Rapport Final du Groupe de Travail

Groupe de Travail sur la Cybersécurité

APRIL 2026

Reference: WATRA/WG/CS/23AGM/26/04/001

Informations sur le document
Nature du document : Rapport Final du Groupe de Travail
Groupe concerné : Groupe de Travail sur la Cybersécurité (GT-Cyber)
Mandat Résolution AGM22/CR/25/R06– Plan annuel/programme d'activités ARTAO 2025
Périmètre : Secteur des télécommunications en Afrique de l'Ouest
Destinataire : Secrétariat Exécutif de l'ARTAO et États membres
Statut : Final – Pour adoption

Contents

1 Résumé Exécutif

Le présent rapport final synthétise les travaux du Groupe de travail sur la cybersécurité de l'Association des Régulateurs des Télécommunications de l'Afrique de l'Ouest (WATRA), issus des différentes réunions tenues à Banjul (2024), Conakry (2024), Accra (2025) et Ouagadougou (2026).

Dans un contexte marqué par l'accélération de la transformation numérique et l'augmentation des cybermenaces, les États membres ont relevé des défis majeurs, notamment la recrudescence des attaques (phishing, ransomware, fraude mobile), les disparités de capacités entre pays, ainsi que l'insuffisance des cadres réglementaires harmonisés.

Les travaux ont permis d'identifier des priorités stratégiques pour la sous-région, notamment :

- le renforcement des capacités humaines et techniques ;
- l'harmonisation des cadres réglementaires ;
- la mise en place de mécanismes efficaces de coopération et de partage d'informations ;
- le développement de structures nationales et sectorielles de réponse aux incidents (CERT/CSIRT).

Le Groupe recommande la mise en œuvre d'un plan d'action structuré comprenant la création d'une plateforme régionale de partage d'informations, l'organisation d'exercices de cybersécurité, le renforcement de la collaboration entre parties prenantes et la promotion d'un cadre régional harmonisé.

Ce rapport constitue ainsi une feuille de route stratégique pour le renforcement de la cybersécurité dans le secteur des télécommunications en Afrique de l'Ouest.

2 Avant-Propos Et Contexte

2.1 Mandat du Groupe de Travail

En application de la Résolution AGM22/CR/25/R06 portant adoption du Plan annuel et du programme d'activités de l'ARTAO pour l'exercice 2025, l'Assemblée Générale de l'ARTAO a décidé la création de trois (3) groupes de travail thématiques chargés de traiter des questions réglementaires critiques dans la sous-région ouest-africaine. Ces groupes couvrent respectivement : (i) le développement des infrastructures, (ii) l'accès et l'expérience des consommateurs, et (iii) la cybersécurité.

Le présent rapport constitue le rapport final du Groupe de Travail sur la Cybersécurité (GT-Cyber). Il rend compte des travaux menés, des analyses réalisées et des recommandations formulées à l'issue du processus de réflexion collectif conduit par les membres du groupe.

2.2 Contexte général

La transformation numérique accélérée que connaît l'Afrique de l'Ouest représente à la fois une opportunité considérable pour le développement économique et social, et un vecteur d'exposition croissante aux risques cyber. La multiplication des utilisateurs connectés, le déploiement de réseaux mobiles de nouvelle génération (4G/5G), l'essor des services financiers numériques et l'accroissement des échanges de données transfrontalières exposent davantage les infrastructures de télécommunications à des menaces sophistiquées et en constante évolution.

Dans ce contexte, l'amélioration de la cybersécurité en Afrique de l'Ouest passe désormais par une approche résolument opérationnelle. L'ARTAO, en tant qu'organe de coordination régionale, doit jouer un rôle moteur dans la mise en place de mécanismes harmonisés, efficaces et durables.

Les actions proposées visent à réduire les écarts opérationnels entre les pays, améliorer la capacité de réponse collective et renforcer la résilience globale de la région face aux cybermenaces croissantes.

Une mise en œuvre progressive, soutenue par un engagement politique fort et des ressources adéquates, permettra d'atteindre ces objectifs.

Les régulateurs de télécommunications jouent un rôle clé non seulement dans la promotion de l'accès et de la concurrence, mais aussi dans la garantie d'un

environnement numérique sûr et résilient pour les citoyens, les entreprises et les gouvernements de la sous-région.

La régulation a pris un virage vers des cadres plus holistiques et plus complets, exigeant une approche collaborative, multisectorielle, prospective et transfrontalière pour répondre aux attentes de ce secteur dynamique.

2.3 Composition et méthode de travail

Le Groupe de Travail sur la Cybersécurité est composé de représentants des autorités de régulation des télécommunications membres de l'ARTAO. Il a travaillé selon une méthodologie participative fondée sur des consultations techniques, des échanges d'expériences et l'analyse comparative des cadres réglementaires en vigueur dans la sous-région et au niveau international.

3 Paysage des Menaces de la Cybersecurite

Le paysage des cybermenaces en Afrique de l'Ouest connaît une mutation rapide, marquée par une professionnalisation des cybercriminels et une diversification des vecteurs d'attaque. Le phishing demeure dominant, notamment via SMS (smishing) et applications de messagerie.

Les attaques par ransomware ciblent de plus en plus les administrations publiques, en raison de la faiblesse des dispositifs de sauvegarde et de continuité d'activité. Par ailleurs, les fraudes liées au Mobile Money constituent un enjeu critique, compte tenu de la forte pénétration de ces services dans la région.

Les analyses ont également révélé que :

- une proportion importante des organisations ne dispose pas de dispositifs adéquats de cybersécurité ;
- les infrastructures critiques restent vulnérables face aux attaques ;
- les nouvelles technologies (IoT, services satellitaires, IA) introduisent de nouveaux vecteurs de menace.

Ces constats soulignent la nécessité d'une approche proactive et coordonnée pour anticiper et atténuer les risques.

3.1 Panorama des menaces dans le secteur des télécommunications

Le secteur des télécommunications en Afrique de l'Ouest fait face à un paysage de menaces cyber diversifié et en rapide évolution. Les opérateurs de réseaux, les fournisseurs de services et les utilisateurs finaux sont exposés à un spectre large d'attaques qui compromettent la disponibilité, la confidentialité et l'intégrité des communications.

3.2 Principales catégories de menaces identifiées

- Hameçonnage (phishing) et ingénierie sociale : les campagnes de phishing ciblées exploitent la confiance des utilisateurs envers les opérateurs télécom pour dérober des données personnelles et des identifiants.
- Attaques par déni de service distribué (DDoS) : ciblant les infrastructures critiques d'opérateurs télécom et les plateformes de services numériques, ces attaques peuvent paralyser des réseaux entiers et interrompre des services essentiels.

- Fraudes télécoms et cyberfraudes : les arnaques par SMS (smishing), la fraude à l'abonnement, la manipulation des systèmes de facturation et les escroqueries financières via mobile money représentent un préjudice économique considérable pour les consommateurs et les opérateurs.
- Intrusions dans les réseaux de signalisation (SS7/Diameter) : les vulnérabilités des protocoles de signalisation permettent à des acteurs malveillants d'intercepter des communications, de localiser des abonnés et de contourner des mécanismes d'authentification.
- Logiciels malveillants et ransomwares : la propagation de malwares via les réseaux mobiles et les plateformes numériques constitue une menace croissante pour les entreprises et les institutions.
- Attaques sur les équipements et les réseaux d'accès : les vulnérabilités dans les équipements des fournisseurs (routeurs, antennes, systèmes de gestion) exposent les réseaux à des compromissions à grande échelle.

3.3 Défis spécifiques à la protection des données

La protection des données personnelles des usagers des télécommunications constitue un enjeu réglementaire central. La collecte massive de données (métadonnées de communications, données de localisation, historiques de navigation) par les opérateurs crée des risques significatifs en cas de violation ou d'utilisation abusive.

- Absence ou insuffisance de législations sur la protection des données dans certains pays membres
- Mécanismes insuffisants de notification des violations de données aux autorités et aux utilisateurs
- Lacunes dans la mise en œuvre de politiques de conservation et de minimisation des données
- Risques liés aux transferts transfrontaliers de données dans un contexte d'intégration économique régionale
- Manque de stratégies claires pour faire face aux défis

3.4 Confidentialité et sécurité des réseaux

La sécurité des réseaux de communications électroniques est une condition sine qua non de la confiance des utilisateurs. Le groupe de travail a identifié plusieurs facteurs de vulnérabilité structurels :

- Vieillissement et hétérogénéité des équipements réseau avec des cycles de mise à jour insuffisants

- Dépendance vis-à-vis de fournisseurs d'équipements présentant des risques potentiels pour la sécurité nationale
- Manque de normes communes d'audit et de certification de sécurité des équipements télécom
- Sous-investissement dans les outils de supervision, de détection et de réponse aux incidents

Recommandations opérationnelles

1. Mettre en place un système régional de veille stratégique cyber ;
2. Standardiser les méthodes de collecte des incidents ;
3. Développer des capacités d'analyse prédictive des menaces.

Constat clé – Défis et menaces

Les pays d'Afrique de l'Ouest font face à une augmentation significative des cyberincidents dans le secteur télécom.

Les attaques DDoS, les fraudes mobiles et les violations de données constituent les principales menaces.

La protection des données et la sécurité des réseaux nécessitent des cadres réglementaires renforcés et harmonisés.

La coopération sous-régionale est indispensable face à la nature transfrontalière des cybermenaces.

4 Strategies et Lignes Directrices Pour le Renforcement des Capacités des Pays Membres

4.1 1. État des lieux des capacités dans la sous-région

L'analyse comparative réalisée par le groupe de travail révèle des disparités importantes entre les pays membres de l'ARTAO en matière de capacités de cybersécurité. Si certains États ont développé des cadres institutionnels solides (Centres opérationnels de sécurité, équipes nationales CERT/CSIRT, politiques nationales de cybersécurité), d'autres en sont encore aux premières étapes de structuration de leur gouvernance cyber.

4.1.1 Diagnostic régional

Les États membres présentent des niveaux de maturité variés. Certains disposent de stratégies nationales opérationnelles, tandis que d'autres sont encore en phase de structuration institutionnelle.

4.1.2 Axes de renforcement

- Mise en place de CERT nationaux pleinement opérationnels ;
- Renforcement des autorités de protection des données ;
- Développement de cadres juridiques robustes ;
- Élaborer ou actualiser les politiques nationales de cybersécurité en intégrant un volet spécifique aux télécommunications

La région de l'Afrique de l'ouest a besoin de mesures de cybersécurité pratiques, harmonisées et abordables, adaptables par les opérateurs de communications et les autorités de régulation malgré les disparités en matière de maturité des infrastructures, de connectivité et de capacités techniques. Une directive sur la cybersécurité et la sécurité de l'information (DCSI), appuyée par des mécanismes nationaux et sectoriels de réponse aux incidents, le renforcement des capacités, le partage d'informations fiable et la coopération public-privé, peut constituer un socle commun de résilience.

Les pays d'Afrique de l'Ouest accélèrent leur transformation numérique dans les secteurs des télécommunications, de l'accès à Internet, de la radiodiffusion, des services financiers et d'autres secteurs essentiels. Cette croissance accroît l'exposition

aux cybermenaces susceptibles de perturber les services, d'éroder la confiance des consommateurs et d'affaiblir l'économie numérique dans son ensemble. Parallèlement, la région évolue dans des environnements techniques variés, notamment des systèmes existants, des équipements hétérogènes et une connectivité inégale. Les stratégies régionales doivent donc être fondées sur une analyse des risques, réalistes et adaptables aux différents niveaux de maturité institutionnelle et infrastructurelle.

4.1.3 Directive régionale sur la cybersécurité et la sécurité de l'information (DRSI

Une DRSI peut servir de référentiel minimal commun aux titulaires de licences et aux opérateurs du secteur des communications. Elle clarifie la réglementation, améliore la préparation de l'ensemble du secteur et favorise la coordination entre les autorités de réglementation, les opérateurs et les institutions nationales de cybersécurité.

- Promouvoir une infrastructure de communications sécurisée et résiliente en renforçant la cybersécurité des entités réglementées.
- Établir un cadre de référence pour identifier, protéger, détecter, contrer et se rétablir face aux cybermenaces affectant les infrastructures et services de communications critiques.
- Exiger des opérateurs la mise en œuvre de dispositifs de gouvernance structurés, incluant des politiques de cybersécurité, des évaluations des risques, des circuits de reporting internes, des audits et une supervision au niveau du conseil d'administration, le cas échéant.
- Faciliter la détection et le signalement rapide et cohérent des incidents à un CERT national, ou à un point focal national désigné lorsqu'un CERT n'est pas encore en place.
- Permettre une réponse coordonnée aux incidents et le partage de renseignements sur les menaces entre les CSIRT sectoriels, les CERT nationaux, les opérateurs, les autorités de réglementation et d'autres partenaires de confiance. • Favoriser la conformité aux lois nationales, aux réglementations sectorielles et aux meilleures pratiques régionales émergentes.
- Renforcer la confiance des consommateurs et la sécurité numérique des services mobiles, fixes, par satellite, des fournisseurs d'accès Internet, de diffusion et autres services sous licence.

4.1.4 Considérations relatives à la conception régionale

Tout cadre régional doit être conçu en tenant compte des conditions d'exploitation locales. Des contrôles de cybersécurité excessivement complexes, coûteux ou

dépendants d'infrastructures de pointe pourraient ne pas être viables dans tous les États membres. Le groupe de travail devrait privilégier des contrôles proportionnés et efficaces dans les environnements à ressources faibles et à technologies mixtes.

- Tenir compte de la faible connectivité et de la disponibilité intermittente dans certains environnements d'exploitation.
- Reconnaître la diversité des infrastructures, notamment les systèmes anciens et les équipements hétérogènes.
- Promouvoir des solutions de sécurité peu coûteuses, évolutives et faciles à maintenir.
- Permettre une mise en œuvre progressive afin que les États membres et les opérateurs puissent progressivement satisfaire aux exigences minimales. 4. Stratégies proposées pour renforcer les capacités régionales en cybersécurité

4.1.5 Domaine stratégique

Les actions suivantes sont recommandées

- Politiques et réglementations : Élaborer des politiques nationales de cybersécurité et des lignes directrices sectorielles alignées sur les principes régionaux et adaptées aux réalités économiques et sociales locales.

- Coopération public-privé : Renforcer les partenariats entre les autorités de réglementation, les opérateurs, les fournisseurs, les universités et les investisseurs afin d'améliorer le financement, la préparation et la mise en œuvre de la cybersécurité.

- Renforcement des capacités : Mettre en place des programmes de formation continue et de certification

4.2 Elaborer des stratégies et des lignes directrices pour renforcer les capacités de cybersécurité des membres

4.2.1 Ressources humaines et expertise technique

- Développer des programmes de formation spécialisée en cybersécurité des télécommunications pour les régulateurs
- Créer un programme de certifications professionnelles régional reconnu par les États membres de l'ARTAO
- Encourager les partenariats avec les universités et instituts de formation pour développer l'expertise locale
- Mettre en place des programmes d'échange d'experts entre régulateurs membres

Lignes directrices pour le renforcement des capacités
1. Chaque État membre devrait disposer d'une politique nationale de cybersécurité télécom.
2. La création d'un CERT/CSIRT sectoriel télécom est recommandée dans chaque pays. 3. L'ARTAO devrait développer un programme régional de formation et de certification.
4. Des exercices de simulation de cyberincidents sous-régionaux annuels sont préconisés.

5 COOPÉRATION ET PARTAGE D'INFORMATIONS

La montée des cybermenaces, de plus en plus sophistiquées, automatisées et souvent transnationales, met en évidence la nécessité d'une action collective. En l'absence de coopération structurée entre les acteurs concernés, les pays de la sous-région se trouvent exposés à des vulnérabilités accrues. Le manque d'harmonisation des cadres réglementaires et l'insuffisance de coordination internationale rendent les réponses aux incidents souvent dispersées, tardives, voire inefficaces. De même, l'absence de collaboration entre les structures techniques, notamment pour le partage d'informations en temps réel, facilite la propagation des attaques et complique les actions de lutte. Cette situation entraîne des conséquences importantes, tant sur le plan opérationnel que financier, perturbe la continuité des services essentiels et fragilise la confiance des usagers et des partenaires.
Afin de renforcer le dispositif régional à faire face ces insuffisances, le groupe de travail de l'ARTAO sur la cybersécurité formule les recommandations ci et encourage leur adoption.

Face à ces différents défis, il est primordial d'adapter les réponses par les mesures ci-après :

- Développer et implémenter une plateforme régionale sécurisée de partage en temps réel ;
- Mettre en place des protocoles de classification des informations ;
- Définir des niveaux d'accès différenciés.

5.1 Mécanismes de coopération régionale

La nature transfrontalière des cybermenaces impose une réponse collective et coordonnée. Le groupe de travail a examiné les mécanismes existants de coopération en matière de cybersécurité dans la sous-région et identifié les gaps à combler pour renforcer la résilience collective.

5.2 Plateforme régionale de partage d'informations

Face à l'augmentation des cybermenaces résultant de la digitalisation croissante des services au sein des pays membres de l'ARTAO, il est crucial de mettre en place une stratégie régionale de partage d'informations en cybersécurité. Un cadre structuré et sécurisé pour l'échange d'informations, soutenu par une plateforme numérique adaptée, permettrait non seulement de mieux gérer les incidents mais aussi d'uniformiser les pratiques de cybersécurité et de renforcer la résilience collective des nations concernées. La coopération transfrontalière, l'amélioration des capacités

locales et l'adoption de normes internationales joueront un rôle clé pour répondre efficacement aux menaces transnationales. De plus, pour garantir l'efficacité et la pérennité du système, la confiance, la transparence et une surveillance régulière des processus de partage d'informations sont indispensables. En somme, il est essentiel que les pays de l'ARTAO adoptent une approche proactive et coordonnée pour assurer la protection de leur sécurité nationale et de leurs économies face à l'évolution rapide des cybermenaces.

Le groupe de travail recommande la création d'une Plateforme Régionale de Partage d'Informations sur les Cybermenaces (PRSIC-ARTAO), dont les caractéristiques principales seraient :

- Une gouvernance partagée entre les régulateurs membres, avec un secrétariat technique assuré par l'ARTAO
- Un mécanisme d'échange d'indicateurs de compromission (IoC) en temps quasi-réel
- Un bulletin de renseignement sur les menaces diffusé périodiquement aux membres
- Des protocoles clairs définissant la classification et les modalités de partage des informations sensibles
- L'interconnexion progressive avec les plateformes continentales (AfricaCERT) et internationales

5.3 Protocoles et accords de coopération

Pour formaliser et encadrer la coopération, le groupe de travail recommande :

- La signature d'accords bilatéraux et multilatéraux entre régulateurs membres sur l'échange d'informations cyber
- La participation conjointe aux exercices internationaux de cybersécurité
- L'établissement de points de contact désignés dans chaque autorité nationale pour la coordination régionale

5.4 Renforcement de la résilience régionale

Au-delà du partage d'informations, la résilience collective de la sous-région repose sur :

- La mise en place de redondances et d'interconnexions sécurisées entre les infrastructures critiques de télécommunications
- Des exercices réguliers de gestion de crise cyber impliquant plusieurs pays membres simultanément
- La sensibilisation conjointe des opérateurs et du public aux bonnes pratiques de cybersécurité

Les États membres de l'ARTAO ont déjà engagé des efforts notables pour renforcer la cybersécurité dans le secteur des télécommunications. Néanmoins, les enjeux actuels imposent une approche davantage coordonnée et structurée à l'échelle régionale.

La mise en œuvre des actions proposées contribuera à améliorer la résilience des infrastructures, à renforcer la protection des données et à instaurer un climat de confiance propice au développement du numérique en Afrique de l'Ouest

Recommandations phare – Coopération/Partage
Institutionnaliser le partage d'informations en créant la Plateforme Régionale de Partage d'Informations sur les Cybermenaces
Mettre en place un cadre juridique pour le partage transfrontalier
Un mécanisme d'échange d'indicateurs de compromission (IoC) en temps quasi-réel
Instaurer un bulletin de renseignement sur les menaces diffusé périodiquement aux membres

6 Défis de Cybersécurité Dans le Secteur Télécom

Dans un contexte marqué par l'accélération de la transformation numérique en Afrique de l'Ouest, le secteur des télécommunications occupe une place stratégique dans le fonctionnement des États, la fourniture des services essentiels et le développement économique. Cette évolution s'accompagne toutefois d'une exposition accrue à des cybermenaces de plus en plus complexes, capables d'affecter les réseaux, les infrastructures critiques et la continuité des services.

Face à la nature transfrontalière de ces risques, une réponse strictement nationale ne saurait suffire. Il apparaît dès lors nécessaire de promouvoir une approche régionale concertée, fondée sur la coopération, l'harmonisation des pratiques, le renforcement des capacités et le partage d'informations. À cet égard, l'ARTAO est appelée à jouer un rôle central dans l'accompagnement des États membres vers une plus grande résilience cyber du secteur télécom.

Le présent rapport vise, dans cette perspective, à identifier les principaux défis de la cybersécurité dans le secteur des télécommunications en Afrique de l'Ouest et à proposer des orientations pratiques en vue de renforcer la coordination régionale et l'efficacité des réponses apportées

Dans le vaste chantier de la transformation numérique de l'Afrique de l'Ouest, le secteur des télécommunications ne se contente plus d'être un simple prestataire de services ; il est devenu l'infrastructure vitale sur laquelle reposent la finance, l'administration et la sécurité nationale. Si les cadres stratégiques et les politiques de gouvernance constituent les fondations de cet édifice, la réalité de la menace exige désormais une transition rapide vers l'action purement opérationnelle. Face à des cybercriminels qui exploitent les moindres failles de connectivité, l'heure est à la mise en œuvre de dispositifs techniques robustes capables de protéger les flux de données et l'intégrité des réseaux ouest-africains.

Ce rapport met l'accent sur les actions concrètes et recommandations visant à améliorer l'efficacité opérationnelle des dispositifs de cybersécurité dans la région.

6.1 Principaux défis opérationnels identifiés

6.1.1 Insuffisance des capacités de détection et de réponse aux incidents

Dans un environnement numérique marqué par la rapidité et la sophistication croissante des cybermenaces, la capacité à détecter et à répondre efficacement aux

incidents constitue un pilier essentiel de la cybersécurité. Pourtant, dans de nombreux États de la région, cette capacité demeure limitée. Le déploiement des SOC (Security Operations Center) et des CSIRT (Computer Security Incident Response Team) reste encore insuffisant, tandis que les outils de surveillance en temps réel font défaut ou ne sont pas pleinement adaptés aux besoins. Cette situation se traduit par des délais de réaction souvent élevés face aux incidents, réduisant ainsi l'efficacité des mesures de mitigation.

6.1.2 Fragmentation des infrastructures techniques

Au cœur des difficultés opérationnelles se trouve également la fragmentation des infrastructures techniques, qui entrave toute approche coordonnée et cohérente. Les systèmes d'information, fortement hétérogènes d'un pays à l'autre et parfois même au sein d'un même État, compliquent l'harmonisation des pratiques. À cela s'ajoute l'absence d'interopérabilité entre les différentes plateformes de cybersécurité, rendant difficile l'intégration des solutions existantes et limitant les synergies possibles.

6.1.3 Faiblesse des mécanismes de gestion des incidents

La gestion des incidents, pourtant cruciale dans la chaîne de réponse aux cyberattaques, souffre de lacunes structurelles importantes. L'absence de procédures standardisées ne permet pas d'assurer une réponse uniforme et efficace. Par ailleurs, la coordination entre les CERT/CSIRT nationaux demeure limitée, ce qui affaiblit la capacité de réponse collective. Enfin, le manque de plans de continuité et de reprise d'activité expose les organisations à des interruptions prolongées en cas de crise.

6.1.4 Contraintes liées aux ressources techniques

Les contraintes techniques constituent un frein majeur à l'efficacité opérationnelle des dispositifs de cybersécurité. L'insuffisance d'équipements spécialisés, combinée à une forte dépendance vis-à-vis de fournisseurs externes, limite l'autonomie des États. En outre, les difficultés liées à la maintenance et à la mise à jour des systèmes compromettent la pérennité et la performance des infrastructures existantes.

6.1.5 Faible niveau d'automatisation

À l'ère de la transformation numérique, l'automatisation des processus apparaît comme un levier incontournable pour améliorer l'efficacité opérationnelle. Toutefois, dans la région, de nombreux processus restent encore largement manuels. Cette situation rend difficile la gestion de volumes croissants de données et d'alertes, tout

en augmentant le risque d'erreurs humaines, susceptibles de compromettre la sécurité globale des systèmes.

6.2 Actions prioritaires proposées

6.2.1 Mise en place d'un cadre opérationnel harmonisé

Face à la diversité des pratiques et des niveaux de maturité, l'établissement d'un cadre opérationnel harmonisé s'impose comme une priorité. Il s'agit notamment d'élaborer des procédures standardisées de gestion des incidents à l'échelle régionale, de définir des protocoles communs de communication en cas de crise, et d'harmoniser les niveaux d'alerte ainsi que les mécanismes de notification, afin de garantir une réponse cohérente et coordonnée.

6.2.2 Déploiement et mutualisation des capacités SOC/CSIRT

Le renforcement des capacités de surveillance passe nécessairement par le développement et la mutualisation des centres opérationnels de sécurité. Il convient d'encourager la création de SOC/CSIRT nationaux interconnectés, tout en promouvant des SOC régionaux mutualisés pour les pays disposant de ressources limitées. La mise en place de plateformes communes de supervision permettrait également d'optimiser l'utilisation des ressources disponibles.

6.2.3 Renforcement des infrastructures techniques

Dans une perspective d'efficacité et de durabilité, le renforcement des infrastructures techniques constitue un levier essentiel. Cela implique la standardisation des outils de cybersécurité utilisés dans la région, la promotion de solutions interopérables et le déploiement de systèmes centralisés de collecte et d'analyse des logs, permettant une meilleure visibilité sur les activités suspectes.

6.2.4 Amélioration des capacités de réponse aux incidents

Une réponse efficace aux cybermenaces nécessite des dispositifs réactifs et bien coordonnés. À cet effet, la mise en place d'équipes d'intervention rapide à l'échelle régionale apparaît indispensable. Il est également crucial d'élaborer des plans de réponse coordonnés aux cyberattaques majeures et d'organiser régulièrement des

exercices de simulation (cyber drills), afin de tester et d'améliorer les mécanismes existants.

6.2.5 Automatisation des processus opérationnels

L'automatisation constitue un facteur clé d'amélioration des performances opérationnelles. Le déploiement de solutions SOAR (Security Orchestration, Automation and Response), l'intégration d'outils d'analyse automatisée des menaces et la réduction de la dépendance aux traitements manuels permettront d'accroître la rapidité, la fiabilité et l'efficacité des opérations de cybersécurité.

6.3 Recommandations stratégiques à portée opérationnelle

6.3.1 Standardisation et interopérabilité

Dans un contexte marqué par la diversité des systèmes, la standardisation et l'interopérabilité apparaissent comme des conditions essentielles à une coopération efficace. L'adoption de normes techniques communes, la promotion de formats standard pour les échanges de données et la garantie de la compatibilité entre les systèmes nationaux permettront de renforcer la cohérence des actions à l'échelle régionale.

6.3.2 Mise en place de mécanismes de financement durables

La pérennité des actions opérationnelles repose sur l'existence de mécanismes de financement adaptés et durables. Il est ainsi recommandé de créer des fonds régionaux dédiés aux infrastructures de cybersécurité, d'encourager les partenariats public-privé pour soutenir l'investissement technologique, et de faciliter l'accès aux financements internationaux.

6.3.3 Développement de centres d'excellence opérationnels

Afin de mutualiser les compétences et les ressources, le développement de centres d'excellence opérationnels constitue une approche stratégique pertinente. Ces hubs régionaux pourraient être spécialisés dans la réponse aux incidents, la conduite d'analyses avancées (malware, forensic) et la gestion de fonctions critiques, permettant ainsi d'optimiser l'utilisation de ressources rares et coûteuses.

6.3.4 Renforcement de la résilience des infrastructures critiques

La protection des infrastructures critiques revêt une importance capitale dans la sécurisation des États. Il convient d'identifier et de prioriser ces infrastructures, d'imposer des exigences minimales de sécurité opérationnelle, et de mettre en place des mécanismes de surveillance continue, afin de garantir leur résilience face aux cybermenaces.

6.3.5 Suivi et évaluation des performances opérationnelles

Enfin, l'amélioration continue des dispositifs de cybersécurité nécessite un suivi rigoureux et une évaluation régulière des performances. La définition d'indicateurs clés de performance (KPI), la mise en place de mécanismes de reporting réguliers et l'évaluation périodique de la maturité opérationnelle des États membres permettront d'assurer une gouvernance efficace et orientée vers les résultats.

L'amélioration de la cybersécurité en Afrique de l'Ouest passe désormais par une approche résolument opérationnelle. L'ARTAO, en tant qu'organe de coordination régionale, doit jouer un rôle moteur dans la mise en place de mécanismes harmonisés, efficaces et durables.

Les actions proposées visent à réduire les écarts opérationnels entre les pays, améliorer la capacité de réponse collective et renforcer la résilience globale de la région face aux cybermenaces croissantes.

Une mise en œuvre progressive, soutenue par un engagement politique fort et des ressources adéquates, permettra d'atteindre ces objectifs.

Priorités réglementaires identifiées
Adoption d'un cadre réglementaire minimal harmonisé sur la cybersécurité télécom au niveau ARTAO.
Intégration d'obligations de sécurité dans les cahiers des charges des licences d'opérateurs.
Mise en place d'un mécanisme régional de certification des équipements réseaux.
Développement d'indicateurs communs de mesure du niveau de maturité cyber des opérateurs.

7 Collaboration Avec les Parties Prenantes

La cybersécurité des télécommunications est une responsabilité partagée qui implique une multiplicité d'acteurs. Une collaboration efficace entre ces parties prenantes est une condition essentielle à la construction d'un écosystème numérique résilient en Afrique de l'Ouest. La collaboration avec les parties prenantes est un pilier fondamental du renforcement de la préparation en matière de cybersécurité en Afrique de l'Ouest. Cela inclut la coopération entre les autorités nationales de réglementation, les CERT, les CSIRT sectoriels, les agences de cybersécurité et autres structures compétentes.

Collaboration entre les États membres et les institutions nationales

Il est nécessaire de renforcer la coopération entre les autorités de régulation nationales, les CERT nationaux, les CSIRT sectoriels, les agences de cybersécurité et les autres structures compétentes. Les États membres ont été encouragés à partager leurs rapports nationaux sur la cybersécurité, à désigner des points focaux, à créer des CSIRT et à échanger des renseignements sur les menaces. Les États membres ont été encouragés à :

Diffuser régulièrement les rapports nationaux sur la cybersécurité et les renseignements sur les menaces afin d'améliorer la connaissance de la situation dans toute la région.

Désigner des points focaux nationaux en matière de cybersécurité qui serviront de personnes de contact pour la coordination régionale.

Créer des unités -CSIRT sectorielles et soutenir les pays qui ne disposent pas encore d'équipes fonctionnelles, comme la Guinée --Bissau.

Échanger des informations sur les menaces émergentes par le biais de mécanismes et de protocoles convenus, notamment des évaluations périodiques et des questionnaires standardisés.

Cette collaboration interétatique est considérée comme cruciale pour la mise en place d'une réponse régionale unifiée aux cybermenaces.

Partenariats régionaux et internationaux

Il est essentiel de souligner l'importance de collaborer avec les entités régionales et mondiales pour accélérer le développement des capacités et promouvoir des pratiques harmonisées en matière de cybersécurité. Parmi les principales recommandations :

En partenariat avec OCWAR -C, qui sert d'intermédiaire entre WATRA et les organisations nationales de cybersécurité dans les cas où les CERT nationaux et les CSIRT sectoriels ne relèvent pas de l'autorité de régulation des télécommunications.

Encourager tous les CERT nationaux et les CSIRT sectoriels à rejoindre FIRST (Forum des équipes de réponse aux incidents et de sécurité) et faciliter le parrainage des pays souhaitant y adhérer.

Tirer parti des canaux existants tels que l'Africa -CERT pour le partage et la coordination des renseignements.

Explorer des cadres de partenariat alignés sur des conventions internationales telles que la Convention de Malabo.

Conformément à ce qui précède, le cadre de cyber-résilience de la Commission nigériane des communications (NCC) (CRF - NCS) renforce la collaboration régionale en établissant des partenariats public - privé structurés, en appliquant l'architecture Zero Trust aux opérateurs de télécommunications et en rendant obligatoire le déploiement de centres d'opérations de sécurité (SOC).

Ce cadre approfondit également la coopération entre le NCC - CSIRT et le ngCERT, renforçant le partage transfrontalier de renseignements sur les menaces et les efforts de résilience sectoriels alignés, complétant pleinement les objectifs de WATRA en matière de gouvernance harmonisée de la cybersécurité.

La collaboration avec des entités régionales et mondiales telles que OCWAR-C, FIRST, AfricaCERT, et l'alignement sur des conventions telles que la Convention de Malabo favorisent un développement harmonisé de la cybersécurité.

Engagement auprès du secteur privé, de la société civile et des groupes spécialisés.

La cybersécurité nécessite un engagement plus large des parties prenantes, notamment des partenariats public-privé, une coopération avec les banques centrales, le soutien du laboratoire DFS de l'UIT et des réseaux d'experts tels que le Réseau des femmes africaines sur la cybersécurité. Engagement auprès du secteur privé, de la société civile et des groupes spécialisés

Les États membres ont souligné que la cybersécurité ne peut être pilotée uniquement par les organismes de réglementation et les gouvernements. Une implication plus large des parties prenantes est essentielle, notamment :

Des partenariats public-privé pour stimuler l'investissement et l'innovation dans les infrastructures de cybersécurité.

Coopération avec les banques centrales et les autorités de réglementation financière, notamment en matière de sécurité des services financiers numériques, soutenue par le laboratoire de sécurité DFS de l'UIT.

Inclusion du Réseau des femmes africaines sur la cybersécurité et de groupes d'experts similaires dans les forums régionaux afin de garantir la diversité et la représentation.

Mise en place d'une base de données d'experts régionaux pour faciliter le partage transfrontalier des ressources et l'assistance consultative.

Cette -approche multipartite élargit le champ d'expertise et renforce la résilience régionale, la collaboration en matière de normes, de lignes directrices et de renforcement des capacités. Il est nécessaire de développer conjointement des cadres de cybersécurité adaptés et des approches réglementaires harmonisées. À cette fin, les États membres se sont engagés à :

- Examiner et comparer conjointement les normes internationales existantes en matière de cybersécurité (ISO/IEC 27001, NIST CSF, CIS Controls, COBIT).

- Collaborer à la fusion de plusieurs propositions nationales ou de sous-groupes en un seul document harmonisé pour -une adoption à l'échelle de WATRA.
- Élaborer collectivement, à l'échelle internationale, des lignes directrices sur le partage d'informations, la réponse aux incidents et les tests de sécurité.
- Organiser des ateliers régionaux et des exercices de cyberdéfense animés par des experts et des institutions partenaires afin de renforcer les capacités. De telles initiatives favorisent l'appropriation collective des cadres de référence et améliorent les capacités techniques dans toute la région.

De plus, le cadre NCC mis en évidence dans la sous-section 2 ci-dessus introduit un modèle de gouvernance de la cybersécurité unifié qui s'aligne sur les normes internationales telles que l'ISO 27001 et le NIST CSF, ce qui en fait un exemple national pratique qui soutient les efforts d'harmonisation régionale de WATRA.

Ses niveaux de conformité structurés, ses piliers de gestion des risques et ses indicateurs de résilience (par exemple, l'indice de capacité cybernétique) démontrent comment les cadres nationaux peuvent opérationnaliser les objectifs régionaux en matière de cybersécurité.

Les États membres ont convenu d'évaluer les normes internationales (ISO 27001, NIST CSF, CIS Controls, COBIT), de fusionner les propositions dans des cadres harmonisés et d'élaborer des lignes directrices pour le partage d'informations, la réponse aux

incidents et les tests de sécurité ; les mécanismes d'échange d'informations et canaux de communication

La mise en place et le renforcement de canaux de communication structurés ont été identifiés comme un facteur essentiel de la collaboration. Parmi les principales propositions figuraient :

- Création d'un protocole d'échange d'informations régional centralisé par le biais d'un groupe de travail multinational.
- Mise en place d'un canal de communication officiel pour les pays membres et d'un observatoire de sécurité centralisé pour agréger les données des CERT.
- Des réunions virtuelles régulières, des enquêtes régionales périodiques et la publication de rapports bilingues (anglais/français) pour assurer l'inclusion et l'accessibilité.

Ces mécanismes garantissent une collaboration continue, structurée et -fondée sur les données.

En conclusion, la collaboration avec les principaux acteurs régionaux et internationaux demeure essentielle au renforcement des capacités de cybersécurité de l'Afrique de l'Ouest. Des mesures concrètes, telles que les bases de données d'experts, les enquêtes harmonisées et les forums régionaux, contribuent à bâtir une -résilience à long terme. Par ailleurs, le cadre de cyber-résilience de la Commission nigériane des communications (NCC) renforce les efforts régionaux en introduisant un -modèle axé sur la résilience, en imposant une architecture « Zéro confiance » et en exigeant le fonctionnement continu des centres opérationnels de sécurité (SOC). Son alignement sur les objectifs de l'ARTAO , notamment grâce à une meilleure réponse aux incidents, -des pratiques de gestion des risques unifiées et une coopération public-privé renforcée via l'équipe d'intervention en cas d'incident de sécurité informatique de la NCC (NCC -CSIRT) et l'équipe nigériane d'intervention d'urgence informatique (ngCERT), contribue significativement à la résilience numérique collective de la région et soutient la création d'un écosystème de cybersécurité sécurisé, cohérent et -adapté aux enjeux futurs.

8 Coordination de La Réponse Aux Cybermenaces

8.1 Coordonner la réponse

Un incident cyber est un événement qui peut nuire à la confidentialité, à l'intégrité ou la disponibilité des systèmes ou des données informatiques. Ces incidents peuvent être causés par des accidents, des erreurs humaines, des actes malveillants ou des pannes du système. C'est pourquoi, avoir un plan de réponse en place est essentiel minimiser pour les dommages par un tel incident. Le secteur des télécommunications présente une particularité critique : il est à la fois *cible* de cyberattaques et *infrastructure support* de la réponse à ces mêmes attaques. Une compromission du réseau télécoms peut donc paralyser simultanément l'entreprise victime et les canaux de communication nécessaires à la gestion de la crise. Cela rend la préparation préalable non pas souhaitable, mais absolument indispensable.

8.2 Cadre de gestion des incidents

Une réponse efficace aux cyberincidents nécessite un cadre de coordination clair, des procédures éprouvées et des lignes de communication établies préalablement à toute crise.

Ce cadre comprend l'ANR des pays membres et l'ARTAO :

Tous les pays membres n'ont pas le même niveau de capacité. La coordination régionale doit permettre de **niveler par le haut en temps réel** .

- Créer une **réserve régionale d'experts cyber** mobilisables en appui aux pays membres dépassés par un incident : pool de spécialistes en analyse forensique, réponse aux incidents, gestion de crise
- Mettre en place un **mécanisme de déploiement rapide** de ces experts, avec des procédures administratives et financières pré-arrangées pour éviter les délais bureaucratiques en situation de crise
- Développer des **capacités mutualisées d'analyse de malwares** accessibles à tous les membres, indispensables à chaque pays de devoir investir individuellement dans des infrastructures coûteuses
- Constituer un **stock régional de solutions techniques d'urgence** : outils d'analyse forensique, solutions de filtrage d'urgence, capacités de communication de substitution

8.3 Mécanismes de signalisation et de notification

Le groupe de travail propose que l'ARTAO joue le rôle de facilitateur dans la coordination des réponses aux incidents.

L'ANR joue le rôle de chaîne d'escalade à l'intérieur d'un pays, en ce sens qu'il constitue le point de contact de l'ARTAO pour toucher l'équipe CERT national.

Le signalement est symétrique c'est-à-dire qu'il pourra provenir d'une ANR ou de l'ARTAO.

- Établir une obligation de notification des incidents de sécurité significatifs aux régulateurs nationaux dans des délais définis (ex. notification initiale sous 24h, rapport complet sous 72h)
- Créer un formulaire standardisé de notification des incidents harmonisé entre les États membres
- définition des seuils de signalement clairs (nombre d'utilisateurs affectés, durée de l'interruption, nature des données compromises)
- Mettre en place un registre régional des incidents télécom pour l'analyse des tendances

8.4 Coordination des efforts d'atténuation

Face à un incident cyber majeur affectant un ou plusieurs pays, la coordination doit s'appuyer sur :

- Un protocole de crise activable rapidement, avec des rôles et clairement définis ;
- Des canaux de communication sécurisés entre les points de contact désignés dans chaque membre régulateur ;
- Des accords préalables avec les CERT nationaux sur les mesures d'atténuation pouvant être déployées en urgence ;
- Des mécanismes de mobilisation rapide d'expertise technique pour appuyer les États membres déficitaires en capacités.

En interne :

- Canaux de communication de substitution, indépendants du réseau potentiellement compromis
- Protocoles de partage d'informations sécurisés entre les équipes

En externe :

- Contacts nominatifs préétablis avec les régulateurs (autorité de régulation nationale, agence nationale de cybersécurité)
- Protocoles de notification clients, différenciés selon la nature de l'incident
- Stratégie de communication publique et médiatique, validée avant la crise

8.5 Exercices et simulations

La préparation aux crises cybernétiques nécessite un entraînement régulier.

L'ARTAO doit donc veiller à tester régulièrement le plan de réponse en organisant des tests et des exercices périodiques :

- Organisateur annuellement un exercice de simulation de crise cyber sous-régionale impliquant au moins la moitié des membres de l'ARTAO ;
- Conduire des exercices nationaux biennaux dans chaque État membre en impliquant les opérateurs de télécommunications ;
- Partager exclusivement les retours d'expérience des exercices et des incidents réels entre membres ;
- Participer aux exercices cyber internationaux organisés par l'UIT et d'autres partenaires

8.6 Recommandations

Le groupe de travail propose les recommandations suivantes

- Inciter les pays membres de l'ARTAO à mettre en place des plans de réponse aux incidents de sécurité au niveau sectoriel. Tous les membres devraient être encouragés à mettre en place des CSIRTS/CERTS sectoriels ou a minima un CERT national ;
- Assurer, au niveau de chaque Etat membre, une coordination efficace entre les différents acteurs y comprend le CERT/CSIRT ;
- Élaborer un **plan régional de réponse aux incidents cybernétiques** définissant les rôles, les seuils de déclenchement et les mécanismes de décision collective ;
- Organiser des **exercices de simulation régionaux** (cyber drills) impliquant plusieurs pays simultanément, pour tester les procédures et renforcer les réflexes collectifs ;
- Désigner une cellule de coordination régionale activable en cas d'incident affectant plusieurs États membres, avec un mandat opérationnel clair ;

- Négocier des accords de coopération avec les organisations homologues (CRASA pour l'Afrique australe, ARICEA pour l'Afrique orientale) pour étendre la coordination au-delà de la sous-région
- Aider les CERT nationaux dans leur procédure d'adhésion aux entités mondiales de gestion des incidents (FIRST) pour bénéficier des formations
- Mettre en place une veille sur les incidents affectant les opérateurs tiers, car la menace est souvent systémique.

9 Initiatives de Renforcement des Capacités

Le renforcement des capacités des acteurs est un levier important pour une cybersécurité renforcée dans l'espace sous régional.

9.1 Programme régional de formation ARTAO-Cyber

Le groupe de travail recommande la création d'un Programme Régional de Formation en Cybersécurité des Télécommunications, structuré autour de plusieurs niveaux de compétences adaptées aux besoins du secteur.

9.2 Partenariats stratégiques pour le renforcement des capacités

Pour atteindre les objectifs ambitieux de renforcement des capacités, l'ARTAO devrait développer des partenariats stratégiques avec des organisations régionales et internationales ayant une expertise reconnue et des Centres régionaux d'excellence en cybersécurité télécom.

- Union Internationale des Télécommunications (UIT/ITU) : programmes de formation et assistance technique
- ENISA (Agence de l'Union Européenne pour la Cybersécurité) : transfert d'expertise et bonnes pratiques
- ITU-IMPACT : accès aux ressources mondiales de cyber-renseignement et assistance en cas de crise
- AfricaCERT : coordination avec le réseau africain des équipes de réponse aux incidents
- GSMA : standards et bonnes pratiques spécifiques aux opérateurs mobiles
- Certains Agréés spécialisés dans les pays de la région
- Partenaires bilatéraux : coopération avec des régulateurs avancés (ARCEP, Ofcom, etc.)

9.3 Centre régional d'excellence en cybersécurité télécom

À plus long terme, le groupe de travail envisage la création d'un Centre Régional d'Excellence en Cybersécurité des Télécommunications (CRECT-ARTAO), qui aurait pour missions :

- Servir de hub de formation et de certification pour les professionnels de la sécurité télécom de la sous-région
- Conduire des travaux de recherche appliquée sur les menaces émergentes spécifiques au contexte ouest-africain

- Fournir une assistance technique aux régulateurs membres disposant de capacités limitées ;
- Développer et maintenir des référentiels, guides et standards régionaux de cybersécurité télécom ;

9.4 Les projets TogoCyber+ et lCentre africain de coordination et de recherche en cybersécurité (ACCRC).

Le projet TogoCyber+, initié dans le cadre du renforcement de la cybersécurité au Togo, s'inscrit dans une dynamique structurante visant à consolider les capacités nationales et régionales en matière de cybersécurité. Conçu comme un dispositif catalyseur, il a pour objectif de poser les bases techniques, humaines et organisationnelles nécessaires à l'émergence du Centre africain de coordination et de recherche en cybersécurité (ACCRC), appelé à devenir un hub continental de référence. À travers le développement des capacités des CERT, la promotion du partage d'information, le renforcement de la coopération régionale et la mobilisation de partenariats techniques et financiers, TogoCyber+ constitue une étape déterminante vers la mise en place d'un écosystème intégré de cybersécurité en Afrique. Dans cette perspective, l'ACCRC apparaît comme l'aboutissement stratégique de cette initiative, en offrant un cadre structuré pour la coordination, la recherche, la formation et l'innovation à l'échelle continentale.

Au regard de ces enjeux, le groupe de trvail sur la cybersécurité recommande fortement que l'ARTAO apporte un appui institutionnel et technique à ces initiatives, notamment en favorisant l'adhésion de ses États membres, en soutenant les mécanismes de coopération régionale et en contribuant à l'intégration de ces projets dans les priorités stratégiques de la sous-région, afin de renforcer durablement la résilience collective face aux cybermenaces.

10 RECOMMANDATIONS ET PLAN D'ACTION

Le groupe de travail sur la cybersécurité formule les recommandations ci-après.

10.1 Recommandations stratégiques

Priorité	Recommandation stratégique
CRITIQUE	Adopter un cadre réglementaire harmonisé de cybersécurité télécom au niveau ARTAO.
HAUTE	Créer la Plateforme Régionale de Partage d'Informations sur les Cybermenaces (PRSIC-ARTAO).
HAUTE	Lancer le Programme Régional de Formation en Cybersécurité des Télécommunications (PRFC-ARTAO).
HAUTE	Établir un réseau de CERT/CSIRT sectoriels interconnectés dans chaque État membre.
MOYENNE	Organiser annuellement un exercice sous-régional de simulation de cyberincidents.
MOYENNE	Développer une bibliothèque de bonnes pratiques cybersécurité adaptées au contexte ouest-africain.
LONG TERME	Créer le Centre Régional d'Excellence en Cybersécurité des Télécommunications (CRECT-ARTAO).

10.2 Plan d'action à court terme (2026-2027)

Les actions prioritaires pour la période immédiate sont les suivantes :

- Validation et adoption du présent rapport final par l'Assemblée Générale de l'ARTAO

- Constitution d'un comité technique de suivi chargé de la mise en œuvre des recommandations
- Développement d'un module de formation introductif disponible en ligne pour tous les régulateurs membres

10.3 Plan d'action à moyen terme (2026-2029)

- Déploiement opérationnel de la PRSIC-ARTAO avec les pays pilotes puis extension progressive
- Lancement du PRFC-ARTAO avec les premiers modules de formation
- Adoption d'un cadre réglementaire minimal harmonisé de cybersécurité télécom
- Premier exercice sous-régional de simulation de crise cyber
- Évaluation à mi-parcours et ajustement du programme de renforcement des capacités

11 Conclusion

La cybersécurité dans la région exige une approche coordonnée, structurée et durable. L'ARTAO joue un rôle central dans la construction d'un écosystème régional de cybersécurité robuste.

Les travaux du Groupe ont souligné que la cybersécurité dans les télécommunications n'est plus une préoccupation secondaire, mais une priorité stratégique essentielle à la confiance des utilisateurs, à la continuité des services essentiels et, en définitive, au développement économique numérique de la sous-région.

Face à l'absence de frontières des cybermenaces, la réponse doit être collective, coordonnée et fondée sur la solidarité entre les États membres de l'ARTAO.

La cybersécurité en Afrique de l'Ouest nécessite une approche coordonnée, structurée et durable. L'ARTAO a un rôle central à jouer dans la construction d'un écosystème régional robuste.

Le présent rapport final du Groupe de Travail sur la Cybersécurité de l'ARTAO dresse un tableau complet des défis, des opportunités et des actions prioritaires pour renforcer la résilience cybernétique du secteur des télécommunications en Afrique de l'Ouest.

Les travaux du groupe ont mis en évidence que la cybersécurité des télécommunications n'est plus une préoccupation annexe mais un enjeu stratégique de premier plan, dont dépendent la confiance des utilisateurs, la continuité des services essentiels et, au final, le développement économique numérique de la sous-région.

Face à des menaces qui ne connaissent pas de frontières, la réponse doit être collective, coordonnée et fondée sur la solidarité entre les États membres de l'ARTAO. Les recommandations formulées dans ce rapport visent à bâtir progressivement cet édifice de sécurité collective, en tenant compte des réalités et des contraintes propres à chaque contexte national.

Le groupe de travail soumet respectueusement ce rapport à l'approbation de l'Assemblée Générale de l'ARTAO et appelle à une mise en œuvre diligente et concertée des mesures préconisées, dans l'intérêt de l'ensemble des utilisateurs des services de télécommunications en Afrique de l'Ouest.

Résumé des engagements recommandés aux États membres
1. Développement d'un système de notification des incidents. 2. Mettre en place un système régional de veille stratégique cyber. 3. Standardiser les méthodes de collecte des incidents. 4. Mise en place d'un mécanisme régional de réponse aux incidents. 5. Organisation d'un forum régional de cybersécurité et des exercices cyberdrills régionaux.
6. Participation aux exercices internationaux et collaboration avec des organisations internationales.