

Convention de Malabo

Décider, financer et vérifier une capacité cyber commune dans l'AES

Synthèse pour les décideurs · 10 septembre 2026

Analyse personnelle de l'auteur

La décision proposée

Faire préparer par les autorités compétentes du Burkina Faso, du Mali et du Niger un programme commun de cybersécurité. Ce programme articulerait les priorités nationales, les fonctions à mutualiser et les responsabilités de coordination à l'échelle de l'AES. Chaque chantier devrait préciser son fondement juridique, son responsable, son financement et la preuve de fonctionnement attendue. Les orientations ci-dessous constituent des propositions de mise en œuvre.

Ce que les faits établissent

Malabo est entrée en vigueur le 8 juin 2023. L'état officiel de l'UA du 2 février 2026 recense 20 ratifications ou adhésions et 20 dépôts sur 55 membres. Dans l'AES, le Niger y figure parmi les déposants ; le Burkina Faso et le Mali n'y présentent ni signature ni ratification. Cet inventaire est daté. [1] [3]

La Convention prévoit stratégie nationale, gouvernance et suivi. [2] Pour l'AES, un cadre commun pourrait soutenir l'harmonisation et la coopération, tout en préservant les responsabilités de chaque État. Les dispositifs publics du Maroc, du Ghana, de Maurice et du Rwanda, comparés dans l'article, offrent des points de référence pour examiner les choix possibles.

Les arbitrages à rendre

Décision	Qui doit trancher ou exécuter	Résultat à demander
Articuler les doctrines et les priorités	Autorités politiques nationales et instance commune habilitée	Services prioritaires, principes partagés et mandats explicites
Organiser l'assistance entre pays	Autorités cyber, équipes de réponse et régulateurs	Échanges sécurisés, procédures et exercice commun
Mutualiser certaines capacités	Autorités budgétaires et responsables de programme	Contributions définies, projets chiffrés et coûts récurrents couverts
Contrôler l'exécution et les droits	Instances de contrôle compétentes	Preuves vérifiées, protection des données et corrections suivies

Les compétences et les mécanismes de coordination doivent être définis conformément aux cadres juridiques applicables.

Ce qu'il faut financer en priorité

Le programme devrait chiffrer les équipes, le partage d'alertes, les exercices et la continuité des services prioritaires. Il préparerait aussi un référentiel commun de sécurité des équipements et une capacité mutualisée d'évaluation. Les projets d'hébergement et d'interconnexion devraient être justifiés par les besoins, les dépendances et les capacités d'exploitation. Personnel, maintenance et formation doivent figurer dans les budgets.

Une progression à organiser

Premiers douze mois. Mandater la coordination technique, désigner les responsables nationaux et arrêter les priorités communes. Définir les règles de partage des informations, tester un canal d'alerte et organiser un exercice conjoint. Chiffrer les projets et leurs dépenses de fonctionnement.

Entre douze et trente-six mois. Déployer progressivement les fonctions mutualisées retenues : analyse des menaces, formation, référentiel des équipements et premières capacités de laboratoire. Relier chaque investissement à des besoins établis et à des compétences disponibles.

Consolidation. Organiser la classification des données, la résilience de l'hébergement et les conditions d'une assistance durable entre les trois pays. Ces horizons, inspirés des propositions du manuscrit, doivent être ajustés après diagnostic et arbitrage budgétaire.

Les preuves à exiger

Objet du contrôle	Preuve utile
Responsabilité	Mandats nationaux et communs définis ; décision de crise exercée
Coopération	Alerte d'essai transmise et traitée entre les trois pays ; délais tracés
Continuité	Restauration testée pour les services prioritaires ; écarts corrigés
Équipements	Évaluations documentées ; accès de maintenance et correctifs vérifiés
Moyens et droits	Contributions exécutées, équipes disponibles et contrôles compétents documentés

Les données publiques peuvent être agrégées ; les détails sensibles doivent rester accessibles aux contrôles habilités. La localisation d'un hébergement et le nombre d'outils acquis doivent être appréciés avec la maîtrise des accès, les compétences et les résultats de reprise.

La question à poser avant chaque dépense

Quel engagement cette dépense exécute-t-elle, qui en répond et quelle preuve permettra d'en juger ? La réponse doit relier le droit, le choix stratégique, le responsable, les moyens et l'exécution, au niveau national comme à celui de la coopération AES.

Cette réflexion est approfondie dans mon livre *Le cyberspace sahélien : un nouveau front*, consacré aux enjeux, aux cybermenaces et à la souveraineté numérique dans l'AES. Actuellement en cours d'édition, il sera bientôt disponible.

Sources essentielles

[1] Union africaine, [fiche officielle de la Convention](#). [2] [Texte intégral](#), art. 24 à 29 et 32. [3] UA, [état des ratifications au 02/02/2026](#). Orientations AES : manuscrit de l'auteur, chapitres 8 à 11 ; développements dans l'article associé.

Note de l'auteur

Les analyses, positions et recommandations de cette synthèse et de l'article associé relèvent exclusivement de l'opinion personnelle de l'auteur, fondée sur son expérience professionnelle, ses réflexions et ses recherches personnelles. Elles n'engagent en aucun cas son employeur, l'Autorité de Régulation des Communications Électroniques et de la Poste du Niger (ARCEP Niger), ni aucune autre institution, autorité ou organisation.

Les éléments factuels reposent sur des sources publiques, vérifiables et référencées. Aucune information interne, confidentielle ou non publique obtenue dans l'exercice de ses fonctions n'a été utilisée. Des erreurs, imprécisions ou données devenues obsolètes peuvent néanmoins subsister.

Corrections et actualisations : feedback@karimgoga.com. Les corrections vérifiées pourront être publiées sur la [page de l'article](#).

Abdoul Karim Mamani Malam Goga

Cybersécurité · GRC · Sécurité des équipements

Portfolio : karimgoga.com | [Lire l'article complet](#)