CREDA
Centre de Recherches et d'Etudes pour le Développement en Afrique

COLLOQUE CYBER 2025
Colloque Sous-régional Ouest Africain sur la Cybersécurité et la Souveraineté Numérique

RAPPORT FINAL
DES TRAVAUX DU COLLOQUE CREDA CYBERSECURE 2025

Sous le Haut Patronage de la Présidence de la République du Sénégal




CYBERSÉCURITÉ ET SOUVERAINETÉ NUMÉRIQUE EN AFRIQUE DE L'OUEST :
ENJEUX, DÉFIS ET SOLUTIONS POUR UNE GOUVERNANCE RESPONSABLE ET UNE PROTECTION RENFORCÉE

13 Octobre 2025

Coordonnateur du Programme
CREDA Cybersecure :

Monsieur Gérard DACOSTA
Ingénieur en Cybersécurité-Coach/Formateur

Rédaction

Comité Scientifique sous la Présidence
de **Monsieur Alioune Badara SY**
(*Coordonnateur de la Rédaction*),
de **Madame TAIROU Alimatou**
(Rapportrice)
et de **Madame Adja Sapé FALL**
(Rapportrice Adjointe)

Lieu : Institut Confucius de l'Université Cheikh Anta DIOP de Dakar (Sénégal)

Table des Matières

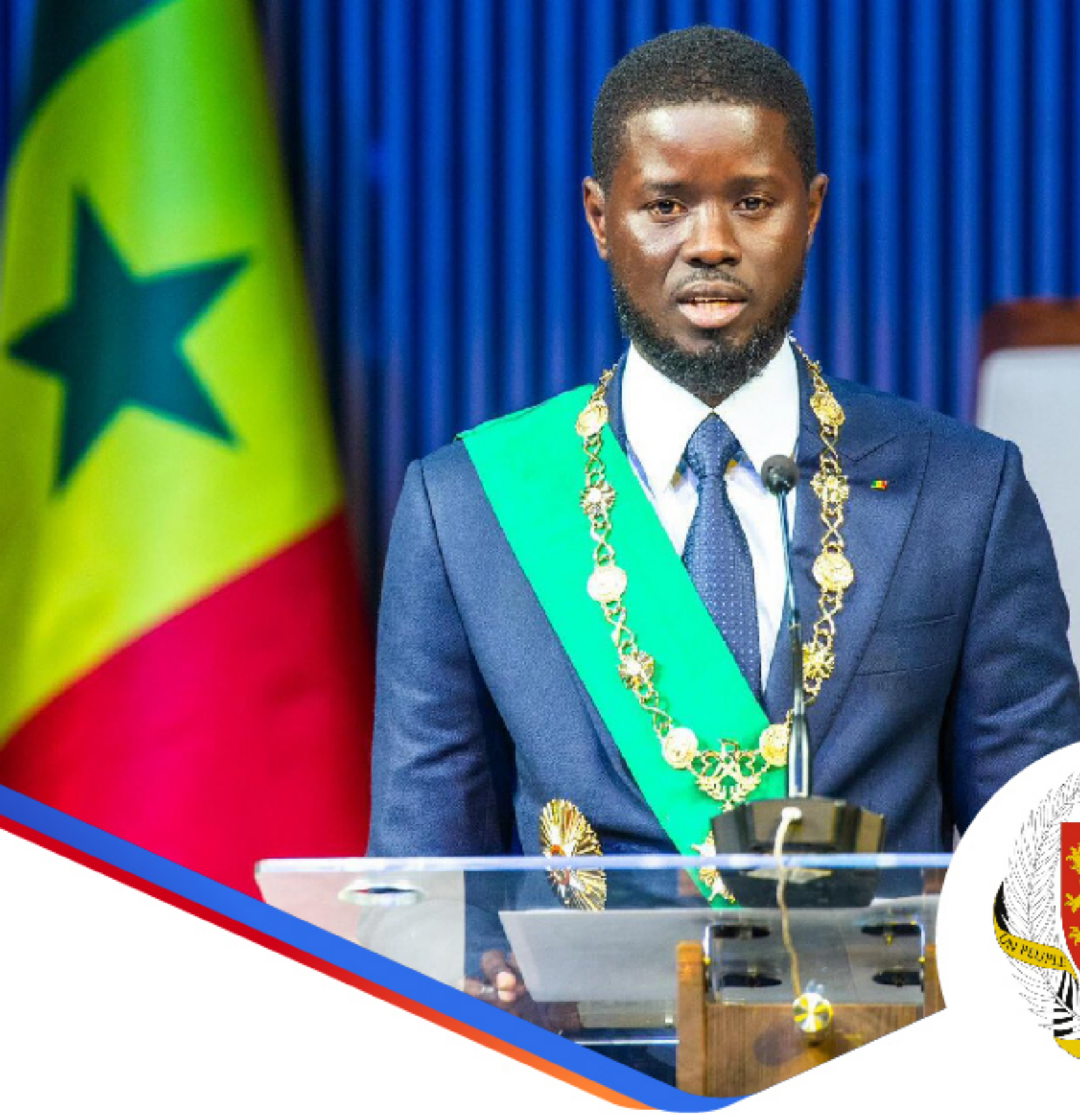
REMERCIEMENTS

Le Comité d'Organisation du Colloque exprime sa profonde gratitude à la **Présidence de la République du Sénégal** pour son appui institutionnel constant, ainsi qu'à **Sénégal Numérique S.A.** pour son accompagnement.

Nos sincères remerciements vont également aux Délégations venues de la **Guinée**, de la **Côte d'Ivoire**, du **Niger** et de la **République Islamique d'Iran (Pays Invité d'Honneur)**, aux Partenaires institutionnels et aux Experts nationaux et internationaux ayant contribué par la richesse de leurs contributions à l'édification d'une vision commune pour une Afrique de l'Ouest numériquement souveraine et sécurisée.

Enfin, le **CREDA** salue la participation engagée des acteurs du secteur privé, de la société civile, du monde académique et des forces de défense et de sécurité (notamment la **Douane Sénégalaise**), dont la mobilisation témoigne d'une prise de conscience collective face à l'urgence numérique.


TOTAL UNITS
40.586.663
46%
32%
0.50 %
0.50 %



Mention Spéciale

à Son Excellence Monsieur

Bassirou Diomaye Diakhar FAYE

Président de la République du Sénégal

Pour son Soutien à la Matérialisation
du **Colloque CREDA Cybersecure 2025**

Mention Spéciale

à Son Excellence le Général Monsieur

Mamadi DOUMBOUYA

Président de la République de Guinée

Pour l'Implication de l'**État Guinéen**
au Colloque CREDA Cybersecure 2025

Mention Spéciale

à Son Excellence le Général Monsieur

Abdourahamane TIANI

Président de la République du Niger

Pour l'Implication de l'**État Nigérien**
au Colloque CREDA Cybersecure 2025

Mention Spéciale

à Son Excellence Monsieur

Alassane Dramane OUATTARA

Président de la République de Côte d'Ivoire

Pour l'Implication de l'**État Ivoirien**
au Colloque CREDA Cybersecure 2025

Mention Spéciale

à Son Excellence

Ayyatolhad Ali KHAMANEI

Guide Suprême

de la République Islamique d'IRAN

Pour l'Implication de l'**État Iranien**

du **Colloque CREDA Cybersecure 2025**

Pays Invité d'Honneur

RÉSUMÉ DU RAPPORT

Le Colloque sur la Cybersécurité et la Souveraineté Numérique en Afrique de l'Ouest a réuni à Dakar les principaux acteurs institutionnels, diplomatiques, techniques et judiciaires pour réfléchir sur les défis croissants du cyberespace et sur la nécessité d'une réponse sous-régionale coordonnée.

Face à la montée des cybermenaces, à la dépendance technologique et à la vulnérabilité des infrastructures critiques, les **États participants** ont réaffirmé la priorité absolue de construire une **gouvernance numérique souveraine**, respectueuse des valeurs africaines et des impératifs de sécurité collective.

La méthodologie adoptée reposait sur une approche participative et collaborative, articulée autour de quatre ateliers thématiques, chacun explorant un pilier essentiel: la Cybersécurité des infrastructures critiques, la Souveraineté Numérique, la lutte contre la cybercriminalité et la protection des données personnelles. Les messages clés issus des échanges mettent en lumière la fragilité des cadres juridiques, le déficit de coordination sous-régionale et la dépendance technologique vis-à-vis des puissances étrangères.

Les recommandations stratégiques convergent vers l'élaboration d'une stratégie nationale et sous-régionale de cybersécurité, la création d'un Conseil ouest-africain de la souveraineté numérique.

Enfin, le Colloque **CREDA Cybersecure** trace des perspectives concrètes pour les prochaines éditions, dans la continuité des travaux initiés à Dakar. Ainsi, la Formation et la Sensibilsation seront les secteurs à explorer pour la prochaine édition.

INTRODUCTION GÉNÉRALE

1 Contexte et Justification

L'Afrique de l'Ouest connaît une expansion numérique rapide, portée par la connectivité croissante, la digitalisation des services publics et l'essor de l'économie numérique. Cependant, cette transformation s'accompagne d'une vulnérabilité accrue. Les cyberattaques, autrefois perçues comme des menaces lointaines, sont désormais une réalité quotidienne pour les États, les entreprises et les citoyens. Face à cette vulnérabilité croissante du cyberespace, la question de la souveraineté numérique s'impose comme un enjeu stratégique majeur. Dans un monde hyperconnecté dominé par des acteurs technologiques mondiaux (GAFAM, clouds étrangers, IoT), la maîtrise des infrastructures, des données et des technologies devient une condition sine qua non de la souveraineté politique, économique et culturelle des nations africaines. C'est dans cette optique que le **CREDA**, avec le soutien de la **Présidence de la République**, a pris l'initiative d'organiser ce colloque, conçu comme un cadre de concertation sous-régionale, un laboratoire d'idées pour l'action collective.

2 Objectifs du Colloque

Le Colloque poursuivait plusieurs objectifs stratégiques :

- **Sensibiliser** les décideurs et les acteurs économiques aux risques et aux opportunités du numérique ;
- **Partager** les expériences et les bonnes pratiques nationales et sous-régionales ;
- **Prévenir** les cybermenaces par la coordination sous-régionale et la planification stratégique ;
- **Protéger** les citoyens et les entreprises à travers une gouvernance numérique responsable et inclusive.

Au-delà des échanges techniques, l'ambition du Colloque était de mobiliser les **États** de la sous-région autour d'un plan d'action commun, posant les fondations d'une gouvernance numérique concertée et souveraine.

3 *Pays Participants en phase pilote*

Le Colloque a réuni des Délégations de plusieurs Pays membres de l'espace francophone ouest-africain, dont le **Sénégal** (Pays hôte), la **Guinée**, la **Côte d'Ivoire** et le **Niger**. La **République Islamique d'Iran est le Pays Invité d'honneur**.

Certains Pays, bien que n'ayant pu être présents physiquement du fait de délai de préparation, ont manifesté leur adhésion immédiate aux principes fondateurs du colloque, témoignant de la volonté collective de bâtir une cybersouveraineté ouest-africaine partagée.

PARTIE I CADRAGE INSTITUTIONNEL ET OUVERTURE OFFICIELLE

L'ouverture du Colloque fut un moment solennel et symbolique, marqué par la richesse des interventions et la diversité des représentations diplomatiques, institutionnelles et techniques.

Des allocutions successives, émanant de la **Présidence de la République du Sénégal** avec son **Représentant Monsieur Massamba GUEYE**, des **Ambassades**, **Ministères** et **Institutions partenaires**, ont mis en exergue la pertinence du thème et la nécessité d'un dialogue multilatéral sur la Cybersécurité. Surtout le rôle d'avant-garde du Sénégal avec le « **New Deal Technologique** ».

Le **Représentant de l'Ambassade d'Iran** a salué l'initiative et a proposé une coopération technique, tandis que les Acteurs gouvernementaux ont insisté sur l'importance de la qualité des processus numériques dans les services publics.

La **Directrice du Cabinet OFBD, Madame Pauline SECK**, a livré un témoignage poignant sur les risques réels du cyberespace, rappelant à travers son expérience personnelle l'urgence d'un encadrement réglementaire et d'une sensibilisation généralisée.

Enfin, le discours de **Monsieur Alioune Badara SY**, Président du **CREDA**, a posé le cadre stratégique et opérationnel des travaux, présentant les quatre ateliers thématiques et réaffirmant la mission de son Organisme c'est-à-dire être un catalyseur de gouvernance numérique responsable en Afrique de l'Ouest.

Dans son intervention, **Monsieur El Hadji Daouda DIAGNE** (Expert International en Cybersécurité et Conseiller Technique Principal du Progamme **CREDA Cybersecure**) a montré l'ampleur de la question mais surtout les solutions possibles avec la mise en place de cadre harmonisé.

Les Représentants des Ministères (Famille – Microfinance) ont montré ont abordé dans le même ordre d'idée.

PARTIE II COMPTE RENDU DES ATELIERS

Atelier I – Cybersécurité et gouvernance sous-régionale des infrastructures critiques

1 Problématique

Cet atelier a permis de mettre en lumière la question cruciale de la vulnérabilité des infrastructures critiques en Afrique de l'Ouest, ces structures vitales qui soutiennent la vie économique et sociale des **États** (réseaux électriques, systèmes de télécommunications, infrastructures sanitaires, financières et hydrauliques). Leur interconnexion croissante, alimentée par la numérisation des services, les rend particulièrement exposées aux cyberattaques transfrontalières, souvent orchestrées depuis l'étranger et dont les effets se propagent au-delà des frontières nationales. L'interdépendance sous-régionale, bien que source de développement, constitue également un facteur de fragilité: une attaque ciblant un pays peut rapidement affecter l'ensemble de la sous-région. Face à ce constat, l'atelier a posé les jalons d'une réflexion commune sur la gouvernance concertée et la résilience collective des infrastructures critiques ouest-africaines.

2 Méthodologie

Les travaux ont été menés selon une approche participative et interactive, privilégiant un format de questions-réponses et de débat ouvert. Cette méthodologie a permis aux participants (experts, représentants institutionnels, opérateurs de services essentiels) d'exprimer librement leurs expériences, leurs difficultés, mais aussi leurs propositions concrètes.

L'objectif était de transformer la session en un véritable laboratoire d'idées, fondé sur la co-construction de solutions pratiques et adaptées aux réalités sous-régionales.

3 Points abordés

Les discussions ont d'abord porté sur la clarification des concepts fondamentaux : cybersécurité, souveraineté numérique, résilience et infrastructures critiques. Ces notions, souvent confondues, ont été redéfinies dans le contexte africain, où la cybersécurité ne se limite plus à la protection des systèmes informatiques, mais englobe désormais la sauvegarde de la vie sociale, économique et institutionnelle.

Le partage d'expériences locales et transfrontalières a permis de dresser une cartographie des menaces sous-régionales, incluant les ransomwares, les intrusions ciblées et les manipulations de données. Des cas concrets ont illustré la nécessité d'une détection précoce des incidents, d'un traitement coordonné des alertes, et d'une communication fluide entre acteurs publics et privés.

Les Participants ont également souligné le rôle crucial des institutions étatiques et techniques (forces de sécurité, agences de Cybersécurité, opérateurs d'importance vitale) dans la mise en œuvre d'un dispositif collectif de défense. Toutefois, ils ont noté des faiblesses structurelles : un déficit de communication interinstitutionnelle, un manque de textes juridiques spécifiques et l'absence de normes sous-régionales harmonisées.

4 Recommandations clés

Les conclusions de cet atelier ont débouché sur des recommandations structurantes :

- Élaborer une feuille de route sous-régionale de Cybersécurité, définissant les priorités, les ressources et les mécanismes de suivi-évaluation communs ;
- Renforcer la coopération public-privé, en impliquant davantage les opérateurs techniques et les entreprises dans la détection et la réponse aux incidents ;

- Promouvoir une gouvernance collective fondée sur le partage d'informations, la mutualisation des moyens et la coordination interétatique ;
- Procéder à une mise à jour des cadres légaux, notamment ceux relatifs aux OIV (opérateurs d'importance vitale opérateurs d'importance vitale) et à la gestion des infrastructures critiques.

L'atelier a ainsi posé les bases d'un projet ambitieux : la construction d'un écosystème de cybersécurité intégré, garantissant la stabilité numérique et la continuité des services essentiels en Afrique de l'Ouest.

Atelier II – Souveraineté numérique et résilience technologique

1 Enjeux abordés

Ce deuxième atelier s'est intéressé à la souveraineté numérique, un concept central mais complexe dans un monde globalisé. Les discussions ont mis en évidence la vulnérabilité des **États africains** face à la domination des grandes entreprises technologiques internationales que sont les **GAFAM**, les fournisseurs de cloud étrangers et les plateformes IoT.

La dépendance aux technologies exogènes fragilise la capacité des nations à maîtriser leurs données, leurs infrastructures et leurs systèmes d'information. À travers des cas pratiques comme ceux de la Chine ou de la Russie, les participants ont pu mesurer la distance entre les ambitions ouest-africaines et les modèles de souveraineté numérique déjà consolidés ailleurs.

2 Contributions notables

Les interventions marquantes ont enrichi le débat :

- **Docteur Gimi Deen TOURÉ (Conseiller Technique du Premier Ministre/Représentant la Guinée)** a introduit la notion de diplomatie des données, en soulignant la question de la territorialité numérique : où se situe réellement la souveraineté d'un État lorsque ses données sont hébergées à l'étranger ? Il a illustré cette réflexion à travers l'idée d'une ambassade de données, espace virtuel où les nations peuvent exercer leur juridiction numérique ;
- **Monsieur Gérard DACOSTA et Monsieur Alioune Badara SY du CREDA** ont développé le concept de souveraineté numérique réfléchie, invitant à dépasser le statut de simples utilisateurs pour devenir concepteurs des technologies que nous consommons. Ils ont insisté sur la formation à la conception, la maîtrise énergétique et la nécessité d'une infrastructure locale autonome ;

- Fort de sa très grande expérience internationale, **Monsieur El Hadji Daouda DIAGNE** a modéré les échanges avec toute la dextérité digne d'un Ingénieur en Cybersécurité qu'il est. Les grandes lignes des conclusions de ces travaux reflètent ses conseils, orientations et expériences dans le domaine de la Cybersécurité.

3 Recommandations stratégiques

Les Participants ont formulé plusieurs pistes d'action :

- Développer dans chaque Pays une stratégie nationale de souveraineté numérique, adaptée à ses réalités économiques et technologiques ;
- Encourager la mutualisation des efforts à l'échelle de la CEDEAO, afin de bâtir une souveraineté numérique sous-régionale cohérente.
- Soutenir la recherche et l'innovation locales, en favorisant la création de laboratoires et d'incubateurs technologiques ;
- Promouvoir des projets pilotes tels que le cloud souverain ouest-africain ou les data centers sous-régionaux, capables de garantir la conservation et la sécurité des données sur le continent.

Cet atelier a ainsi ouvert la voie à une réflexion ambitieuse : celle d'un numérique sous-africain émancipé, fondé sur la connaissance, l'autonomie technologique et la coopération.

Atelier III – Lutte contre la cybercriminalité et coopération judiciaire

1 Constat général

La cybercriminalité s'impose aujourd'hui comme l'un des défis les plus pressants pour les **États** de la sous-région. Cet atelier, tenu en **webinaire** (devant permettre à d'autres Experts qui étaient hors du Continent de participer), a dressé un constat alarmant : la multiplication des fraudes, des attaques numériques, et des détournements de données s'accompagne d'une insuffisance criante de coordination judiciaire régionale. Les cadres légaux actuels peinent à suivre la rapidité de l'évolution technologique, tandis que les dispositifs de preuve numérique demeurent limités. Cette situation crée un vide propice à l'impunité et à la prolifération des crimes numériques.

2 Éléments discutés

Les échanges ont porté sur les failles structurelles du système judiciaire face aux cybermenaces. Des cas emblématiques ont été évoqués, notamment ceux de la **DGID (Direction Générale des Impôts et Domaines)** et d'Ecobank au Sénégal, illustrant la sophistication croissante des attaques et la fragilité des mécanismes de riposte.

Les Participants ont également souligné le manque d'interopérabilité entre les services compétents (police, gendarmerie, régulateurs, banques, entre autres), ainsi que les failles de communication et de coordination qui ralentissent les enquêtes numériques.

3 Initiatives et bonnes pratiques

Malgré ces difficultés, des initiatives prometteuses émergent dans l'écosystème ouest-africain.

Des structures comme la **CENTIF**, l'**OFNAC**, le **GIM-UEMOA** ou la **BCEAO** contribuent activement à renforcer la traçabilité financière et la sécurité des transactions numériques.

L'atelier a également mis en avant deux projets d'envergure continentale :

- Le CIX (**Continental Internet Exchange**), premier réseau africain d'internet souverain, interconnectant plus de 200 millions d'utilisateurs via 47 data centers ;
- Le **Protocole Digital Africain** (ADP), initiative novatrice valorisant les **langues africaines** dans le développement d'algorithmes autochtones.

4 *Recommandations clés*

Les recommandations issues des travaux sont précises et ambitieuses :

- Harmoniser les lois et cadres juridiques entre les Pays de la CEDEAO pour lutter efficacement contre la cybercriminalité ;
- Former les Magistrats et Enquêteurs aux spécificités des infractions numériques et à la gestion des preuves électroniques ;
- Créer des canaux sécurisés d'échange judiciaire pour favoriser la coopération transfrontalière ;
- Mettre en place une Task Force judiciaire CEDEAO, chargée de la coordination des enquêtes et du partage d'informations ;
- Lancer un Programme sous-régional de cybersécurité judiciaire, garantissant une réponse institutionnelle durable face aux menaces cybernétiques.

Atelier IV – Protection des données personnelles et confiance numérique

1 Problématique

La quatrième session a porté sur un enjeu fondamental de la société numérique : la protection des données personnelles, véritable colonne vertébrale de la confiance numérique.

Les intervenants ont reconnu que ces données, désormais considérées comme une ressource stratégique, constituent le nouvel or noir du **XXIe siècle**. Au Sénégal, malgré la loi de 2008 et la création de la **Commission des Données Personnelles (CDP)**, de nombreuses failles juridiques et techniques persistent face à l'évolution rapide des usages numériques.

2 Contributions majeures

Deux interventions majeures ont marqué les débats :

- **Monsieur Yatma NIANG (Juriste)** a analysé en profondeur les objectifs et limites de la loi de 2008, en soulignant son manque de précision sur les lieux de stockage, les publics concernés et les procédures de consentement. Il a également mis en évidence le déficit de formation des Magistrats et Juristes spécialisés.
- **Madame Adja Sapé FALL (Spécialiste des Relations Internationales)** a pour sa part évoqué le vide juridique préoccupant dans des domaines sensibles tels que le harcèlement en ligne, le droit à l'image ou l'extraterritorialité du numérique, plaidant pour une refonte globale du cadre législatif.

3 Points de débat

Le débat a soulevé des questions essentielles :

Comment garantir aux citoyens l'accès et le contrôle de leurs propres données ?

Comment rendre les sanctions plus effectives et dissuasives ?

Les Participants ont dénoncé la faible application des peines, la dépendance excessive aux plateformes étrangères et l'inefficacité du « droit à l'oubli », difficilement applicable dans un environnement numérique mondialisé. Le cas du **GIM-UEMOA**, devenu acteur bancaire, a été cité pour illustrer les dérives possibles d'acteurs opérant en dehors du périmètre initialement prévu par la loi.

4 Recommandations

Les Participants ont unanimement convenu de la nécessité d'une réforme profonde et actualisée de la législation sur les données personnelles.

Les principales recommandations sont les suivantes :

- Réviser la loi de 2008 pour l'adapter aux réalités contemporaines du numérique ;
- Renforcer la CDP (**Commission de Protection des Données Personnelles**), tant dans ses moyens d'action que dans son autorité ;
- Développer des mécanismes de sanctions spécifiques et dissuasives ;
- Lancer des campagnes massives de sensibilisation pour que chaque citoyen connaisse ses droits numériques ;
- Promouvoir la **création d'algorithmes locaux** et la valorisation de l'expertise africaine pour un numérique souverain et éthique.

Cet atelier a clos les travaux sur une note d'engagement collectif : celle de **bâtir une confiance numérique durable**, condition essentielle pour le développement d'une Afrique de l'Ouest résiliente, souveraine et tournée vers l'avenir.

PARTIE III ANALYSE TRANSVERSALE ET ENJEUX STRATÉGIQUES

1 *Défis majeurs identifiés*

Les travaux menés au cours des quatre ateliers ont permis de dresser un diagnostic lucide des défis structurels et stratégiques auxquels se heurte la région ouest-africaine dans sa quête de souveraineté numérique.

Malgré une prise de conscience collective de l'importance du numérique, les Participants ont souligné plusieurs faiblesses qui freinent l'émergence d'un espace digital sécurisé, autonome et durable.

Faiblesses juridiques

L'un des constats les plus saillants demeure la fragilité du cadre juridique relatif à la cybersécurité et à la gouvernance numérique. Dans la majorité des Pays, les textes en vigueur datent de plus d'une décennie, à une époque où les réalités technologiques étaient très différentes.

Les lois nationales n'intègrent pas toujours les enjeux contemporains tels que la protection des données biométriques, la cyberdéfense, les cryptomonnaies, ou encore les cyberattaques transnationales.

Cette obsolescence juridique engendre un vide réglementaire qui complique la sanction des infractions et affaiblit la protection des citoyens, des entreprises et des institutions publiques.

Fragmentation institutionnelle

Les débats ont également révélé une fragmentation préoccupante des structures institutionnelles chargées de la gouvernance numérique. Dans plusieurs **États**, les missions se chevauchent entre Ministères, Agences de régulation, Forces de sécurité et Autorités indépendantes, sans cadre de coordination unifié.

Cette dispersion des compétences entraîne des lenteurs administratives, une duplication des efforts et une dilution des responsabilités.

Les Participants ont plaidé pour une harmonisation institutionnelle et la création de mécanismes clairs de gouvernance multi-acteurs, capables de fédérer les initiatives publiques, privées et académiques.

Manque de coopération inter-États

Sur le plan sous-régional, le manque de coopération opérationnelle entre **États** constitue une faiblesse majeure. Bien que les cybermenaces soient par nature transfrontalières, la réponse reste encore largement nationale, fragmentée et réactive. L'absence de mécanismes de partage d'informations, de protocoles conjoints d'intervention et de mutualisation des moyens techniques empêche la constitution d'un écosystème de cybersécurité intégré à l'échelle de la **CEDEAO**.

Cette situation nourrit une vulnérabilité collective et limite la capacité des Pays à anticiper et à contenir les attaques coordonnées.

Vulnérabilité technique et dépendance extérieure

Enfin, la dépendance technologique à l'égard des solutions étrangères, qu'il s'agisse des systèmes d'exploitation, des infrastructures cloud, ou des logiciels de sécurité, a été unanimement identifiée comme un risque stratégique.

Cette dépendance compromet la souveraineté numérique des États ouest-africains, en confiant à des acteurs extérieurs la gestion ou la détention de données sensibles.

L'absence d'alternatives locales accentue la vulnérabilité technique et freine la montée en puissance des compétences africaines dans le domaine des technologies critiques.

Les Participants ont ainsi souligné la nécessité impérieuse de promouvoir l'innovation endogène, la formation à la conception technologique et le développement de solutions locales, afin de réduire cette dépendance structurelle.

2 Points de convergence des Ateliers

Malgré la diversité des thématiques abordées, les quatre ateliers ont convergé vers un ensemble d'orientations communes qui traduisent une vision partagée du futur numérique de la sous-région.

Ces points de convergence témoignent d'un alignement stratégique entre les différents acteurs (publics, privés, académiques et institutionnels) autour d'une ambition collective : celle de bâtir une Afrique de l'Ouest souveraine, sécurisée et inclusive dans le domaine numérique.

Urgence d'une stratégie nationale et sous-régionale

Tous les Participants ont reconnu l'urgence d'élaborer et de mettre en œuvre des stratégies nationales de cybersécurité et de souveraineté numérique, articulées autour d'une vision sous-régionale concertée.

Ces stratégies devront intégrer la prévention des menaces, la résilience des infrastructures critiques, la protection des données et la gouvernance éthique de l'intelligence artificielle.

L'objectif est de dépasser la logique de réaction ponctuelle pour instaurer une culture proactive de cybersécurité, inscrite dans les politiques publiques de développement.

Rôle crucial de la formation et de la recherche

La formation et la recherche scientifique sont apparues comme des leviers incontournables pour construire la souveraineté numérique.

Les Participants ont insisté sur la nécessité de former des experts locaux en Cybersécurité, en Cryptographie, en Analyse forensique et en Gouvernance de l'information.

De même, ils ont plaidé pour la création de centres de recherche appliquée, capables de générer des connaissances et des innovations adaptées aux contextes ouest-africains. Cette montée en compétence constitue la clé d'une indépendance technologique durable.

Besoin d'un plaidoyer politique fort

Un autre point de convergence majeur concerne le rôle du leadership politique. Les Participants ont souligné que, sans volonté politique affirmée, aucune stratégie numérique ne peut se déployer efficacement.

Ils ont donc appelé à un plaidoyer sous-régional de haut niveau, visant à sensibiliser les décideurs, à mobiliser les ressources budgétaires et à inscrire la Cybersécurité au cœur des priorités gouvernementales.

Ce plaidoyer doit également s'accompagner d'un engagement diplomatique africain, afin de défendre les intérêts du Continent dans les instances internationales de régulation du cyberespace.

Coopération publique–privée–institutionnelle

Enfin, la coopération entre les secteurs public, privé et institutionnel est apparue comme une condition essentielle à la réussite de toute politique de Cybersécurité.

Les acteurs privés, souvent en première ligne face aux attaques, disposent d'une expertise technique précieuse, tandis que les institutions publiques détiennent la légitimité réglementaire et la capacité de coordination.

L'établissement de partenariats stratégiques durables entre ces différents pôles constitue donc une nécessité impérieuse pour créer un écosystème cohérent et résilient.

3 *Cadre institutionnel en évolution*

L'analyse transversale des échanges a également mis en évidence une évolution institutionnelle notable au Sénégal, porteuse d'espoir pour l'ensemble de la sous-région.

Création du Conseil National du Numérique (CNN)

La récente création du **Conseil National du Numérique (CNN)**, en 2025 marque une étape décisive dans la structuration de la gouvernance numérique au Sénégal.

Cette institution se veut un organe stratégique de concertation, d'orientation et de prospective, chargée d'assurer la cohérence des politiques publiques en matière de numérique, d'innovation et de Cybersécurité.

Le **CNN** symbolise une volonté politique forte de placer le numérique au cœur du développement national, tout en garantissant la souveraineté technologique et la sécurité des systèmes critiques. Son rôle d'interface entre l'**État**, les acteurs privés et la société civile pourrait inspirer d'autres Pays de la sous-région, en tant que modèle de gouvernance participative du numérique.

Conclusion partielle

En définitive, l'analyse transversale des travaux du Colloque révèle une prise de conscience collective et une volonté de transition vers un modèle africain de gouvernance numérique fondé sur la sécurité, la souveraineté et la solidarité. Les défis demeurent nombreux, mais les bases d'un dialogue durable et structuré sont désormais posées.

L'Afrique de l'Ouest dispose de ressources humaines, intellectuelles et institutionnelles considérables pour affirmer sa place dans le cyberespace mondial, à condition de consolider la coopération régionale, d'unifier les cadres juridiques et de promouvoir une véritable culture de la cyber sécurité.

PARTIE IV RECOMMANDATIONS GÉNÉRALES ET PERSPECTIVES

1 Recommandations structurantes

Les conclusions du Colloque sur la Cybersécurité et la Souveraineté numérique en Afrique de l'Ouest ont abouti à une série de recommandations structurantes visant à consolider les acquis, combler les lacunes identifiées et donner une orientation claire à l'action sous-régionale. Ces recommandations s'inscrivent dans une vision stratégique à moyen et long terme, fondée sur la sécurité, la coopération et l'autonomie technologique des **États ouest-africains**.

Élaboration prioritaire d'une Stratégie Nationale de Cybersécurité

La première urgence identifiée par les experts et les représentants institutionnels réside dans la mise en place d'une stratégie nationale de Cybersécurité dans chaque pays de la sous-région.

Cette stratégie devra être conçue comme un instrument transversal de gouvernance publique, articulant la protection des infrastructures critiques, la formation des ressources humaines, la sensibilisation citoyenne et la coordination interinstitutionnelle.

Elle devra également intégrer une approche prospective, tenant compte des évolutions rapides du cyberespace, de la montée de l'intelligence artificielle et des nouvelles formes de criminalité numérique.

L'objectif est d'ancrer durablement la Cybersécurité dans les priorités étatiques, au même titre que la défense, la santé ou l'éducation.

Création d'une structure spécialisée de coordination stratégique

Les Participants ont unanimement reconnu la nécessité de créer, au niveau national et sous-régional, une structure

permanente de coordination stratégique dédiée à la Cybersécurité et à la Souveraineté Numérique.

Cette entité aurait pour mission de centraliser les informations, de coordonner les réponses aux incidents majeurs et de faciliter la coopération entre les forces de défense, les agences techniques et les opérateurs privés.

Elle jouerait également un rôle de veille, de conseil et d'orientation stratégique auprès des décideurs politiques, garantissant la cohérence et la continuité des politiques numériques dans un environnement en perpétuelle mutation.

Élaboration d'un Plan sous-régional de résilience numérique

Au-delà des frontières nationales, la cybersécurité appelle une réponse collective.

Ainsi, il a été proposé l'élaboration d'un Plan sous-régional de résilience numérique, sous l'égide de la **CEDEAO** et avec l'appui technique des institutions partenaires.

Ce plan aurait pour vocation de renforcer la coopération entre **États membres**, d'harmoniser les protocoles d'intervention en cas d'attaque majeure et de mutualiser les ressources humaines, matérielles et financières.

Il constituerait un instrument de solidarité numérique sous-régionale, garantissant la continuité des services essentiels et la stabilité institutionnelle face aux menaces transfrontalières.

Mutualisation des ressources techniques et juridiques

L'efficacité d'une stratégie régionale repose sur la mutualisation des compétences et des moyens.

Les Participants ont souligné que de nombreux Pays disposent déjà de structures techniques et juridiques performantes, mais isolées les unes des autres.

Il s'agit désormais de les interconnecter, de partager les expertises, les cadres normatifs et les outils de surveillance,

afin de créer une véritable communauté de Cybersécurité ouest-africaine.

Cette mutualisation devrait aussi s'étendre à la recherche, à la formation et à l'élaboration de référentiels juridiques communs, favorisant une approche harmonisée et solidaire de la Cybersécurité sous-régionale.

Mise en place d'une école sous-régionale de cybersécurité

L'un des points d'accord les plus forts du Colloque concerne la **création d'une école sous-régionale de cybersécurité**, qui deviendrait un centre d'excellence ouest-africain dédié à la formation, à la certification et à la recherche appliquée dans le domaine du numérique sécurisé.

Cette institution académique aurait pour mission de former des Ingénieurs, des Magistrats, des Analystes et des Décideurs capables de répondre aux défis émergents du cyberespace africain.

Elle favoriserait également la production de savoirs endogènes et le développement de technologies locales, tout en servant de levier d'intégration sous-régionale et d'émancipation technologique.

Plaidoyer pour une convention ouest-africaine de souveraineté numérique

Enfin, le Colloque a formulé une recommandation d'envergure politique : **Un plaidoyer pour l'adoption d'une Convention ouest-africaine sur la Souveraineté numérique**.

Cette convention établirait un cadre juridique et diplomatique commun, définissant les principes fondamentaux de la souveraineté numérique ouest-africaine : protection des données, autonomie technologique, sécurité collective et respect des droits numériques des citoyens.

Elle renforcerait la position des Pays ouest-africains dans les négociations internationales et garantirait une **voix unie de l'Afrique de l'Ouest** dans les instances de gouvernance mondiale du cyberespace.

2 Recommandations spécifiques aux parties prenantes

Afin d'assurer la mise en œuvre effective des recommandations précédentes, le Colloque a précisé les responsabilités spécifiques de chaque catégorie d'acteurs impliquée dans la gouvernance du numérique et la Cybersécurité.

Aux États : harmonisation des cadres législatifs et politiques

Les Gouvernements sont appelés à jouer un rôle moteur dans l'harmonisation des législations nationales relatives à la Cybersécurité, à la protection des données et à la criminalité numérique. Ils doivent œuvrer à la création de politiques publiques cohérentes, alignées sur les standards internationaux, tout en veillant à préserver les spécificités socioculturelles et économiques africaines.

L'engagement politique doit se traduire par un financement durable de la Cybersécurité, l'intégration du numérique dans les programmes scolaires, et le renforcement des cadres de coopération régionale.

Aux institutions judiciaires : formation continue et coopération renforcée

Les institutions judiciaires constituent le dernier rempart de la Cybersécurité, en assurant la sanction effective des infractions et la protection des droits fondamentaux.

Les Participants ont insisté sur la nécessité d'une formation continue des Magistrats et des Enquêteurs, afin de les outiller face à la complexité croissante des crimes numériques. La mise en place de canaux sécurisés d'échange judiciaire et de mécanismes de coopération transfrontalière est également essentielle pour accélérer les enquêtes et améliorer la traçabilité des flux illicites.

Aux Partenaires Techniques et au Monde Académique : soutien à la souveraineté numérique

Les Partenaires Techniques Internationaux, ainsi que les Institutions Académiques, sont invités à soutenir la souveraineté numérique ouest-africaine non pas par substitution, mais par accompagnement.

Leur rôle doit consister à transférer des compétences, à financer la recherche locale et à co-construire des projets structurants, tels que les clouds souverains ouest-africains, les laboratoires d'innovation ou les observatoires sous-régionaux de la cybersécurité.

La priorité doit être donnée à la création de valeur sur le Continent, afin de garantir un développement durable et autonome du secteur.

Au secteur privé : conformité, éthique et collaboration

Les entreprises, notamment les opérateurs télécoms, les banques, les startups et les prestataires technologiques, sont des acteurs de première ligne dans la Cybersécurité.

Elles sont encouragées à adopter des normes de conformité et d'éthique numérique élevées, à renforcer leurs dispositifs de sécurité interne et à collaborer activement avec les autorités publiques lors de la détection et de la gestion des incidents.

Leur engagement en matière de transparence, de protection des données clients et de responsabilité sociale est un pilier fondamental de la confiance numérique.

À la population : sensibilisation et appropriation des droits numériques

Enfin, le citoyen demeure le maillon central de la chaîne de sécurité numérique.

Les participants ont souligné l'importance de campagnes massives de sensibilisation visant à éduquer les populations sur les bonnes pratiques en ligne, la protection de leurs données personnelles et la reconnaissance de leurs droits numériques.

L'appropriation de ces droits doit s'accompagner d'une citoyenneté numérique active et responsable, condition sine qua non pour ancrer la confiance et la sécurité dans l'espace numérique ouest-africain.

Conclusion générale

Le Colloque sur la Cybersécurité et la Souveraineté Numérique en Afrique de l'Ouest s'est conclu sur un bilan extrêmement positif, marqué par une forte mobilisation, une richesse des échanges et une convergence des visions.

Les débats ont permis d'établir un diagnostic clair des défis actuels, tout en dessinant les contours d'une feuille de route ambitieuse et réaliste pour la sous-région.

Une prise de conscience manifeste s'est exprimée à travers l'engagement des différentes parties prenantes que sont les États, les institutions, les entreprises, les chercheurs et la société civile, tous unis autour d'un objectif commun : bâtir une Afrique de l'Ouest numériquement souveraine, compétente et résiliente.

Les travaux ont jeté les bases d'un projet historique : la **préparation des Assises sous-régionales de la Souveraineté numérique en Afrique de l'Ouest**, prévues pour 2026, dont la formation et la sensibilisation seront les axes d'intervention au niveau du cyberespace.

En somme, le Colloque de Dakar aura été bien plus qu'un simple espace de discussion : il marque le **début d'un mouvement collectif et structurant**, porteur d'un avenir numérique souverain, sûr et durable pour toute l'Afrique de l'Ouest.

Nota Bene :

Pour des besoins de protection des données personnelles, la Feuille de présence n'est pas publiée.

Monsieur Alioune Badara SY

Président du CREDA
Expert en Ingénierie du Développement
Maître d'œuvre du Programme CREDA Cybersecure

Les Partenaires du Programme CREDA Cybersecure

Téléphones : + 221 70 321 44 02 / + 221 77 380 45 49 - E-mail : creda28creda@yahoo.fr