels. Elles servent ainsi de moyen de paiement pour les données volées ou les attaques par rançongiciel. Les escrocs exploitent également le manque de familiarité des consommateurs avec les cryptomonnaies.[69]

Ainsi, de mai 2018 à mars 2021, plusieurs centaines de milliers de personnes ont été escroquées en Afrique du Sud par Mirror Trading International. Grâce à un ingénieux système de Ponzi, des bitcoins pour une valeur de 1,7 milliard USD ont été dérobés. Comme une partie des victimes étaient américaines, l'affaire a été portée devant la justice aux États-Unis et en avril 2023 une pénalité record de 3,4 milliards USD a été prononcée.[70]

En avril 2021, l'Afrique du Sud a de nouveau fait parler d'elle pour un piratage cryptographique encore plus important, cette fois par une société appelée Africrypt, dont les deux fondateurs âgés de 18 et 20 ans ont dérobé 3,6 milliards de dollars à des investisseurs en l'espace de quelques heures. Avant de disparaître, les deux jeunes escrocs avaient déclaré être eux-mêmes victimes d'un vol…[71]

Les cryptomonnaies ont donné naissance à tout un écosystème de finance à structure décentralisée que l'on appelle DeFi (en anglais Decentralized Finance). On y propose des services bancaires classiques (percevoir des intérêts, emprunter, prêter, acheter des assurances, négocier des produits dérivés et des actifs) mais avec plus de rapidité, sans paperasse et sans intermédiaire.

À l'image de la plupart des cryptomonnaies, la DeFi est fondée sur la blockchain ainsi que de technologies open-source publiques et « composables ». Cette souplesse structurelle signifie que chaque créateur de plateformes peut assembler les composants mis au point par d'autres entreprises et se concentrer uniquement sur la construction des composants manquants pour son propre projet. Cela augmente de façon exponentielle le taux d'expérimentation et d'innovation.

Mais l'industrie de la DeFi est particulièrement vulnérable aux risques du marché et au risque cyber. Les cyberattaques, qui peuvent être graves pour les banques traditionnelles, sont souvent meurtrières pour ces plateformes car elles dérobent les actifs financiers et ébranlent la confiance des usagers. L'absence de garantie des dépôts sur les plateformes DeFi expose tous les dépôts à un risque extrême.[72]

## *Le cas de la monnaie numérique*

La monnaie numérique de banque centrale (MNBC) n'est pas encore déployée sur une base commerciale - hormis le Nigéria - mais la dimension cybersécurité est d'ores et déjà considérée comme cruciale. En effet, les MNBC ont vocation à accroître considérablement la centralisation du système financier en stockant dans un registre unique les données de transactions de toute une population, y compris celles qui sont jusqu'à présent effectuées en argent liquide.

> **Le principal défi opérationnel relevé est le risque cyber, encore plus en Afrique qu'ailleurs : il figure parmi les trois principales préoccupations de toutes les banques centrales africaines et en tête de liste pour plus de la moitié d'entre elles. Une cyberattaque réussie contre les MNBC pourrait causer des dommages étendus et graves et éroder la réputation des banques centrales.**
>
> "Central bank digital currencies in Africa", BIS Papers, novembre 2022

Une centralisation aussi radicale des MNBC pourrait avoir des effets imprévisibles. Imaginons la cible que représenterait pour les cybercriminels une base de données contenant les transactions financières d'une nation entière. Pour les forces de l'ordre aussi, la tentation sera grande d'accéder à certaines données confidentielles pour faciliter les enquêtes en cours. Bref, avant même d'être déployées à grande échelle, les MNBC posent des problèmes aux banques centrales qui doivent absolument être résolus avant qu'une catastrophe cyber sans précédent ne survienne.[73]

*69 "Cyber Threats to the Financial Sector in Africa", Banque mondiale, mars 2022, 37 pages. Cf. p. 8.*
*70 Tom Mitchelhill, "CFTC wins record $3.4B penalty payment in Bitcoin-related fraud case", CoInTelegraph, 28 avril 2023.*
*71 Brian Quarmby, "$3.6B in Bitcoin vanishes in 'hack' along with owners of South African crypto platform", Cointelegraph, 24 juin 2021.*
*72 Antonio Garcia Pascual et Fabio Natalucci, "L'évolution rapide des fintechs, un défi pour les régulateurs", IMF Blog, 13 avril 2022.*
*73 "Missing Key: The Challenge of Cybersecurity and Central Bank Digital Currency", Atlantic Council, 2022, 49 pages. Cf. p. 8.*

# 4

# COMMENT LE SECTEUR FINANCIER LUTTE CONTRE LA CYBERCRIMINALITÉ

Nous abordons ici les aspects de la lutte contre le cybercrime exclusivement aux niveaux politique et réglementaire. La gestion proprement dite de la cybersécurité dans le secteur bancaire a été traitée dans notre livre blanc La fraude bancaire en Afrique subsaharienne (2019).

# 4 COMMENT LE SECTEUR FINANCIER LUTTE CONTRE LA CYBERCRIMINALITÉ

## 4.1 - L'approche politique

### • *Stratégie nationale de cybersécurité*

Selon la Conférence des Nations unies sur le commerce et le développement (CNUCED), 39 des 54 pays africains ont mis en place une législation sur la cybersécurité, tandis que deux ont des projets de législation en cours d'élaboration (Congo et Eswatini). Toutefois, il reste encore beaucoup à faire, car 14 pays n'ont pas encore entamé le processus d'élaboration d'une législation sur la cybersécurité (voir figure 15 - L'état de la législation sur la cybercriminalité en Afrique)[74].

Au chapitre des mesures techniques, la mesure la plus notable est l'installation graduelle d'une infrastructure de cybersécurité en Afrique subsaharienne. Il y a déjà 27 CERT en activité répartis dans 16 pays et 22 CIRT nationaux[75]. Deux nouveaux CIRT nationaux sont actuellement en voie de déploiement au Burundi et au Malawi avec la coopération de l'UIT. Ces chiffres sont en augmentation rapide.

**Quelle est la différence entre un CERT et un CIRT ?**

Le sigle CERT est une marque de commerce de l'Université Carnegie Mellon. Pour l'utiliser, il faut en demander l'autorisation auprès des autorités de cette institution. On réserve le terme de CERT aux grandes organisations de sécurité informatique. De son côté, le sigle CIRT est plus générique et peut recouvrir des petites organisations. Son rôle est d'intervenir en cas d'incident de sécurité informatique à titre de responsable de la réception, de la révision et du traitement des rapports d'incident. On parle parfois de CSIRT.

En Tunisie, l'Association professionnelle tunisienne des banques et des établissements financiers (APTBEF) a créé en 2018 le premier CERT sectoriel en Afrique du Nord dans le cadre d'une convention avec l'ANSI. Devenue depuis lors le Conseil bancaire et financier (CBF), cette association regroupe 22 banques universelles, deux banques offshores, deux banques d'affaires, huit compagnies de leasing et deux sociétés de factoring. Son CERT accrédité auprès du Forum of Incident Response and Security Teams (FIRST) assure une activité de veille pour identifier les menaces potentielles et alerter les parties concernées. Il agit comme un hub de communication pour tout le secteur bancaire tunisien[76].

De son côté, la firme marocaine de cybersécurité Dataprotect a mis au point le premier CSIRT privé en Afrique, également accrédité FIRST. Une équipe d'une trentaine d'analystes certifiés travaille en relation étroite avec le SOC de l'entreprise afin de superviser les incidents de sécurité en mode 24/7. Leur mission est d'anticiper, analyser et contrer les menaces. Le CSIRT émet plus de 300 bulletins de cybersécurité par an sur l'actualité cyber à l'intention de la clientèle.

*74 "Africa Cyber Security Outlook", KPMG, September 2022, 47 pages. Cf. p. 7.*
*75 Pour les CERT, la liste complète est disponible sur le site: FIRST Teams - https://www.first.org/members/teams/?#*
*Pour la liste des CIRT, veuillez consulter: National CIRT, International Telecommunications Union (ITU). - https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx.*
*76 "Le CERT bancaire", présentation, APTBEF, octobre 2018. - https://www.ansi.tn/sites/default/files/présentation%20cert%20bancaire.pdf*

**FIGURE 12 -** L'ÉTAT DE LA LÉGISLATION SUR LA CYBERCRIMINALITÉ EN AFRIQUE


*Source : Jules Hervé Yimeumi, Africa Data Protection, janvier 2023.*

Une législation nationale est indispensable, mais nullement suffisante. En effet, de plus en plus d'entreprises stockent leurs données dans le « cloud ». Il est impossible de garantir la sécurité de ces données avec une législation traditionnelle. En outre, la cybercriminalité est un phénomène international. Si on veut que les forces de l'ordre soient sur un pied d'égalité avec les organisations criminelles, il faut que la lutte contre la cybercriminalité soit aussi transfrontalière.

## • *Concertation panafricaine*

La première étape de la coopération internationale est continentale. Dans cette optique, l'Union africaine a adopté en juin 2014 la Convention de Malabo. Celle-ci prévoit que « chaque État partie s'engage à adopter des mesures législatives et/ou réglementaires pour identifier les secteurs considérés comme sensibles pour sa sécurité nationale et le bien-être de l'économie »[77]. Le texte s'attache à la régulation des transactions électroniques et à la protection des données personnelles.

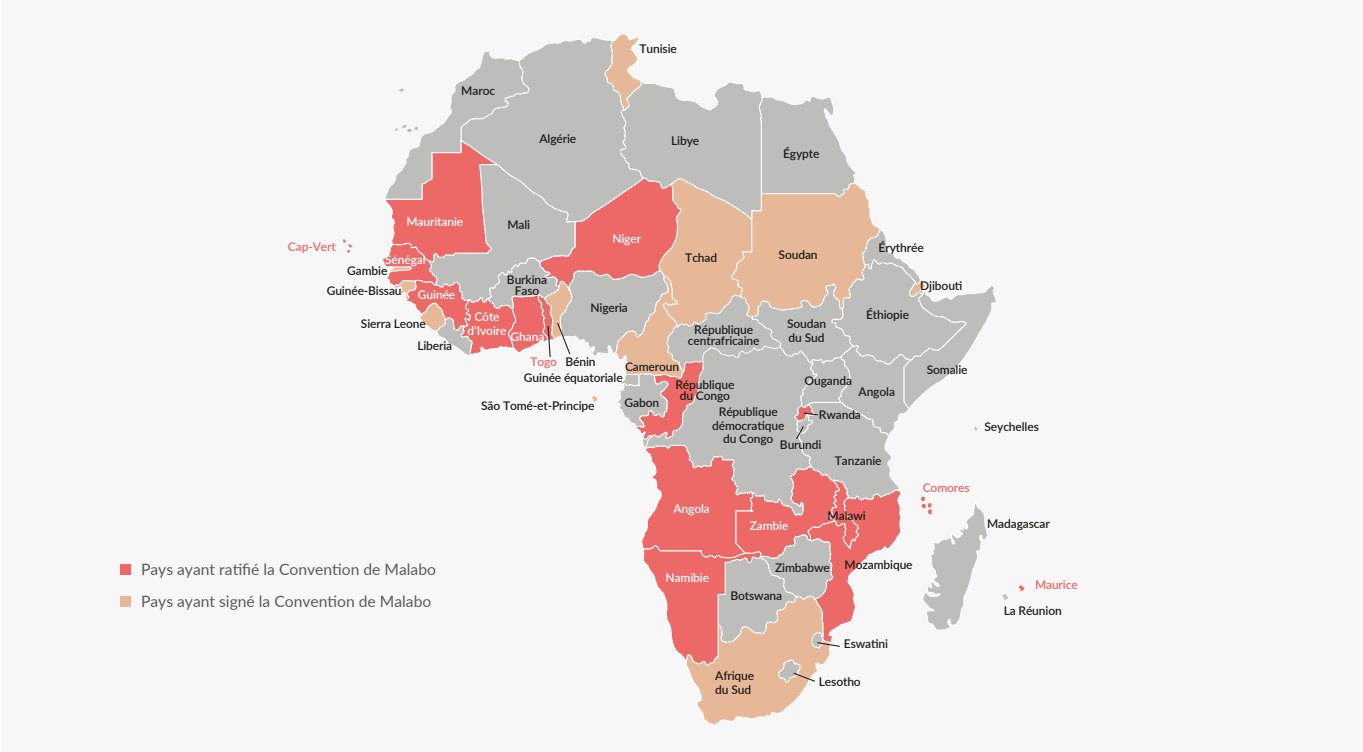
Pour entrer en vigueur, la Convention de Malabo doit être ratifiée par 15 pays. Or, cet objectif n'a été atteint qu'en avril 2023 avec la ratification de la Mauritanie. Par ailleurs, 12 autres pays ont posé leur signature mais ne l'ont pas encore ratifié. Après un démarrage extrêmement lent, il faut souhaiter que l'adoption toute récente de la Convention suscite un momentum et que les géants de l'Afrique l'adoptent enfin (Égypte, Nigéria, Afrique du Sud…).

Ce retard apporté à la généralisation de la ratification d'un accord continental aussi crucial est d'autant plus inexplicable que, comme on l'a vu, la majorité des États s'est déjà dotée d'un cadre légal national. Néanmoins, l'adhésion à la convention de l'UA reste primordiale pour consolider l'arsenal juridique de la protection du cyberespace ainsi que pour favoriser la coopération inter-étatique.[78]

*77 "Convention de l'Union africaine sur la cyber-sécurité et la protection des données à caractère personnel", Union africaine, 27 juin 2014.*
*78 Christelle Houeto, "Bilan de la ratification de la convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel", Africa Cybersecurity Magazine, 15 février 2023.8.*

# 4 COMMENT LE SECTEUR FINANCIER LUTTE CONTRE LA CYBERCRIMINALITÉ

**FIGURE 13 -** PAYS AYANT SIGNÉ OU RATIFIÉ LA CONVENTION DE MALABO




*Source : Dataprotect/Sciencetech, 2023*

## • *Concertation régionale*

Pendant que la coopération continentale marque le pas, la coopération régionale semble progresser. Peut-être la proximité avec la situation sur le terrain permet-elle d'établir des liens plus concrets? Toujours est-il que les quatre grands regroupements régionaux africains ont tous adopté des mesures relatives à la cybersécurité :

- La Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) a émis en août 2011 une Directive relative à la lutte contre la cybercriminalité. Elle invite les États à transférer ce cadre juridique dans les législations nationales.
- En octobre de la même année, le Marché commun de l'Afrique orientale et australe (COMESA) approuvait une loi-type relative à la cybercriminalité ainsi que d'une feuille de route de mise en œuvre pour la cybersécurité.
- De son côté, la Communauté de développement de l'Afrique australe (SADC) adoptait en mars 2012 une loi-type sur la criminalité informatique et la cybercriminalité.
- Enfin, la Communauté économique des Etats de l'Afrique centrale (CEEAC) adoptait sa propre loi type sur la cybersécurité en décembre 2016.[79]

## • *Le cas particulier d'AFRIPOL*

S'il est un champ crucial en matière de cybersécurité, c'est bien celui de la coopération policière. Particulièrement important pour notre propos est la création par l'Union africaine d'Afripol (African Police Office) en 2014 à partir d'un projet de la conférence régionale africaine d'INTERPOL. Le but de l'agence est de faciliter l'échange de renseignements entre polices africaines en matière de criminalité, de terrorisme, de stupéfiants ou de trafic d'armes.

Le siège d'AFRIPOL est à Alger et 41 pays sont déjà membres de l'agence, ce qui en soi est un succès. AFRIPOL a un partenariat privilégié avec INTERPOL. Ainsi, les deux organisations ont mis en place en 2020 le Programme INTERPOL d'appui à l'Union africaine en relation avec AFRIPOL (ISPA). Ce programme encadre la coopération des deux organisations dans des domaines clés, notamment la cybercriminalité.

**79** *"Des voix africaines plus fortes dans le numérique", Diplo, novembre 2022, 223 pages. Cf. p. 110.*

Entre juillet et novembre 2022, l'opération Cyber Surge Afrique a réuni les forces de polices de 27 pays pour lutter contre la cybercriminalité transfrontière. Cette opération conjointe INTERPOL-AFRIPOL a permis de démanteler le réseau criminel nigérian connu sous le nom de Black Axe. Plus de 70 fraudeurs ont été arrêtés en Afrique du Sud, au Nigéria et en Côte d'Ivoire, ainsi qu'en Europe, au Moyen-Orient, en Asie du Sud-Est et aux États-Unis.

L'opération Cyber Surge Afrique a été suivie d'une réunion de bilan organisée à Maurice pour permettre aux pays membres de partager leurs réussites, d'analyser les difficultés et d'identifier les domaines à améliorer. L'opération a également conduit à l'introduction de nouveaux protocoles législatifs et à la création d'une série de services de lutte contre la cybercriminalité dans les forces de police des pays membres.[80]

Dans le cadre de cette politique de lutte contre la cybercriminalité, AFRIPOL a organisé en septembre 2022 la première édition de son bootcamp sur les enquêtes en matière de cybercriminalité, y compris l'hameçonnage, les logiciels malveillants, le renseignement de sources ouvertes (OSINT), le darknet et les crypto-monnaies. Ce bootcamp a réuni 136 participants des forces policières de 22 pays.[81]

### • *Traités internationaux*

La réglementation internationale présente l'avantage de prendre en compte le caractère global de la cybercriminalité. L'Organisation des Nations unies travaille à l'élaboration d'une politique de coopération entre les États pour réduire les risques dans le cyberespace. Plusieurs groupes de travail ont été créés à cet effet (voir Annexe III).

De nombreux pays africains ont participé à ces travaux. Malheureusement, tous ces efforts ont débouché dans une impasse en raison de l'opposition entre les États-Unis qui estiment que le droit international existant doit s'appliquer dans le cyberespace et la Chine qui estime qu'un nouveau traité doit être conclu qui serait basé sur un code de conduite en matière de cybersécurité.

C'est ainsi que certains pays africains se tournent vers le seul traité international existant, à savoir la Convention sur la cybercriminalité de Budapest entrée en vigueur en juillet 2004. Bien qu'adoptée sous l'égide du Conseil de l'Europe, la Convention de Budapest est ouverte à tous les États. Au total, 68 pays ont ratifié la Convention de Budapest, dont six pays africains : Maurice, Sénégal, Cap Vert, Ghana, Nigéria et Maroc[82].

Une fois la Convention de Budapest mise en place, un problème est vite apparu: comment exercer la justice dans le cyberespace quand les preuves électroniques du délit sont stockées à l'étranger ? Le Conseil de l'Europe a adopté en novembre 2021 le deuxième Protocole additionnel à la Convention de Budapest qui met en place des outils de coopération inter-étatique à cet effet. Trente-cinq pays ont déjà signé le deuxième Protocole additionnel, dont un pays africain (Maroc). D'autres devraient suivre prochainement.

## 4.2 - L'approche réglementaire

### • *Réglementation nationale*

La banque centrale et, quand elle est distincte, l'autorité de réglementation, constituent la cheville ouvrière de la cyber-résilience du secteur bancaire en Afrique. Or, une enquête menée par l'Association des banques centrales africaines (ABCA) montre que 60% seulement des banques centrales africaines ont mis en place un système spécifique d'analyse des risques de cybersécurité ou s'apprête à le faire. Plus précisément, 27,5% des banques centrales sont déjà dotées d'un tel outil et 32,5% sont en cours de s'en doter.[83]

Qui plus est, aux dires de l'ABCA, dans la plupart des banques centrales, le dispositif de suivi des risques "n'est pas encore totalement opérationnel" et n'a pas donné lieu au déploiement de mesures préventives adéquates. Par ailleurs, la sensibilisation et l'implication des banques commerciales ne fait pas encore l'objet d'une programmation formalisée. Ces données ont été recueillies en 2019, juste avant la crise du Covid. Il y a peu de chances qu'elles aient été sensiblement améliorées depuis lors.

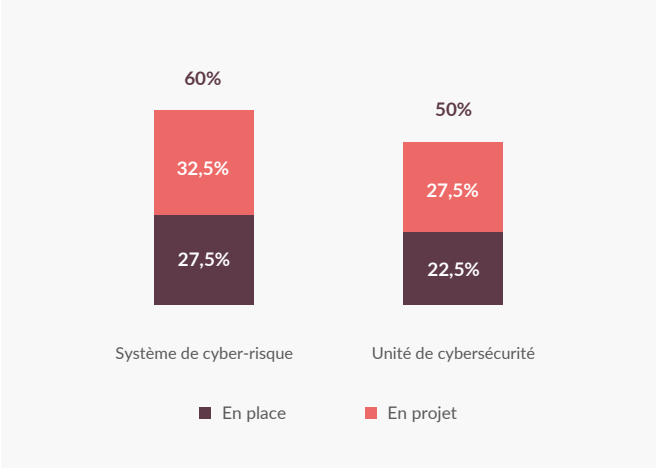
---

***80*** *"Une opération à travers le continent africain permet d'identifier des cybercriminels et les infrastructures virtuelles à risque", INTERPOL, 25 novembre 2022.*
*- Jason Burke, "Gangs of cybercriminals are expanding across Africa, investigators say", The Guardian, 27 novembre 2022.*
***81*** *Site web d'AFRIPOL: https://afripol.africa-union.org/?lang=fr*
***82*** *L'Afrique du Sud, le Bénin, le Burkina Faso, le Cameroun, la Côte d'Ivoire, le Niger, la Sierra Leone et la Tunisie ont signé la Convention, mais ne l'ont pas ratifiée.*
***83*** *"Projet de rapport sur les expériences et les initiatives des banques centrales membres de l'ABCA en matière de développement des fintechs et de cybersécurité", Association des banques centrales africaines (ABCA), août 2019, 26 pages + annexes. Cf. p. 13. Sur une population totale de 40 banques centrales au moment de l'envoi du questionnaire, il y a eu 31 réponses. Nous avons supposé que les non-répondants auraient répondu non.*

# 4 COMMENT LE SECTEUR FINANCIER LUTTE CONTRE LA CYBERCRIMINALITÉ

Ce n'est pas tout, 50% seulement des banques centrales africaines ont créé un groupe d'experts en cybersécurité ou s'apprêtent à le faire. Plus précisément, 22,5% des banques centrales disposent d'une telle unité, tandis que 27,5% envisagent d'en créer une.[84] Cela ne signifie pas que les autres banques centrales soient entièrement démunies. Dans certains pays, la cybersécurité de la banque centrale et du secteur financier en général est assurée par un service spécialisé gouvernemental.

**FIGURE 14 -** BANQUES CENTRALES AYANT UN CADRE D'ANALYSE DES CYBER-RISQUES ET UNE UNITÉ DE CYBERSÉCURITÉ




*Source : ABCA, 2019.*

Il n'empêche que l'absence d'une unité de cybersécurité dans une banque centrale prive celle-ci d'une composante cruciale de sa stratégie de résilience ainsi que des ses moyens d'agir sur l'écosystème financier en général. Aucun service gouvernemental de cybersécurité ne saurait remplacer l'expertise de la banque centrale en matière financière.

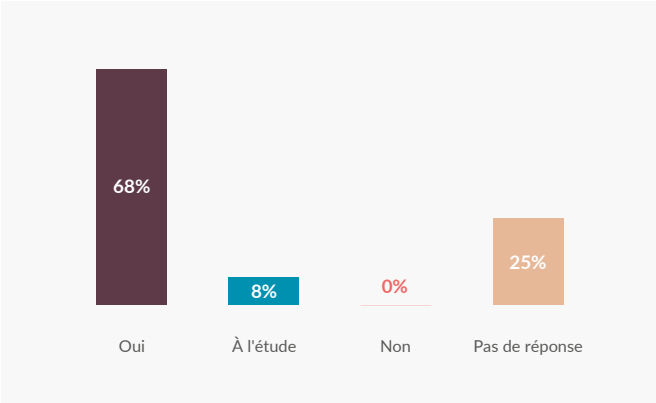
## • *Approche associative*

L'Association des banques centrales africaines (ABCA) existe depuis 1965 et compte 41 membres. Cette institution a pour mission de favoriser l'instauration et le maintien d'une coordination efficace des politiques monétaire, bancaire et financière entre les membres, ainsi que la promotion de l'avènement d'une monnaie unique et d'une banque centrale commune en Afrique.[85]

L'ABCA comprend également une entité appelée Communauté des Superviseurs Bancaires Africains (CSBA) qui est appelée à devenir le cadre d'échange de vue entre les superviseurs de banques, d'apprentissage entre les pairs, de réflexion sur les sujets pertinents à l'échelle mondiale et de formulation des préoccupations du continent. Elle maintient des liens réguliers avec la Banque Centrale Européenne (BCE) et la Réserve Fédérale de New York (FRBNY).

La coopération en matière de réglementation des fintechs et de cybersécurité exige le partage d'information. Les banques centrales africaines sont d'accord avec cet énoncé puisque dans le cadre du sondage organisé par l'ABCA, elles ont répondu à 68% qu'elles souhaitaient participer à une plateforme organisant une telle coopération. Pas une seule banque centrale africaine ne souhaitait rester au-dehors d'une plateforme dédiée aux échanges d'expériences dans ces deux domaines.

**FIGURE 15 -** LES BANQUES CENTRALES AFRICAINES SONT FAVORABLES AU PARTAGE D'INFORMATION...

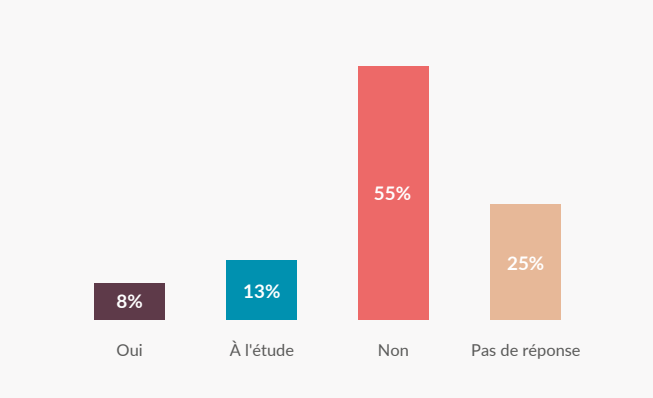



*Source : ABCA, 2019.*

En revanche, quand on demande aux banques centrales si elles partagent déjà de l'information sur les cyber-incidents avec leurs consœurs, une infime minorité de 8% d'entre elles répond qu'elle le fait et 13% qu'elle y songe. La grande majorité des banques ne partage pas son information.

**84** *ABCA, idem, cf. p. 14.*
**85** *Jean-Pierre Malou, "Création de la banque centrale africaine : l'ABCA s'auto-évalue", Sud Quotidien, 11 mars 2023.*

**FIGURE 16 -** ... MAIS ELLES NE PARTAGENT PAS L'INFORMATION SUR LES CYBER-INCIDENTS




*Source : ABCA, 2019.*

Cette réponse semble en porte-à-faux avec celle qui précède. Pourtant, ce n'est pas forcément le cas. Le même sondage de l'ABCA pose aussi une série d'autres questions sur la participation à une plateforme structurée de soutien aux incidents. Dans ce cas précis, le taux des banques centrales qui se déclarent en faveur d'une telle initiative s'élève à 40%.

Les réponses des banques centrales sont riches d'informations. Elles mettent en évidence que le partage d'information, quand bien même il est souhaité par la grande majorité des intervenants, ne va pas de soi. C'est une pratique incertaine qui demande à être encadrée et accompagnée avec soin.

## • *Réglementation internationale*

Au cœur de la réglementation internationale se trouve la Banque des règlements internationaux (BRI) que l'on peut définir comme étant la « banque des banques centrales ». Sa principale mission est la coopération entre banques centrales (forum de discussion, plateforme d'innovation, analyses sur les enjeux et services financiers) et elle joue un rôle déterminant dans la gestion des réserves de devises de ces institutions.

La BRI est détenue par 63 banques centrales, représentant principalement les pays membres de l'OCDE et seulement trois pays africains (Bank of Algeria, Bank Al-Maghrib[86] et South African Reserve Bank). La moitié du capital appartient aux banques centrales d'Allemagne, d'Angleterre, de Belgique, de France, d'Italie et des États-Unis. Ce sont les gouverneurs de ces six banques centrales qui se partagent la direction de la BRI.

Le Comité de Bâle, qui traite plus précisément des aspects relatifs à la supervision bancaire, est hébergé dans les locaux de la BRI. Le Comité de Bâle compte 28 pays membres dont un seul africain (South African Reserve Bank).[87] Initialement consacré à la supervision du risque financier, le Comité de Bâle couvre depuis 2005, le risque opérationnel, dont le risque cyber une composante de plus en plus importante.

Les banques africaines sont soumises à la réglementation et à la supervision bancaire internationale, principalement définies dans le cadre du Comité de Bâle par les accords de Bâle I, Bâle II et Bâle III ainsi qu'à la finalisation de ce dernier accord que l'on appelle parfois Bâle IV. En Afrique, comme dans bien des pays en voie de développement, l'application de cette réglementation internationale conçue pour des pays fortement industrialisés, pose un défi majeur.

Selon la Banque mondiale, un grand nombre de pays en développement adoptent à la pièce les aspects "les moins compliqués" des accords réglementaires internationaux de Bâle II et III. C'est précisément le cas en Afrique, où la majorité des banques utilise toujours l'approche relativement simple des actifs pondérés par les risques, préconisée dans Bâle I, et n'adopte pas l'approche fondée sur les notations internes de Bâle II/Bâle III. Seule l'Afrique du Sud satisfait aux accords de Bâle dans leur intégralité.[88]

> **En raison de la complexité des normes de Bâle, les pays non-membres (du Comité de Bâle) peuvent ne pas disposer de l'infrastructure ou de la capacité de surveillance nécessaire pour contrôler efficacement le respect de ces normes. En outre, les avantages de Bâle II pourraient ne pas compenser les coûts de mise en œuvre dans les pays qui ne comptent que quelques grandes banques internationales.**
>
> Banque mondiale, 2020[89]

*86 Banque centrale marocaine.*
*87 En fait, le Comité de Bâle appartient à 45 membres répartis dans 28 pays, car certains pays sont représentés par plusieurs institutions.*
*88 Nkhangweleni Masindil et Paul Singh, "Banking regulation and supervision in Africa: A conceptual framework", International Journal of Innovation, Creativity and Change, vol. 16, N°3, 2022. - "Overview of Africa's Financial Sector", Africa, Mediterranean, and Europe Network (AMENET) et Making Finance Work for Africa (MFW4A), mai 2021, 67 pages. Cf. p. 64.*
*89 "Bank Regulation and Supervision a Decade after the Global Financial Crisis", World Bank, 2020, 135 pages. Cf. p. 93.*

# 5

# DISCUSSION SUR DEUX EXEMPLES DE RÉGLEMENTATION NATIONALE

Chaque banque centrale est le reflet des spécificités de son environnement politique, juridique et financier. D'emblée, on peut distinguer les pays où les banques centrales exercent la réglementation du secteur financier et les pays où il existe une autorité de régulation distincte - au Maroc, la banque centrale Bank Al-Maghrib illustre le premier cas, tandis que le Canada dispose d'un Bureau du surintendant des institutions financières (BSIF).

Même si cette dernière illustre un modèle relativement éloigné du modèle africain, elle représente une méthodologie riche d'enseignement pour notre propos. Les témoignages de responsables de ces deux institutions permettent de documenter différentes facettes de la lutte contre le risque cyber.

# 5 DISCUSSION SUR DEUX EXEMPLES DE RÉGLEMENTATION NATIONALE

## 5.1 - Cas de Bank Al-Maghrib : Innovation et promotion de la cyber-résilience

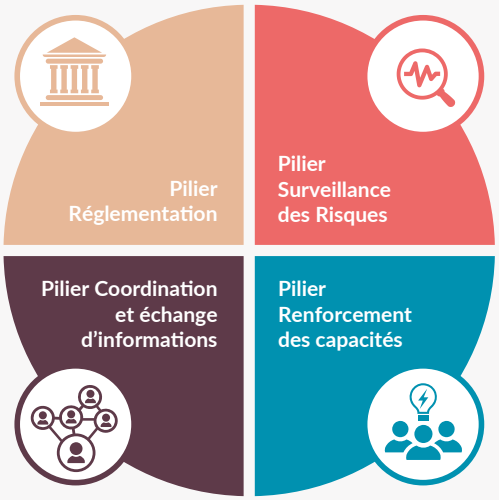
La Bank Al-Maghrib (BAM) est la banque centrale du Maroc et à ce titre a une double responsabilité en matière de cybersécurité: comme entreprise et comme régulateur du système financier marocain. En tant qu'entreprise, elle est désignée comme infrastructure d'importance vitale (IIV) par la Loi sur la cybersécurité de 2020. En tant que régulateur, BAM est désignée comme coordonnateur sectoriel pour le secteur bancaire.

Dans les deux cas, en matière de cybersécurité, BAM se rapporte à la Direction générale de la sécurité des systèmes d'information (DGSSI) qui, elle-même relève de l'Administration de la Défense marocaine. En sens inverse, la DGSSI consulte BAM chaque fois qu'elle projette d'émettre un texte réglementaire qui concerne le secteur bancaire. La banque centrale est ainsi devenue un acteur majeur dans la stratégie de cybersécurité du Maroc.

Il convient de noter que tous les acteurs du secteur bancaire ne sont pas considérés comme des infrastructures d'importance vitale. Seules les banques ayant une importance systémique le sont. Alors que l'autorité de la DGSSI couvre uniquement les banques classées IIV, l'autorité de BAM s'étend à l'ensemble du secteur bancaire. Les échanges entre BAM et la DGSSI sont constants pour tout ce qui touche les banques d'importance systémique.

Le dispositif de supervision du risque cyber dans le secteur bancaire par BAM est articulé autour de quatre piliers d'action :
- Réglementation,
- Surveillance des risques,
- Coordination,
- Échange d'information, renforcement des capacités.

**FIGURE 17 -** LES QUATRE PILIERS D'ACTION DE LA BANQUE CENTRALE DU MAROC




*Source : Bank Al-Maghrib (BAM).*

## • *La réglementation*

Au cœur de la réglementation du risque cyber se trouve une circulaire sur le contrôle interne adoptée par la banque centrale marocaine en 2016. Celle-ci définit le risque opérationnel, la continuité d'activités et le risque informatique et s'applique à tous les établissements de crédit et organismes assimilés.

La même année, BAM a émis une directive qui exige des établissements de crédit qu'ils élaborent une cartographie des risques cyber et qu'ils réalisent régulièrement, sur la base de cette cartographie, des tests d'intrusion de leurs systèmes d'information. Cette directive a été établie conjointement avec la DGSSI et après consultation avec les membres du secteur bancaire, les prestataires spécialisés en cybersécurité ainsi que certains homologues étrangers - le tout en conformité avec les normes internationales.

L'objectif de ce processus complexe est de mettre au point une réglementation qui soit à la fois exhaustive et facilement applicable. Le même exercice a été effectué en 2022 pour l'usage du cloud computing et la banque centrale travaille actuellement à une directive sur la résilience opérationnelle numérique dans l'esprit de ce qui a été fait dans le cadre de l'Union européenne avec la réglementation DORA (voir Annexe 4). D'autres projets sont prévus qui portent sur la dépendance vis-à-vis des tiers, l'interconnexion des différents secteurs, etc.

Quand il y a un incident ou une crise, BAM ne joue pas le rôle de régulateur, mais celui de "pompier" pour aider et accompagner les banques, pour leur faciliter l'accès aux organismes de régulation et de contrôle (principalement la DGSSI) et leur permettre de traiter les incidents ainsi que de renforcer leur cybersécurité. La régulation vient par la suite en cas de manquements ou pour vérifier la conformité avec les directives.

> **La cybersécurité est le seul volet d'activité du secteur bancaire où il ne peut pas et ne doit pas y avoir de concurrence.**
>
> Lhoussaine Derouich, Manager projets digitaux, BAM, 2023

Sur le plan pratique, cela signifie qu'en cas d'incident, BAM va organiser des réunions bilatérales avec la banque, suivre le plan d'action, prendre les mesures préventives qui s'imposent et, pour finir, dresser le bilan de l'intervention. Celui-ci donne ensuite lieu à une séance de partage d'expérience avec l'ensemble des établissements du secteur. Si la banque est d'accord, elle expose elle-même l'incident, sinon c'est BAM qui partage les bonnes pratiques ayant servi à réduire la cyberattaque, tout en préservant l'anonymat de la victime.

Chaque fois que la situation le justifie, un courrier est ensuite envoyé à l'ensemble du secteur bancaire qui reprend les mesures prises durant l'incident qui ont fait l'objet d'un consensus durant la séance de partage d'information. Chaque établissement doit alors adopter à son tour ces mesures et les déployer. Les actions ne sont pas imposées par la banque centrale, elles sont mises au point par le milieu lui-même. La banque centrale intervient seulement dans les cas où il faut dégager des budgets ou toute autre forme de soutien.

BAM est bien évidemment une infrastructure d'importance vitale et tout ce qu'elle impose aux banques commerciales en matière d'exigences réglementaires est également appliqué à sa propre organisation. Le Groupe des projets digitaux appartient à la fonction de régulation de la banque centrale, mais il participe également aux réunions du Comité de sécurité. Il est ainsi amené à vivre de l'intérieur les mêmes difficultés d'application des exigences de cybersécurité que les banques commerciales. Cette dualité régulateur/régulé constitue un atout précieux.

BAM finalise actuellement le plan stratégique 2024-2026 avec un accent particulier sur le digital et la cybersécurité. Cette stratégie va au-delà des normes réglementaires internationales. Si la base du plan est constituée par les recommandations des accords de Bâle, la banque centrale marocaine prend aussi en considération les normes internationales (ISO, NIST...), le cadre réglementaire national (DGSSI, Loi 05-20...) et bien sûr les pratiques spécifiques du secteur bancaire domestique

# 5 DISCUSSION SUR DEUX EXEMPLES DE RÉGLEMENTATION NATIONALE

## • *Coordination et échange d'information*

À la faveur de l'implantation des banques marocaines en Afrique subsaharienne, BAM a été amenée à faire face aux risques internationaux et donc à mettre en place des dispositifs de suivi à l'échelle du continent. C'est ainsi que BAM a développé son propre CERT afin de gérer les incidents de sécurité informatique. Son équipe de réponse à incident exerce une veille de la menace générique et sectorielle. CERT-BAM promeut l'échange au sein de la banque centrale et avec ses pairs en vue de prévenir des attaques potentielles. Des mémorandums d'entente et des échanges d'information ont lieu régulièrement avec la Banque centrale des États de l'Afrique de l'Ouest (BCEAO) et la Banque des États de l'Afrique centrale (BEAC) ainsi que plusieurs autres banques centrales.

Les activités internationales de BAM épousent étroitement les recommandations du Comité de Bâle qui prévoit la création d'un collège de superviseurs par l'autorité de contrôle du pays d'origine d'un groupe bancaire donné ayant des activités transfrontières importantes. Ces collèges constituent un forum de discussion entre l'autorité de contrôle du pays d'origine, à savoir BAM, et les autorités de contrôle des pays où est implanté le groupe en question. On y aborde le profil des risques des succursales ou filiales établies dans leurs juridictions respectives et, le cas échéant, des actions de supervision conjointe à mener.

**Origine des collèges de superviseurs**

**Les collèges de superviseurs devraient être des structures permanentes mais flexibles de collaboration, de coordination et d'échange d'informations entre les autorités responsables du contrôle des groupes bancaires transfrontaliers et impliquées dans ce contrôle. Si des accords bilatéraux et multilatéraux entre autorités de surveillance de groupes bancaires mondiaux existent depuis des décennies, nombre d'entre eux n'ont été officialisés sous la forme de collèges superviseurs que dans les années qui ont précédé la crise financière mondiale (de 2008), et cette tendance s'est accélérée par la suite. Les collèges sont désormais une composante importante de la surveillance efficace d'un groupe bancaire international et le G20 a renforcé l'importance des collèges dans le sillage de la crise financière.**

Comité de Bâle, juin 2014[90]

BAM a ainsi créé trois collèges de superviseurs qui traitent des questions de réglementation transfrontière de trois groupes marocains, y compris la cybersécurité qui prend au fil des années une importance croissante. À ce propos, il convient de noter qu'il existe un Groupe des superviseurs bancaires francophones (GSBF) qui compte 34 pays. Ce groupe réunit chaque année les superviseurs des pays membres et non membres du Comité de Bâle, afin de développer des relations étroites avec ce dernier.

La création du GSBF a pour vocation de favoriser la communication et le dialogue entre les superviseurs francophones et le Comité de Bâle. BAM a assuré la présidence du GSBF pendant deux ans (2020-2022), tandis que le secrétariat du groupe est assuré par l'Autorité de contrôle prudentiel et de résolution (ACPR) et siège donc à Paris.

Le partage d'information passe par deux comités BAM-DGSSI et BAM-RSSI qui se réunissent sur initiative de BAM ou en cas d'incident sur demande de l'établissement de crédit concerné. Ainsi, quand la banque centrale a émis sa directive sur le cloud computing, elle a réuni le groupe RSSI pour expliquer les implications pratiques de son application. Il existe aussi des rencontres bilatérales quand un établissement a des questions particulières sur une thématique qui lui est propre.

**90** *"Principles for effective supervisory colleges", Basel Committee on Banking Supervision, juin 2014, 26 pages. Cf. p. 1.*

BAM est actuellement en passe de mettre la dernière main à la création d'une Communauté de cybersécurité bancaire - les banques ont déjà approuvé le projet de charte. Cette communauté va traiter du partage de l'information et non de gestion des incidents. Le partage d'information porte généralement sur des données publiques, tandis que la gestion des incidents est par nature confidentielle, comme c'est le cas dans le Comité BAM-RSSI. Les deux structures vont se compléter. La communauté se concentrera sur les échanges de bonnes pratiques, le renforcement des capacités, l'organisation d'événements conjoints, etc.

BAM entreprend également des activités de sensibilisation du public. C'est ainsi que la banque a publié en mars 2023 un guide bilingue français-arabe intitulé "Pour un usage sécurisé des services bancaires en ligne" qui contient toutes les bonnes pratiques à adopter, notamment comment se protéger du phishing, la nécessité de mettre à niveau les applications, l'importance de notifier l'opérateur en cas de vol, etc. Le guide fait partie d'une action continue de BAM auprès des membres pour les inciter à organiser des campagnes de sensibilisation à leur niveau.

### • *Surveillance des risques*

La base du travail de surveillance des risques de BAM consiste à exercer une veille et une compilation des cyberincidents pour identifier les facteurs émergents de cyberattaques et formuler des recommandations destinées à atténuer le risque cyber. Le groupe des projets digitaux établit un benchmark international sur l'ensemble des événements identifiés par les banques centrales.

Une étude documentaire est aussi faite en matière de cybersécurité à partir des rapports annuels d'organismes tels que IBM Security, Ponemon Institute, Sophos, Crowdstrike ou encore le rapport d'activités de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Il en résulte un panorama mondial de la cybersécurité qui identifie les principaux vecteurs d'attaques non seulement dans le secteur financier mais, en raison du risque de contagion, dans toutes les infrastructures d'importance vitale.

> **À la suite de la crise du Covid, BAM a noté une recrudescence du rançongiciel qui est la première source de criminalité, mais aussi du phishing, du sabotage et de l'espionnage informatique. Nous menons une réflexion pour démultiplier notre capacité d'intervention.**
>
> Karima Fatmi, Chargée du suivi des risques technologiques et cybersécurité, BAM, 2023.

En 2021, BAM a mis en place un référentiel d'évaluation de la cyber-résilience des banques commerciales sous forme d'enquête d'auto-évaluation de la maturité basée sur la méthodologie CROE (Cyber Resilience Oversight Expectations for Financial Market infrastructures) mise au point par la Banque centrale européenne. Chaque rapport d'enquête est accompagné de pièces justificatives pour étayer les notes attribuées.

Cette autoévaluation a lieu tous les deux ans[91]. Elle permet aux banques, dans un premier temps, d'identifier leur surface d'exposition aux risques cyber et, dans un deuxième temps, d'évaluer leur maturité en termes de niveau de sécurité du système d'information. Les conclusions qui en ressortent font état d'une maîtrise du risque globalement satisfaisante. Quand il y a une anomalie, une réunion bilatérale a lieu avec l'établissement concerné pour mettre au point un plan d'amélioration.

Le benchmark effectué à ce propos constitue un panorama fidèle de la cybersécurité du secteur bancaire marocain. Cela permet à chaque établissement de se comparer avec la moyenne sectorielle ou uniquement avec les autres établissements qui ont les mêmes activités qu'eux-mêmes - ce qu'on appelle les groupes homogènes.

**91** *L'autre année, la DGSSI procède à une enquête de type NCRA (National Cyber Risk Assessment) en coopération avec le gouvernement du Royaume-Uni.*

# 5 DISCUSSION SUR DEUX EXEMPLES DE RÉGLEMENTATION NATIONALE

• *Pilier renforcement des capacités*

BAM a conclu des mémorandums d'entente (MOU) avec la plupart des régulateurs africains où sont implantées les banques marocaines. Si un régulateur veut effectuer une mission de contrôle avec une banque marocaine, il peut faire appel aux services de BAM pour organiser une mission conjointe. Il n'existe pas encore de collaboration formelle et étroite entre BAM et les banques centrales africaines sur les sujets de cybersécurité.

En revanche, BAM a des relations suivies avec les régulateurs mondiaux à l'instar de l'European Banking Authority (EBA) ou l'Autorité de Contrôle Prudentiel et de Résolution (ACPR). BAM a aussi commencé à travailler avec la Banque du Canada sur le dossier des monnaies numériques de banque centrale (MNBC).

Dans cet esprit, BAM a mis au point un programme de coopération avec la Banque d'Angleterre sur la cybersécurité. Dans le cadre de ce programme, un atelier a été organisé en novembre 2022 avec la participation de représentants de 20 banques centrales d'Afrique et du Moyen-Orient. Plusieurs thèmes ont été abordés en matière de cyber-protection, cyber-gouvernance et cyber-résilience. L'atelier a remporté un tel succès qu'il a été décidé de mettre en place un réseau d'échange virtuel portant sur l'ensemble des thématiques liées à la cybersécurité.

## 5.2 - Cas de la Banque du Canada : Réduire les risques et renforcer la résilience

Au Canada, on estime que 78 % de la population accèdent aux services bancaires par Internet ou depuis leur téléphone mobile. Par la force des choses, les banques canadiennes ont dû investir massivement dans les mesures de prévention pour protéger le système financier ainsi que les renseignements personnels de leurs clients. Au cours de la période 2009-2019, elles ont investi 100 milliards de dollars en technologie, ce qui comprend les plateformes numériques pour mettre les services en ligne et les solutions technologiques destinées aux mesures de cybersécurité.[92]

Une telle activité exige un encadrement. Au Canada, le secteur bancaire est placé sous l'autorité du gouvernement fédéral et du Centre canadien pour la cybersécurité. À ce titre, les banques doivent mettre en œuvre efficacement la Stratégie nationale de cybersécurité du gouvernement canadien et atteindre l'objectif commun de créer un environnement en ligne plus résilient et plus sécuritaire pour les particuliers et les entreprises. Mais les banques ont aussi leur propre cadre réglementaire spécialisé.

Contrairement à d'autres banques centrales, la Banque du Canada ne réglemente ni ne supervise les banques canadiennes. Cette responsabilité relève du Bureau du surintendant des institutions financières (BSIF).

Toutefois, la Banque du Canada est chargée de la surveillance réglementaire des infrastructures désignées des marchés financiers (systèmes de paiement d'importance systémique et systèmes de compensation et de règlement). Sous peu, elle sera également responsable de la supervision des prestataires de services de paiement.

**Un régulateur distinct**

Le Bureau du surintendant des institutions financières (BSIF) est un organisme indépendant du gouvernement du Canada, créé en 1987 pour assurer la sécurité et la solidité du système financier canadien. Le BSIF supervise et réglemente les banques et les assureurs enregistrés au niveau fédéral, les sociétés de fiducie et de prêt, ainsi que les régimes de retraite privés soumis à la surveillance fédérale.

**92** *Fiche info-banques et cybersécurité, Association des banquiers canadiens, 5 avril 2022.*

## • *Le parcours de la Banque du Canada en matière de cybersécurité*

Afin de mener à bien sa mission, la Banque du Canada a créé en 2018 le poste de chef de la sécurité de l'information (RSSI) qui a pour mission d'harmoniser et de coordonner les activités de cybersécurité, au sein de la Banque comme à l' extérieur. La même année, la Banque a conclu un partenariat formel nommé Programme de résilience du système de paiement de gros (RSPG) avec Paiements Canada et les six grandes banques canadiennes pour favoriser la continuité des opérations. Paiements Canada est un organisme sans but lucratif qui exploite l'infrastructure de compensation et de règlement des paiements du Canada.

La Banque du Canada lance en 2019 le Groupe sur la résilience du secteur financier canadien (GRSF) qui a une double mission: favoriser le partage d'information et, au-delà, coordonner l'intervention de l'ensemble du secteur bancaire en cas d'incident opérationnel systémique. Ce Groupe est un partenariat public-privé qui comprend tous les intervenants majeurs du secteur, à savoir le ministère des Finances, le Bureau du surintendant des institutions financières (BSIF), les six grandes banques ainsi que les systèmes de paiement, de compensation et de règlement (comme Virement Interac, par exemple).

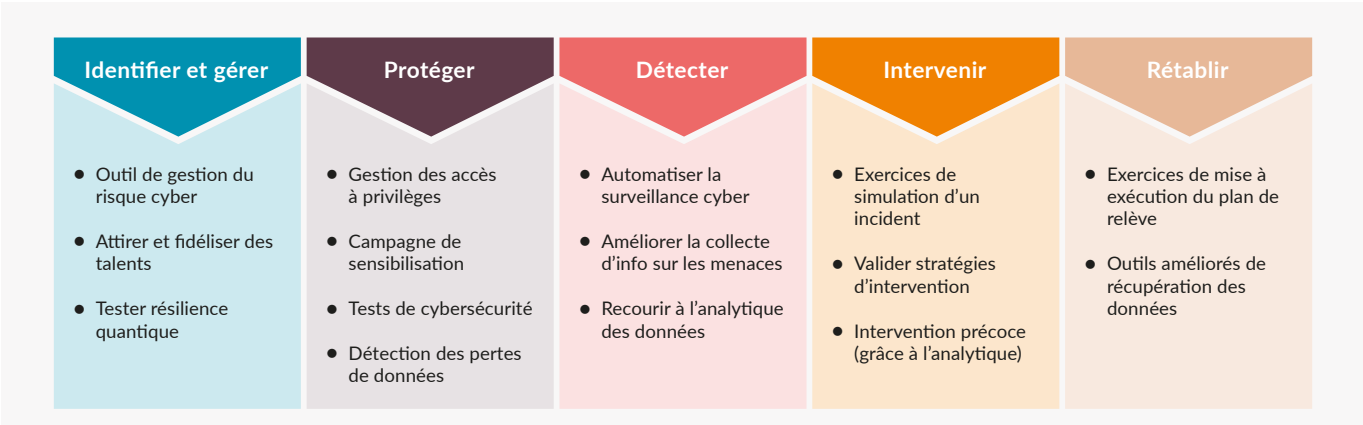
Typiquement, la Banque du Canada procède à des tests de sécurité pour détecter les vulnérabilités au sein du personnel, des systèmes et des processus, afin d'y remédier. Un programme de sensibilisation des utilisateurs a été mis sur pied afin d'informer les utilisateurs réguliers ou privilégiés des systèmes de la Banque au sujet des risques liés à leur travail, y compris l'hameçonnage (phishing) et le vol d'identité.

## • *Stratégie de cybersécurité de la Banque du Canada*

Toutes ces mesures de protection adoptées au fil des années ne suffisaient pas, c'est pourquoi en 2019 la Banque a mis au point sa première Stratégie de cybersécurité. Actuellement, une deuxième Stratégie de cybersécurité a été émise qui couvre la période 2022-2024. Bien que les deux stratégies suivent le même canevas, la deuxième version a été élargie pour tenir compte de l'évolution de l'environnement du risque cyber, à savoir la propagation du télétravail subséquente à la crise du Covid et la montée des cybermenaces d'États-nations.

Les nouvelles cybermenaces sont également liées à l'évolution des activités et des processus de banque centrale, comme les systèmes de paiement actualisés, la monnaie numérique, la technologie de chaîne de blocs et la numérisation croissante de tous les services financiers. Les objectifs internes de la stratégie de la Banque du Canada ont été définis en fonction des cinq paramètres de la méthodologie du National Institute of Standards and Technology (NIST) qui est une agence du département du Commerce des États-Unis.

**FIGURE 18 -** OBJECTIFS INTERNES DE LA STRATÉGIE DE CYBERSÉCURITÉ DE LA BANQUE DU CANADA



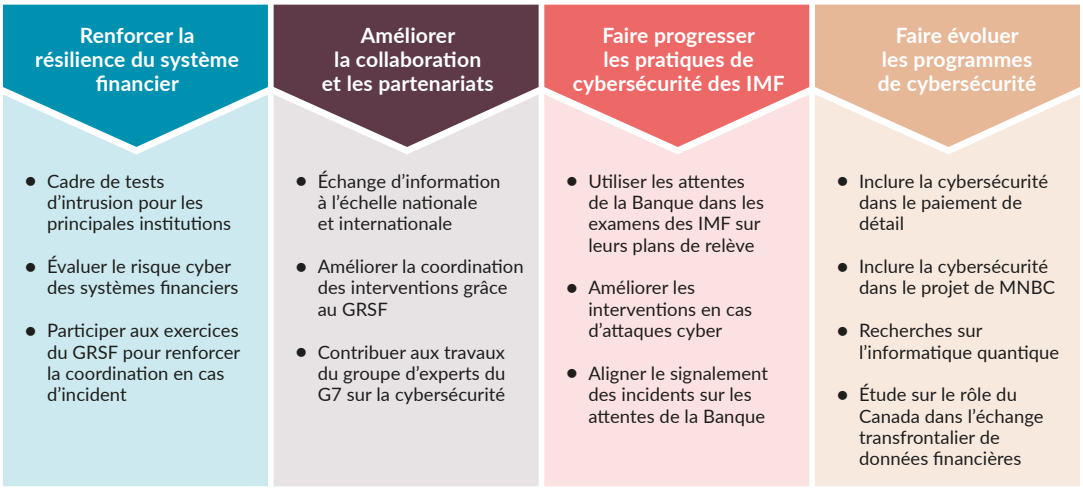
# 5 DISCUSSION SUR DEUX EXEMPLES DE RÉGLEMENTATION NATIONALE

À l'externe, la Banque a collaboré avec des partenaires canadiens et internationaux des secteurs public et privé pour renforcer la cybersécurité des systèmes financiers nationaux et mondiaux. Son action prend appui, en particulier, sur deux partenariats importants de la Banque qui sont le Groupe de résilience du secteur financier canadien (GRSFC) et le Programme de résilience du système de paiement de gros (RSPG) examiné ci-dessus.

Dans un document intitulé Cyber-résilience : attentes à l'égard des infrastructures de marchés financiers, la Banque a publié en 2021 de nouvelles lignes directrices qui viennent préciser et compléter la réglementation en vigueur au Canada et qui sont elles-mêmes inspirées des principales normes internationales (méthodologie NIST, norme ISO/IEC 27001/27002 et référentiel COBIT 2019). La Stratégie de cybersécurité 2022-2024 distingue quatre priorités qui visent à mieux aligner les pratiques des infrastructures de marchés financiers (IMF) sur ces nouvelles lignes directrices.

Au demeurant, les activités de cybersécurité internes et externes de la Banque sont de plus en plus interreliées, particulièrement dans le cas des systèmes essentiels, comme les systèmes de compensation et de règlement des paiements, d'adjudication des titres et de gestion des réserves de change. La sécurité interne de la Banque du Canada se confond en grande partie avec la sécurité de l'ensemble des IMF, voire du système financier international. Il faut considérer les priorités externes comme indissociables des priorités internes.

**FIGURE 19 -** OBJECTIFS EXTERNES DE LA STRATÉGIE DE CYBERSÉCURITÉ DE LA BANQUE DU CANADA




D'une façon générale, la Banque du Canada mettra davantage l'accent sur le modèle « confiance zéro » (Zero Trust) pour la cyberdéfense, qui part du principe que tous les appareils connectés comportent un certain risque, même au sein de réseaux sécurisés. La Banque travaillera également avec des partenaires des secteurs public et privé pour se préparer à la nouvelle ère de l'informatique quantique. Répondre au marché concurrentiel des talents en cybersécurité demeure une priorité. À cette fin, la Banque vise à offrir aux spécialistes en cybersécurité les meilleures conditions de travail sur le marché et à mettre à leur disposition un programme de formation et de perfectionnement continus des compétences.

> Au Canada, la politique macroprudentielle est une responsabilité partagée entre différentes autorités. Pour sa part, la Banque fournit des analyses et des conseils afin d'identifier et d'atténuer les risques systémiques susceptibles d'entraver le fonctionnement du système financier.
>
> Rebecca Spence, porte-parole, Banque du Canada

## *Rôle de l'autorité de réglement*

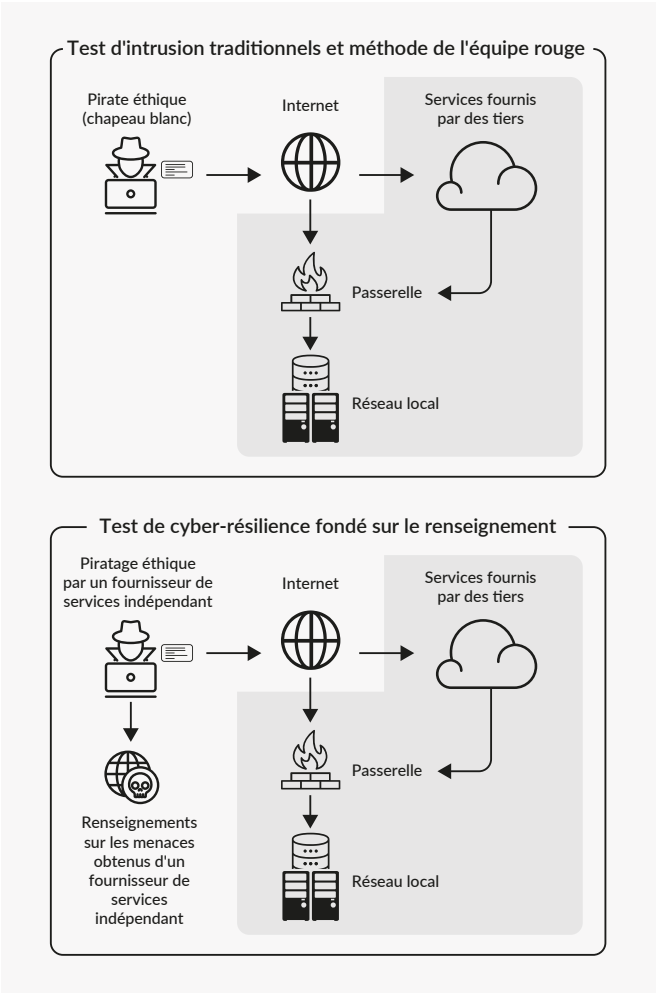
L'autorité réglementaire à proprement parler du secteur financier est assurée par le Bureau du surintendant des institutions financières (BSIF). Par l'intermédiaire de sa ligne directrice B-13 intitulée "Gestion des risques technologiques et cybernétiques", le BSIF définit les attentes en matière de résilience à l'égard de toutes les institutions financières fédérales (IFF), ce qui comprend plus de 400 institutions financières et 1 200 régimes de retraite fédéraux.

Un préavis sur le Signalement des incidents liés à la technologie et à la cybersécurité publié en août 2021 précise les exigences régissant la façon dont les IFF signalent au BSIF les incidents (délai de notification de 24 heures au maximum). Si une institution omet de signaler un incident, elle s'expose à une surveillance accrue, notamment des activités de suivi renforcées, une inscription à la liste de surveillance ou son classement à un stade d'intervention.

En avril 2023, le BSIF rendait publique une "Ligne directrice sur la gestion des risques liés aux tiers" qui mettait à jour l'ancienne ligne directrice B-10. Cette mise à jour assujettit à toute fin pratique les fournisseurs des banques, y compris les fintechs, aux mêmes règles que le reste du secteur financier. À cette fin, chaque entente conclue par une banque avec une fintech doit être soumise au BSIF, à la demande de celui-ci. Un service financier offert par le truchement d'une fintech doit pouvoir être supervisé par le BSIf exactement comme s'il était offert directement par la banque.

Le BSIF a publié au même moment un cadre permettant aux IFF d'effectuer des évaluations renforcées grâce à l'utilisation des Tests de cyber-résilience fondée sur le renseignement (TCFR). Le TCFR diffère du test d'intrusion classique car le pirate éthique met à profit les renseignements précis sur les menaces ciblées qui pèsent sur l'institution évaluée. Il peut alors simuler en toute connaissance de cause les tactiques, les techniques et les procédures les plus sophistiquées employées sur le marché du crime. L'inclusion d'information sur cible fait en sorte que l'évaluation du TCFR soit très réaliste.

**FIGURE 20 -** TEST D'INTRUSION TRADITIONNEL ET TCFR




*Source : Bureau du surintendant des institutions financières (BSIF).*

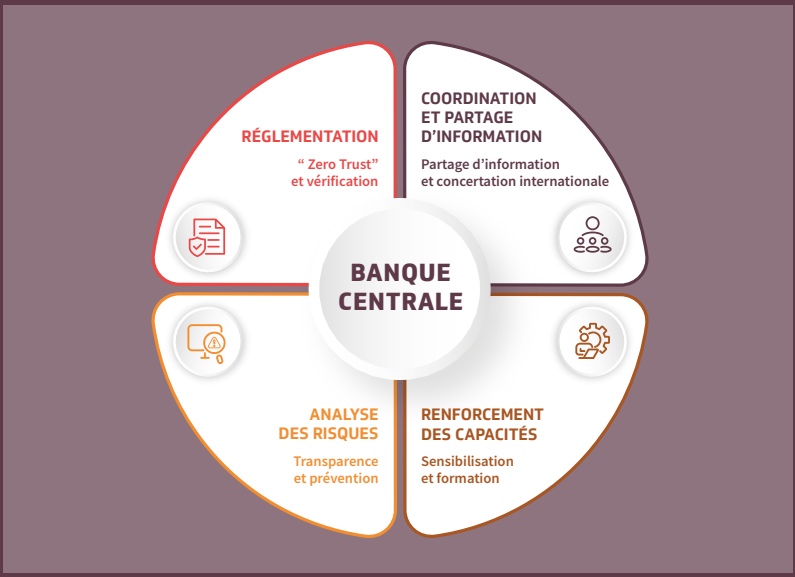
Au total, on peut dire que le niveau de contrôle de la réglementation bancaire canadienne est assez élevé. Cette implication des régulateurs canadiens dans les activités quotidiennes des banques est rendue possible par la concentration du secteur. Le Canada ne compte que 28 banques nationales, dont six sont vraiment importantes (Toronto Dominion, Banque Royale du Canada, Banque de Nouvelle-Écosse, Banque de Montréal, Banque Canadienne Impériale de Commerce et Banque Nationale du Canada).

# 6

# CONCLUSIONS ET MEILLEURES PRATIQUES

Aux fins de ce chapitre de conclusion, nous avons repris la typologie de la banque centrale marocaine pour définir les quatre fonctions de l'action réglementaire et d'accompagnement qui régissent le secteur bancaire (voir figure 24 - Les grands vecteurs d'action des banques centrales). Cela ne préjuge en rien de la nature de nos conclusions qui sont basées sur une étude en profondeur de la littérature scientifique (voir annexe 1 - Bibliographie choisie) ainsi qu'avec des interviews non seulement avec des représentants de la banque centrale marocaine, mais aussi de la banque centrale canadienne.

**FIGURE 21 - LES GRANDS VECTEURS D'ACTION DES BANQUES CENTRALES**




Une idée force se dégage de ce tour d'horizon qui est la nécessité de dépasser le paradigme de la cybersécurité trop lié à son soubassement technologique et territorial au profit de celui de cyber-résilience qui englobe l'écosystème bancaire dans son ensemble et met de l'avant la notion de "confiance zéro" (Zero Trust). Nous avons ainsi essayé de dégager des meilleures pratiques qui gagneraient à être incorporées sous une forme ou l'autre dans la feuille de route du secteur bancaire.

Ces meilleures pratiques ont été énoncées sous forme de principes, dont bon nombre sont déjà implantés dans le secteur bancaire africain. D'autres peuvent sembler inapplicables tels quels et nous en sommes bien conscients. Le but de ces conclusions se limite à favoriser un dialogue fructueux entre le secteur bancaire et celui des prestataires de services de cybersécurité. Quand nous utilisons le vocable "banque centrale" ici, nous nous référons aussi à l'autorité de régulation financière quand celle-ci est distincte. Pour ne pas alourdir inutilement la phrase, nous parlons uniquement de banque centrale.

# 6 CONCLUSIONS ET MEILLEURES PRATIQUES

## 6.1 - Pilier Réglementation

### *Principe 1 : Cyber-résilience du secteur financier*

Alors que les principes réglementaires nationaux et internationaux sont généralement connus des responsables des banques centrales africaines, les implications pratiques sont souvent ignorées par la communauté financière. Pour que toutes les entités supervisées et connexes du secteur bancaire aient la même compréhension du cadre réglementaire que le régulateur, il est souhaitable que dans chaque pays la banque centrale publie les lignes directrices opérationnelles et les attentes en matière de cyber-résilience en tenant compte des exigences internationales, mais en les adaptant au contexte local.

**→ Les meilleures pratiques consistent pour la banque centrale à publier les lignes directrices opérationnelles et les attentes en matière de cyber-résilience en tenant compte des exigences internationales, mais en les adaptant au contexte local.**

### *Principe 2 : Nécessité de garantir la cyber-résilience*

Le respect de la réglementation ne suffit pas à garantir la cyber-résilience. Les entités du secteur financier doivent généralement administrer chaque année un test de résilience opérationnelle numérique qui comprend une série d'évaluations et analyses de la vulnérabilité, analyses des sources ouvertes, évaluations de la sécurité des réseaux, analyses des lacunes, examens de la sécurité physique, questionnaires et solutions logicielles d'analyse, examens du code source lorsque cela est possible, tests fondés sur des scénarios, tests de compatibilité, tests de performance ou tests de bout en bout.

Pour les entités d'importance systémique, il faut pousser la garantie un cran plus haut et procéder à des tests d'intrusion fondés sur la menace de type TLPT (aussi appelés tests d'intrusion Red Team).[93] Il s'agit d'une tentative contrôlée pour compromettre la cyber-résilience d'une entité financière en simulant les tactiques, techniques et procédures d'acteurs réels de la menace. Cette procédure nécessite une grande préparation et doit impérativement être administrée par une tierce partie. Les tests de pénétration fondés sur la menace sont un concept déjà appliqué dans plusieurs pays d'Europe et d'Asie et devront être effectués au moins tous les trois ans.

**→ Pour respecter les meilleures pratiques, les banques systémiques devraient procéder régulièrement à des tests de pénétration guidés par la menace (aussi appelés tests d'intrusion Red Team).**

### *Principe 3 : Convergence panafricaine des réglementations*

Chaque banque centrale a intérêt à accorder sa réglementation et ses meilleures pratiques avec celles des autres banques centrales pour éviter de plonger les banques commerciales et entités connexes qui ont des activités transnationales, dans un imbroglio opérationnel. Chaque fois que le cadre réglementaire national est amené à évoluer, une concertation panafricaine devrait être prévue.

À cette fin, il serait intéressant de vérifier la possibilité de recourir aux services de l'Association des banques centrales africaines (ABCA) pour partager les documents de travail réglementaires et consultatifs avant leur entrée en vigueur. Le cas échéant, il sera aussi possible d'utiliser d'autres structures de concertation comme le Conseil de stabilité financière, le Comité sur les paiements et les infrastructures de marché et le Comité de Bâle.

**→ Établir une plateforme de consultation permettant à chaque banque centrale d'accorder sa réglementation et ses meilleures pratiques avec celles des autres banques centrales en utilisant les organisations internationales existantes.**

*93 "Threat-Led Penetration Testing (TLPT). Les tests de pénétration basés sur les menaces consistent essentiellement à utiliser les renseignements sur les menaces pour imiter les tactiques, techniques et procédures d'un adversaire.*

## 6.2 - Pilier Surveillance des Risques

### *Principe 4 : Surveillance et mise en place d'un SOC*

Toute banque a pour objectif de prévenir les incidents de cybersécurité et, quand ils surviennent malgré tout, de les contenir. Pour cela, il est nécessaire de formaliser le traitement des incidents depuis leur détection jusqu'à leur traitement et centraliser les processus de façon à avoir une visibilité globale de la situation en temps réel. L'outil capable de satisfaire à ce double objectif est le centre d'opérations et de sécurité ou SOC.

Le SOC a pour fonction d'exercer une surveillance efficace sur un périmètre informatique déterminé et un suivi des incidents de bout en bout. Il transforme les données brutes qui sont générées par l'équipement informatique, s'il y a lieu, sous forme de notifications d'alertes. Le SOC prévient alors le CSIRT du danger en cours et c'est ce dernier qui procède au traitement de l'alerte et à la restauration du système attaqué. Quand tout est terminé, la banque est alors en mesure de faire un rapport détaillé à l'intention de l'autorité nationale.

La banque centrale a tout intérêt à ce que les banques commerciales à importance systémique se dotent d'un SOC interne ou externe (par voie de sous-traitance). Cette exigence est particulièrement appropriée car elle aidera les banques à se conformer à un cadre réglementaire de plus en plus complexe et contraignant (Accords de Bâle III, SWIFT, PCI-DSS…).

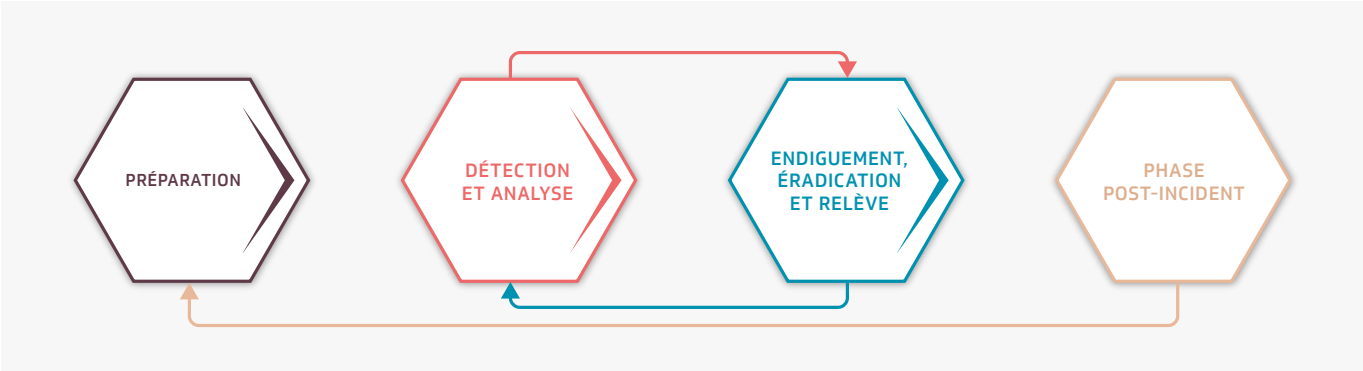
→ Inciter les banques commerciales d'importance systémique à se doter d'un SOC interne ou externe (par voie de sous-traitance).

### *Principe 5 : Plan d'intervention en cas de cyberincident*

Les instances de réglementation internationales, BRI, Banque mondiale, FMI…) préconisent que toute banque centrale prépare à ses propres fins toute une série de scénarios de cybercrises plausibles, y compris les plus extrêmes. À partir de cette hypothèse de travail, les banques centrales devraient développer un plan de réponse aux cyberincidents ou plan de continuité.[94]

Or, les banques commerciales ont souvent de la difficulté à produire de tels plans d'intervention pour les incidents. Dans de nombreux cas, il leur manque une compréhension pratique sur la manière dont ces plans doivent être mis en œuvre en cas d'incident de façon à être efficaces, appliqués de manière homogène d'un département à l'autre, tout en demeurant conforme au cadre réglementaire.

**FIGURE 22 -** CYCLE D'INTERVENTION EN CAS D'INCIDENT




*Source : "Computer Security Incident Handling Guide", NIST, 2012.*

**94** *"Cyber Resilience for Financial Market Infrastructures" World Bank, novembre 2019, 42 pages. - "Principles for Operational Resilience", Basel Committee on Banking Supervision, mars 2021, 8 pages.*

# 6 CONCLUSIONS ET MEILLEURES PRATIQUES

Voilà pourquoi, il serait souhaitable que la banque centrale produise un modèle générique de plan d'intervention en cas d'incidents, neutre sur le plan technologique. Ce plan à l'intention des banques commerciales et entités connexes, permettra à ces dernières de mieux comprendre comment mettre en œuvre les mesures de cyber-résilience appropriées, y compris les protocoles de tests à répéter régulièrement.

→ Mise au point par la banque centrale d'un modèle générique de plan d'intervention en cas d'incidents à l'intention des banques commerciales et entités connexes.

## *Principe 6 : Notification obligatoire des incidents*

Pas de gestion des risques sans connaissance en temps réel des incidents dont sont victimes les banques. Il est donc prioritaire pour toutes les banques centrales d'adopter un régime formel de notification obligatoire concernant les cyber-attaques.

Tout incident de cybersécurité doit être notifié dans un délai de 60 minutes à compter du moment où il se produit, en incluant autant d'informations que possible. Une fois l'incident maîtrisé, un rapport doit être établi, comprenant un ensemble élargi d'informations qui devront être énumérées dans le règlement de notification obligatoire.

Les clients et les utilisateurs doivent être informés et tenus au courant, mais uniquement si l'incident affecte la continuité ou la qualité du service, ou s'il est de notoriété publique.

→ Notification obligatoire de tout incident cyber à la banque centrale dans un délai de 60 minutes à compter du moment où il se produit.

## *Principe 7 : Cartographie et quantification des risques*

Le secteur bancaire est une industrie réseautée et chaque entité financière est tributaire de la bonne santé cybersécuritaire de toute une série d'autres entités. En effet, nombre de ces entités dépendent des mêmes fournisseurs de services: opérateurs de services en nuage, prestataires de cybersécurité ou de matériel informatique, etc. Un tiers peut ainsi devenir un acteur systémique du secteur financier dès lors que ses services ou produits sont utilisés par de nombreuses entités.

Il est donc recommandé de cartographier les principales interconnexions opérationnelles et technologiques de chaque banque, y compris de la banque centrale. L'ensemble de ces exercices de cartographie sera recueilli et compilé au niveau de la banque centrale qui bénéficiera ainsi d'un panorama complet des interdépendances du système financier national.

→ Production par chaque banque d'une cartographie détaillée de l'ensemble de ses interconnexions opérationnelles et technologiques et, à partir de cette base, production par la banque centrale d'une cartographie sectorielle.

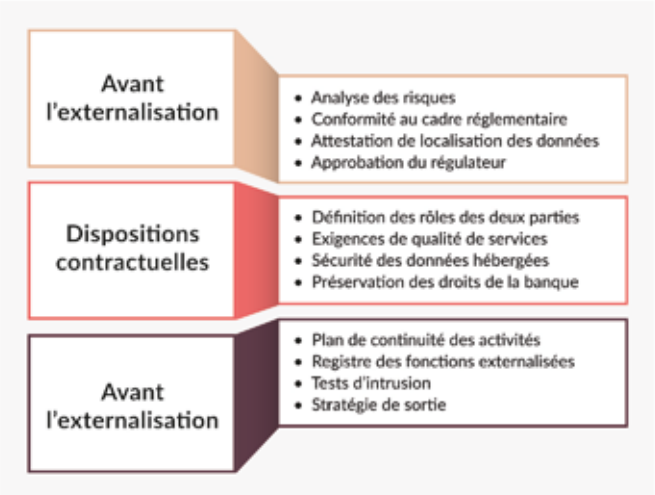
## *Principe 8 : Produire un référentiel sur l'utilisation du nuage (cloud)*

La multiplication des services financiers hébergés dans le nuage a un impact direct sur la stratégie de cybersécurité de l'organisation. En effet, en externalisant plusieurs de ses processus essentiels, une organisation perd une partie de sa visibilité et de son contrôle sur son propre système d'information. Il s'agit désormais d'une responsabilité partagée entre l'organisation et l'opérateur de services infonuagiques.

Dans le secteur hautement réglementé des banques, cela implique une extension du domaine réglementaire. Au Maroc, le régulateur du secteur financier, Bank Al-Maghrib a émis une directive en mai 2022 qui stipule que toute externalisation vers le nuage respecte les lois et réglementations auxquelles est assujettie la banque en question.[95] Avant même de procéder à l'externalisation, la banque doit procéder à une analyse des risques, vérifier la conformité de l'opérateur par rapport au cadre réglementaire et, finalement, obtenir l'accord préalable du régulateur.

L'hébergement lui-même sur le nuage doit être encadré par un contrat d'externalisation qui définit les rôles précis des deux parties, les exigences de qualité des services infonuagiques, la sécurité des données hébergées et le maintien des droits de la banque sur celles-ci. L'engagement ne prend fin qu'avec la sortie du nuage qui doit être prévue dans un stratégie documentée et cohérente.

**FIGURE 23 -** MODÈLE DE RÉFÉRENTIEL SUR LE RECOURS AU NUAGE




*Source : Interprétation schématique des prescriptions de la directive sur le nuage de BAM, 2022.*

→ Publication par les banques centrales d'un référentiel détaillé encadrant les modalités d'externalisation des institutions financières vers le nuage (cloud). Le cœur de ce référentiel pourrait être constitué par un contrat-type entre la banque et l'opérateur de services infonuagiques.

## *Principe 9 : Effectuer un cyber stress test*

Les banques centrales sont habituées à soumettre les grandes banques commerciales à des stress tests, spécialement depuis la crise financière de 2008. La finalité des stress tests est d'étudier le comportement des banques dans un environnement adverse afin d'évaluer leur résistance face à une dégradation prononcée de l'environnement macro-économique et financier.

C'est sans doute la Banque d'Angleterre qui en 2021 a appliqué pour la première fois le concept du stress test au contexte de la cybersécurité. Il s'agissait de modéliser l'impact d'une cyberattaque sur le système de paiement. La BCE a suivi cet exemple et se trouve à présent en train d'élaborer un scénario impliquant une violation théorique des cyberdéfenses du système financier européen afin d'évaluer la manière dont les banques réagiraient.[96]

Il est souhaitable que les banques centrales africaines procèdent également à un stress test cyber, de préférence en se regroupant sur une base régionale ou même continentale. En outre, il semble que la BCE ait l'intention de convier des banques africaines à son premier stress tests cyber qui devrait se tenir au milieu de 2024. Il convient d'encourager les banques centrales africaines à profiter de cette occasion.

→ Les banques centrales africaines pourraient organiser un stress test cyber à l'intention des établissements systémiques sous leur autorité, sur le modèle de la Banque d'Angleterre ou de la BCE.

*95 "Directive fixant les règles minimales en matière d'externalisation vers le cloud par les établissements de crédit", Bank Al-Maghrib, 19 mai 2022.*
*96 Martin Arnold, "ECB tells banks to run cyber stress tests after rise in hacker attacks", Financial Times, 9 mars 2023.*

# 6 CONCLUSIONS ET MEILLEURES PRATIQUES

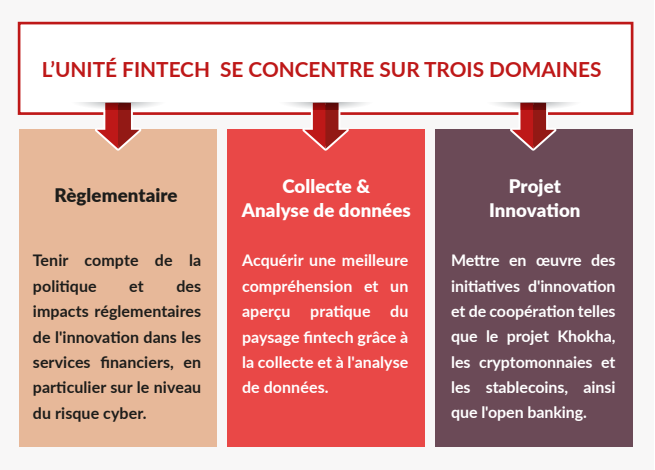
## *Principe 10 : Unité interne de fintech*

Il est souhaitable que la banque centrale crée une unité interne de fintech dans les pays où l'activité du secteur financier le justifie - en partant les quatre pays qui regroupent la majeure partie des fintechs africaines: Nigéria, Afrique du Sud, Kenya, Égypte (voir 2.3 - La déferlante des fintechs).

La mission d'une telle unité administrative serait d'explorer les implications de l'innovation fintech pour la banque centrale ainsi que l'ensemble de l'écosystème, en particulier en matière du niveau de risque cyber. Un modèle intéressant est offert par la South African Reserve Bank (SARB) qui a créé sa propre unité interne de fintech en août 2017.[97]

→ Dans les pays où l'activité du secteur financier le justifie, création par la banque centrale d'une unité interne de fintech.

**FIGURE 24 -** OBJECTIFS DE L'UNITÉ INTERNE DE FINTECH DE LA BANQUE CENTRALE D'AFRIQUE DU SUD




*Source : SARB (notre traduction).*

## 6.3 - Pilier Coordination et échange d'information

Au cœur de la transition de la banque centrale vers la cyber-résilience se trouve la coordination et l'échange d'information. Il s'agit dans un premier temps de mobiliser l'ensemble des départements de l'institution financière, puis d'étendre cette discipline à la chaîne logistique (sous-traitants), au secteur financier dans son ensemble, ce qui inclut les fintechs et enfin d'harmoniser l'action réglementaire avec celle des autres banques centrales africaines pour éviter la création d'un imbroglio de juridictions contradictoires.

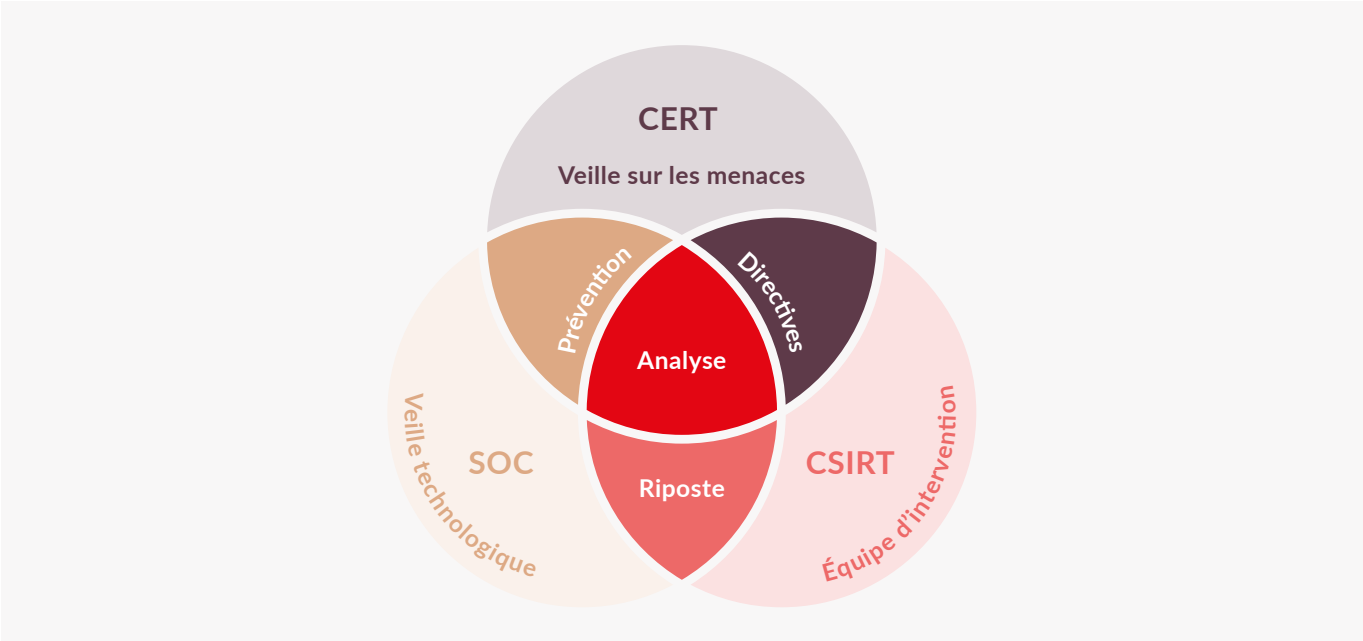
> Il faut toujours avoir présent à l'esprit que les cybercriminels se concertent entre eux pour commettre leurs méfaits, ils partagent des outils, des processus et des données personnelles qu'ils ont volés. Le tout se retrouve sur le web invisible où des millions de dollars circulent en permanence. Pour demeurer en amont de cette menace en constante évolution, il faut faire la même chose qu'eux !
>
> Fred Bedrich, Banque de développement du Canada (BDC), 2019

## *Principe 11 : Création d'un CERT financier*

À la base de tout dispositif de partage de l'information, il convient de prévoir un outil pour analyser et qualifier l'information. Tel est précisément le rôle du Computer Emergency Response Team (CERT). Tout processus de cybersécurité a trois fonctions: effectuer une activité de veille, assurer la cyber-surveillance et offrir une réponse aux incidents de sécurité (forensic).

**97** *Source: Page web fintech de la SARB: https://www.resbank.co.za/en/home/quick-links/fintech*

**FIGURE 25 -** PLACE DU CERT DANS LA CYBERSÉCURITÉ




*Source : Dataprotect, 2023*

Pour coordonner les mesures préventives et les interventions en cas d'incident sur le territoire national, plusieurs pays africains ont créé des CERT ou des CSIRT nationaux (voir 4.1 - L'approche politique, section Stratégie nationale de cybersécurité). Comme ils sont extérieurs au secteur financier, ces organismes n'ont qu'une expertise limitée pour veiller sur les actifs informationnels et technologiques des banques. Par la force des choses, ils se concentrent sur l'analyse générale des menaces et des incidents ainsi que d'autres formes de soutien indirect.

Voilà pourquoi, il est recommandé que soit créé un CERT sectoriel en matière bancaire ou finCERT. On a vu que les banques tunisiennes s'étaient dotées d'un tel outil pour protéger leurs infrastructures critiques via leur association spécialisée (Conseil bancaire et financier). Il n'existe pas de telles associations dans tous les pays. Voilà pourquoi, les banques centrales gagneraient à se doter de finCERT qui veilleraient sur leurs actifs informationnels propres ainsi que sur ceux des banques soumises à leur autorité.

Un des modèles les plus achevés de finCERT est indéniablement le Centre de continuité cyber et financière (FC3) mis au point en Israël par le ministère des Finances et la Direction nationale cyber. Grâce à une solide coordination avec l'ensemble du secteur financier, le FC3 a pu dresser une cartographie complète du secteur financier israélien afin d'en améliorer la résilience. Des synergies supplémentaires sont réalisées parce que FC3 a son siège sur un campus qui réunit des chercheurs universitaires et des experts militaires en cybersécurité.

Entre le modèle tunisien de finCERT entièrement privé et le modèle israélien entièrement étatique, il y le modèle italien de finCERT public-privé qui est dirigé conjointement par la Banque d'Italie et l'Association bancaire italienne. La participation au finCERT est ouverte et toute institution financière ou prestataire de services opérant dans le secteur financier italien peut s'y inscrire.[98]

Un finCERT est également un canal essentiel au partage de l'information technologique. En effet, la coopération et la coordination se font systématiquement entre les CERT nationaux, les CERT sectoriels et les CSIRT d'entreprises individuelles au niveau international par le biais du Forum of Incident Response and Security Teams (FIRST). On a vu que le CERT du CBF tunisien et le CSIRT de Dataprotect étaient tous deux accrédités FIRST.

**98** *"International Strategy to Better Protect the Financial System Against Cyber Threats", Carnegie Endowment for International Peace, 2020, 233 pages. Cf. p. 55-56.*

# 6 CONCLUSIONS ET MEILLEURES PRATIQUES

**→ Il est préconisé que la banque centrale en tant que leader du secteur financier ou, le cas échéant, qu'un regroupement structuré de banques commerciales, se dote d'un finCERT pour anticiper les incidents, coordonner la réponse en cas d'attaques et maintenir une base de données des vulnérabilités.**

## *Principe 12 : Partage d'information dans le secteur financier*

La mise en place d'un CERT ne se substitue pas à la constitution d'un groupe public-privé de partage et de coordination d'information en matière de cybersécurité sur une base nationale. Seule la banque centrale a l'autorité nécessaire pour piloter une telle initiative. En effet, le groupe devrait réunir les banques commerciales, les entités connexes (sous-traitants, fintechs, opérateurs de réseaux de paiement) ainsi que les représentants du ministère des Finances et de tout autre organisme public concerné.

Il doit être clair que le groupe de partage et de coordination d'information ne doit pas être une instance réglementaire et se substituer au pouvoir réglementaire qui relève de la seule banque centrale.

Le mandat du groupe public-privé de partage et de coordination d'information sur la cybersécurité a vocation à être double :

- Faciliter les initiatives visant à accroître la résilience opérationnelle du secteur financier en organisant des réunions régulières de partage d'information sur la situation en matière de cybersécurité ;
- En cas d'incident ou de crise systémique, échanger en temps réel l'information pertinente, discuter des moyens à prendre pour régler le problème et coordonner les interventions des différents acteurs du secteur financier.

Les travaux de chaque groupe national devront être formalisés et autant que possible automatisés. À cette fin, il serait souhaitable de recourir à une plateforme de connaissances spécialisées pour les cyber-risques et les innovations pouvant exercer un impact sur les systèmes d'information bancaires. La plateforme pourrait être créée en partenariat avec les universités et les entités connexes du secteur financier comme les fintechs et les prestataires de services de cybersécurité.

Pour maximiser l'impact des groupes nationaux de partage d'information, il importe de leur conférer une dimension continentale et internationale. Deux pistes de solution s'offrent alors aux banques centrales : l'Association des banques centrales africaines (ABCA) et la Banque des règlements internationaux (BRI) :

- Comme en Afrique chaque banque centrale est membre de l'ABCA, l'utilisation de cette structure associative permettrait d'organiser des réunions inter-groupes sur une base africaine et ainsi de continentaliser le partage d'information. En outre, le concours de l'ABCA permettrait de mettre à contribution l'expertise de ses partenaires (FRBNY et BCE).[99]
- Chaque groupe de partage et de coordination d'information gagnerait à travailler aussi avec le Cyber Resilience Coordination Centre (CRCC) de la BRI. Cette plateforme internationale offre une approche structurée (1) du partage des connaissances, (2) de la collaboration et (3) de la préparation opérationnelle entre les banques centrales dans tous les domaines de la cyber-résilience. Depuis janvier 2021, le CRCC est devenu une nouvelle unité d'affaires de la BRI, distincte de l'unité de sécurité de l'entreprise, afin de mieux se concentrer sur sa mission de base et d'accroître sa capacité à fournir des services à valeur ajoutée à ses interlocuteurs.[100]

**→ Les meilleures pratiques en matière de partage d'information passe par la création d'un groupe public-privé d'échange et de coordination d'information sur la cybersécurité qui comporte une dimension continentale et internationale. Dans la mesure du possible, chaque groupe devrait recourir à une plateforme de connaissances pour automatiser ses travaux.**

***99*** *Proposition extraite du "Projet de rapport sur les expériences et les initiatives des banques centrales membres de l'ABCA en matière de développement des fintech et de cybersécurité", Association des banques centrales africaines (ABCA), août 2019, 26 pages + annexes. Cf. p. 24.*
***100*** *BIS Annual report 2020-21, idem, p. 87.*

## 6.4 - Pilier Renforcement des Capacités

L'édition 2022 du Baromètre des risques du groupe d'assurance allemand Allianz classe la pénurie de talents qualifiés en technologies de l'information parmi les dix principaux risques auxquels sont confrontées les entreprises du monde entier. En Afrique, ce défi est exacerbé par le fait que 50 % des développeurs de logiciels africains sont basés dans cinq pays seulement (Afrique du Sud, Égypte, Kenya, Maroc, Nigéria), ce qui laisse le reste du continent dans un état de grande vulnérabilité. En outre, l'exode des cerveaux frappe particulièrement le secteur des technologies de l'information, à commencer par la cybersécurité.[101]

### *Principe 13 : Sensibilisation continue*

Il est indispensable de sensibiliser les utilisateurs aux différents types de risques encourus et aux parades les plus efficaces. La sensibilisation se distingue de la formation. En matière de cybersécurité, la formation est dispensée aux cyberspécialistes afin de les aider à ériger une infrastructure étanche autour des informations stratégiques de l'organisation. La sensibilisation, quant à elle, s'adresse à l'ensemble du personnel.

La sensibilisation vise à rendre une population réceptive à des thèmes souvent connus mais qu'elle a tendance à penser qu'ils ne la concernent pas. C'est une composante de la stratégie d'éducation d'une organisation qui tente de modifier le comportement et les pratiques de ses publics cibles (employés, cadres, direction, etc.). Son but est de modifier les comportements. Comme les activités de sensibilisation sont brèves, elles doivent être marquantes et répétées en continu.

Les banques centrales doivent veiller à ce que des campagnes de sensibilisation soient entreprises dans les banques commerciales ainsi que dans les entités connexes. Il existe des outils de sensibilisation à base de capsules vidéo qui permettent de transformer cette nécessité quelque peu rébarbative en une activité ludique. Reste à promouvoir la sensibilisation elle-même auprès des instances dirigeantes du secteur bancaire.
Les États-Unis observent le National Cyber Security Awareness Month (NCSAM) depuis 2004. Commandité par le Département de la Homeland Security et l'organisme sans but lucratif National Cyber Security Alliance (NCSA), l'événement vise à diffuser les meilleures pratiques auprès des utilisateurs de services en ligne. Depuis 2012, l'Union européenne a également consacré le mois d'octobre à la sensibilisation à la cybersécurité (European Cybersecurity Month).

Ne serait-il pas opportun que les banques centrales africaines fassent aussi d'octobre le mois de sensibilisation à la cybersécurité, de préférence dans le cadre de l'ABCA ? Chaque mois d'octobre pourrait ainsi être consacré à un thème qui serait abordé par l'ensemble du secteur financier africain. L'ABCA aurait ainsi le mandat de fixer chaque année un thème pour le mois africain de la sensibilisation à la cybersécurité dans le secteur bancaire.[102]

→ **Promouvoir l'organisation de campagnes de sensibilisation dans toutes les banques commerciales ainsi que dans les entités connexes et, à cette fin, proclamer le mois d'octobre comme mois de la sensibilisation à la cybersécurité à l'échelle africaine.**

***101*** *"Fintech in Africa: The end of the beginning", idem, cf. p. 30.*
***102*** *À titre d'exemple, l'European Union Agency for cybersecurity (ENISA) a consacré le mois d'octobre 2022 à l'hameçonnage et au rançongiciel.*

# 6 CONCLUSIONS ET MEILLEURES PRATIQUES

## *Principe 14 : Recrutement des talents internes*

Face à la pénurie de ressources humaines spécialisées en cybersécurité, il existe une alternative: le recrutement de talents internes. Cette forme spéciale de recrutement comprend plusieurs facettes :

- Plusieurs institutions financières proposent déjà à leurs employés des programmes d'études pendant les vacances. Il serait avantageux de promouvoir les certifications en cybersécurité dans le cadre de ces programmes de façon à constituer un vivier de ressources cyber.
- Il serait opportun de séparer les fonctions technologiques et managériales au sein de la filière des carrières en cybersécurité. Il deviendrait alors possible de proposer aux employés non technophiles des programmes de travail axés sur la gestion administrative de la cybersécurité.
- Toujours dans le but de développer des talents internes, il est souhaitable de faciliter les transferts internes pour permettre l'observation du poste de travail disponible et offrir des possibilités de formation sur le terrain aux candidats intéressés.[103]

D'une façon générale, les personnes visées par le recrutement des talents internes sont des cadres expérimentés. Par rapport à des ressources recrutées à l'externe, ils ont l'avantage de bien connaître la culture d'entreprise. Au début, ils auront besoin d'un mentorat de la part d'un expert chevronné en cybersécurité afin de faciliter leur recyclage.

→ **Favoriser le recrutement de talents internes dans le secteur bancaire africain en utilisant tous les moyens disponibles (formation et aide à la certification, séparation des fonctions technologiques et managériales au sein de la cybersécurité, transferts internes et stages au sein du groupe spécialisé en cybersécurité).**

## *Principe 15 : nécessité d'une cyber-gouvernance*

La banque centrale a intérêt à exiger que les conseils d'administration des grandes banques commerciales disposent de connaissances, de compétences et d'une expérience suffisantes en cybersécurité. Or, en Afrique comme dans le reste du monde, la majorité des administrateurs du secteur En l'absence des compétences cyber minimales, le conseil d'administration risque de se contenter de consommer passivement les mesures et les informations préparées par la direction de la banque. Cette situation est dangereuse. Dans certains pays, les règles relatives à la cybersécurité et à la protection des données vont jusqu'à rendre les membres du conseil d'administration, personnellement responsables, des risques liés à la cybersécurité.

Sans attendre l'existence de telles juridictions, les banques centrales doivent inciter les banques commerciales à importance systémique à doter leurs conseils d'administration d'une expertise suffisante pour qu'ils puissent s'approprier les enjeux de cybersécurité et de cyber-résilience. Pour cela, il convient d'imposer à ces entités quelques exigences incontournables :

- Les conseils d'administration doivent avoir un accès adéquat à l'expertise en matière de cybersécurité.
- Les membres du conseil d'administration sont tenus personnellement responsables des incidents liés à la cybersécurité qui pourraient survenir à la banque.
- Chaque conseil d'administration devra nommer au moins un administrateur indépendant ayant une formation ou une expérience en informatique ou en cybersécurité, à court terme (le délai doit être fixe et suffisamment court pour imposer sentiment d'urgence, horizon trois à cinq ans).
- En attendant la nomination d'un administrateur spécialisé, la banque aura l'obligation d'améliorer les compétences de ceux qui siègent déjà au conseil d'administration au moyen de séances fixes ou encore d'une journée de formation par an.

→ **Pour satisfaire aux meilleures pratiques, les banques commerciales d'importance systémique doivent nommer au moins un administrateur indépendant ayant une formation ou une expérience en informatique ou en cybersécurité.**

***103*** *"Africa Cyber Security Outlook", KPMG, septembre 2022, 46 pages. Cf. p. 23.*

## *Principe 16 : Enregistrement des fintechs*

La banque centrale doit exiger que toutes les entreprises de type fintech qui exploitent un système de paiement soient enregistrées auprès d'elle. En outre, elle doit également exiger que toutes les entreprises fintechs se conforment aux lois nationales sur la cybersécurité ainsi qu'à tous les autres règlements pertinents. Enfin, la banque centrale doit exiger que les entreprises fintech signalent immédiatement (délai maximum de 60 minutes) toute fraude dont elles seraient victimes ou toute transaction suspecte.

→ Il est fortement souhaitable que toutes les entreprises de type fintech qui exploitent un système de paiement aient l'obligation de s'enregistrer auprès de la banque centrale.

## *Principe 17 : Sandbox réglementaire*

Dans les pays où l'activité économique le justifie, il est recommandé de favoriser une approche de "sandbox" réglementaire ou bac à sable à l'intention des fintechs ainsi que des banques qui effectuent de la R-D. Il s'agit d'un environnement contrôlé où le cadre réglementaire est assoupli pendant que des innovations financières sont testées. Une fois que le régulateur a pu constater comment fonctionnent les nouveaux produits financiers, la réglementation peut être réintroduite, modifiée ou supprimée. Cette approche a été utilisée avec succès au Kenya afin de permettre au secteur de l'argent mobile de se développer.

Cependant, la banque centrale doit superviser étroitement les banques ou les fintechs bénéficiant du bac à sable réglementaire afin de prévenir l'instabilité financière, toute atteinte à la protection des consommateurs ou encore les risques de fraude, et ne pas hésiter à réimposer rapidement le niveau de réglementation nécessaire si certaines innovations particulières engendraient des effets pervers. Toute participation au bac à sable doit faire l'objet d'un accord écrit portant sur une durée limitée (typiquement six à 12 mois).

→ Il est suggéré de favoriser une approche de "sandbox" réglementaire ou bac à sable où les fintechs ainsi que les banques avancées pourront tester des innovations financières, dans tous les pays où l'activité économique le justifie.

**Fonctionnement du bac à sable de la banque centrale d'Indonésie**

Le bac à sable de Bank Indonesia (BI) est géré par un comité de pilotage composé d'experts de la réglementation, de l'octroi de licences, des technologies de l'information, de la gestion de risques et de l'exploitation de services financiers ainsi que de juristes. Ce groupe d'experts est chargé d'évaluer les risques des participants potentiels au bac à sable réglementaire. Pour limiter les risques liés à l'innovation, BI exige que tous les systèmes de paiement mis au point par les participants soient enregistrés auprès d'elle, et limite la collaboration aux banques et aux seuls fintechs licenciées.

IMF Working Paper, 2021[104]

***104*** *"Central Bank Risk Management, Fintech, and Cybersecurity", IMF Working Paper, 2021, 75 pages. Cf. pp. 60-61.*

# ANNEXE 1
# BIBLIOGRAPHIE CHOISIE

| Titre | Organisme | Pays | Date | Pages |
|---|---|---|---|---|
| Africa Cyber Security Report | Serianu | Kenya | 2017 | 86 |
| Africa Cyber Security Outlook | KPMG | Pays-Bas | 2022 | 47 |
| Africa Payments: Insights into African transaction flows | SWIFT | Belgique | 2018 | 38 |
| African Cyberthreat Assessment Report: Cyberthreat Trends | INTERPOL | France | 2023 | 31 |
| African Cybersecurity Research Report | KnowBe4 | USA | 2019 | 8 |
| Annual report 2020-21 | Bank for International Settlements (BIS) | Suisse | 2022 | 219 |
| Bank Regulation and Supervision a Decade after the Global Financial Crisis | World Bank | USA | 2020 | 67 |
| Baromètre de l'industrie financière africaine | Deloitte | G-B | 2023 | 59 |
| Building Confidence – Solving Banking's Cybersecurity Conundrum | Accenture Security | Irlande | 2017 | 11 |
| Central bank digital currencies in Africa | Bank for International Settlements (BIS) | Suisse | 2022 | 22 |
| Cyber Crime & Cyber Security: Trends in Africa | Symantec | USA | 2016 | 95 |
| Cyber Resilience for Financial Market Infrastructures | World Bank | USA | | |
| Central bank digital currencies in Africa | Bank for International Settlements (BIS), | Suisse | 2022 | 22 |
| Central Bank Risk Management, Fintech, and Cybersecurity | IFM | USA | 2021 | 75 |
| Cyber risk in central banking | Bank for International Settlements (BIS | Suisse | 2022 | 22 |
| Cyber threats on African subjects | IDC Herzliya | Israël | 2018 | 37 |
| Cybersécurité au Sénégal | SAYTU | Sénégal | 2019 | 61 |
| Digital Access: The Future of Financial Inclusion in Africa | International Finance Corporation (IFC) | Afrique du Sud | 2018 | 89 |
| Des voix africaines plus fortes dans le numérique | Diplo | Suisse | 2023 | 110 |
| Digital Access: The future of financial inclusion in Africa | Internal Finance Corporation (IFC) | USA | 2018 | |
| Digital Banking Fraud: Best Practice for Technology-Based Prevention | NetGuardian | Suisse | 2021 | 21 |
| Disrupting Africa: Riding the wave of the digital revolution | PwC | G-B | 2016 | 53 |
| Évaluation des cybermenaces en Afrique | INTERPOL | France | 2021 | 34 |
| État de la menace liée au numérique en 2018 | Ministère de l'Intérieur | France | 2018 | 112 |
| Fintech in Sub-Saharan African Countries | FMI | USA | 2019 | 51 |

# ANNEXE 1
# BIBLIOGRAPHIE CHOISIE

| Titre | Organisme | Pays | Date | Pages |
|---|---|---|---|---|
| FinTechs in Sub-Saharan Africa | EY | G-B | 2019 | 21 |
| Global Software Survey 2018 | BSA (Software Alliance) | USA | 2018 | 20 |
| Information Security Risks: Supervision and Control | BRICS | India | 2021 | 36 |
| International Strategy to Better Protect the Financial System Against Cyber Threats | Carnegie Endowment for International Peace | USA | 220 | 233 |
| Kingdom of Morocco Cyber Readiness at a Glance | Potomac Institute for Policy Studies | USA | 2018 | 30 |
| La finance en Afrique : naviguer en eaux troubles | Banque européenne d'investissement (BEI) | Luxembourg | 2022 | 148 |
| La fraude bancaire en Afrique subsaharienne | Dataprotect | Maroc | 2019 | 55 |
| Making Finance Work for Africa | MFW4A | Côte d'Ivoire | 2021 | 67 |
| Missing Key: The Challenge of Cybersecurity and Central Bank Digital Currency | The Atlantic Council of the United States | USA | 2022 | 49 |
| Numérique et technologies financières en Afrique | Agence française de développement | France | 2023 | 13 |
| Principles for effective supervisory colleges | Basel Committee on Banking Supervision | Suisse | 2014 | 26 |
| Principles for Operational Resilience, | Basel Committee on Banking Supervision | Suisse | 2021 | 8 |
| Projet de rapport (...) en matière de développement des fintechs et de cybersécurité | Association des banques centrales africaines (ABCA) | Sénégal | 2019 | 26 |
| Project Khokha | South African Reserve Bank (SARB) | Afrique du Sud | 2020 | 58 |
| Roaring to life: Growth and innovation in African retail banking | McKinsey & Company | USA | 2018 | 54 |
| Sacco Cybersecurity Report | Serianu | Kenya | 2018 | 22 |
| The end of the beginning | McKinsey & Company | USA | 2022 | 46 |
| The Geography of BEC | ACID (Agari Cyber Intelligence Division) | USA | 2022 | 15 |
| The Global Findex Database | World Bank | USA | 2021 | 184 |

# ANNEXE 2
# EFFORTS DES NATIONS UNIES EN MATIÈRE DE CYBERSÉCURITÉ

Tout naturellement, c'est l'Organisation des Nations Unies qui a pris l'initiative d'élaborer une politique de coopération entre les États pour réduire les risques dans le cyberespace. C'est ainsi qu'a été créé en 2004 un Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (GGE). Huit pays africains ont participé aux travaux du GGE au fil des ans (Égypte, Ghana, Kenya, Mali, Maurice, Maroc, Sénégal et Afrique du Sud).

Malheureusement, le Groupe d'experts des Nations Unies n'a pas réussi à dégager un consensus sur les solutions à adopter pour réagir aux cyberattaques ni sur le rôle que les Nations Unies devraient jouer, le cas échéant, dans l'imposition de sanctions contre les auteurs des cyberattaques.

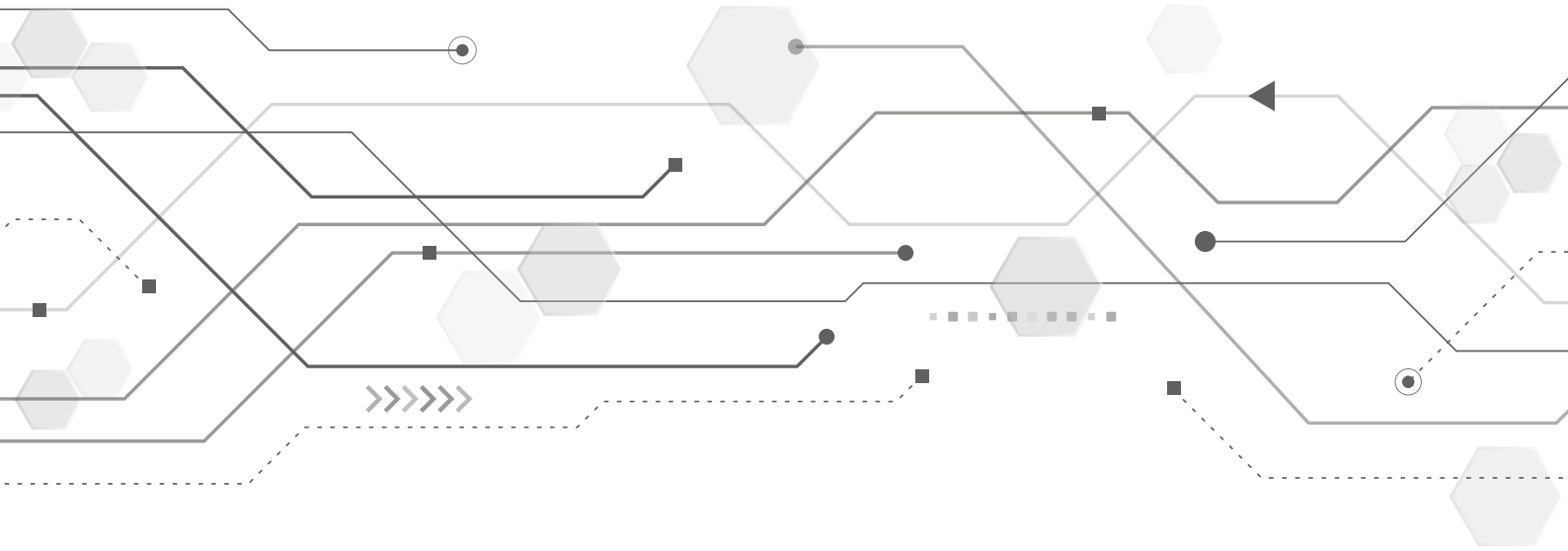
L'impasse est survenue en 2017 en raison de l'opposition entre les États-Unis et ses alliés qui estiment que le droit international existant doit s'appliquer dans le cyberespace et la Chine qui estime qu'un nouveau traité doit être conclu qui serait basé sur un code de conduite en matière de cybersécurité .

En 2018, l'Assemblée générale de l'ONU a créé le Groupe de travail à composition non limitée (GTCNL) sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Il a pour tâche de poursuivre l'élaboration des règles, normes et principes de comportement responsable des États, de discuter des moyens de les mettre en œuvre et d'étudier la possibilité d'établir un dialogue régulier sous les auspices de l'ONU.

Le premier GTCNL a conclu ses travaux en mars 2021 et a été suivi par un nouveau GTCNL pour la période 2021-2025. Seize pays africains ont participé au GTCNL de 2019-2021 (Afrique du Sud, Algérie, Botswana, Cameroun, Côte d'Ivoire, Égypte, Éthiopie, Ghana, Kenya, Malawi, Maroc,
Maurice, Mozambique, Nigéria, Ouganda, Zimbabwe).

En 2019, l'Assemblée générale des Nations unies a créé le Comité spécial à composition non limitée chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, sous les auspices de la Troisième Commission. Le Comité spécial a été proposé par la Fédération de Russie et 27 coauteurs, parmi lesquels neuf pays africains (Algérie, Angola, Burundi, Égypte, Érythrée, Libye, Madagascar, Soudan et Zimbabwe).

Le groupe africain a noté que le renforcement des capacités est une condition préalable à la lutte contre la cybercriminalité, et que la convention devrait créer un cadre permettant de fournir des programmes de formation et de renforcement des capacités à long terme afin de renforcer les capacités nationales de détection et d'enquête en matière de cybercriminalité. Le groupe a également souligné l'importance d'un financement prévisionnel et stable pour l'assistance technique aux pays en développement, et la nécessité d'une utilisation efficace de ces ressources pour assurer la durabilité de la mise en œuvre de la future convention.



# DATAPROTECT

Security is our commitment

# LA CYBER-RÉSILIENCE DU SECTEUR BANCAIRE EN AFRIQUE

Une étude DATAPROTECT
Casablanca, 2023

DATAPROTECT
Security is our commitment


# LA CYBER-RÉSILIENCE DU SECTEUR BANCAIRE EN AFRIQUE

## NOUVEAUX DÉFIS POUR LE RÉGULATEUR

Livre Blanc