NOTE DE RECHERCHE N°216
OCTOBRE 2026

Thinking Africa

LES NOUVELLES FORMES DE MENACES À LA PAIX ET À LA STABILITÉ EN AFRIQUE

À L'ÈRE DU NUMÉRIQUE ET DE L'INTELLIGENCE ARTIFICIELLE

Auteur: Neema Toyb

Table des matières

À propos de l'auteure : 2
Quand l'information devient un champ de bataille : l'Afrique francophone face aux menaces numériques 2
1. Des États qui se numérisent plus vite qu'ils ne se protègent 3
2. Désinformation et guerre cognitive 4
3. L'intelligence artificielle au service de la manipulation 5
4. Des conflits armés augmentés 6
5. La géopolitique des infrastructures 6
6. Faire entrer la menace informationnelle dans l'alerte précoce 7
Conclusion : *quatre chantiers prioritaires* 9
Références 10

À propos de l'auteure :

Neema Toyb est conseillère stratégique, spécialiste de la diplomatie économique et des questions de paix et de sécurité en Afrique. Depuis plus de quinze ans, elle travaille avec des institutions publiques, des organisations internationales et des acteurs privés dans des contextes de transition et de fragilité institutionnelle, notamment sur la prévention des conflits et la mobilisation de partenariats. Ses travaux portent sur la souveraineté, les menaces hybrides et les technologies émergentes, ainsi que sur leurs liens avec le développement économique. Son approche privilégie des solutions ancrées dans les réalités africaines, le renforcement des capacités locales, la coopération régionale et les dynamiques Sud-Sud. Elle contribue aux travaux de Thinking Africa et participe à des réflexions sur la paix, la sécurité et la gouvernance africaines. Elle défend une vision d'une Afrique capable de produire ses propres réponses, normes et modèles de résilience.

Quand l'information devient un champ de bataille : l'Afrique francophone face aux menaces numériques

Rumeurs virales, deepfakes, cyberattaques contre les fichiers d'État, drones aux mains de groupes armés : le numérique ne crée pas les conflits en Afrique francophone, mais il les accélère et les rend plus difficiles à voir venir. Cet article examine cinq de ces menaces et propose une piste concrète : apprendre aux systèmes d'alerte précoce à lire les signaux informationnels.

Vers le 20 janvier 2024, en pleine Coupe d'Afrique des nations, une vidéo montrant un village en flammes a commencé à circuler sur WhatsApp en Côte d'Ivoire. Le texte qui l'accompagnait, rédigé en mooré, affirmait que des cultivateurs burkinabè venaient d'être attaqués par des Baoulé dans la région de Bouaké. Le service de vérification de l'Agence ivoirienne de presse a démenti l'information. Mais, comme l'a relevé l'agence, la vidéo est arrivée au pire moment, alors que des milliers de supporters burkinabè se trouvaient à Bouaké pour les matchs de poule.

L'épisode n'a rien d'exceptionnel. Il résume même assez bien ce que le numérique change à la paix sur le continent. Un contenu fabriqué en quelques minutes, dans une langue que les plateformes ne surveillent pas, s'appuie sur une tension réelle et choisit son moment. Le numérique ne crée pas les conflits. Il les accélère, il les déplace, et surtout il brouille les signaux qui permettaient jusqu'ici de les anticiper.

L'Afrique francophone constitue un observatoire particulièrement utile de ces dynamiques, en raison de la rapidité de sa numérisation, de la diversité de ses espaces linguistiques et de la fragmentation de ses cadres de coopération.

Le premier de ces traits tient au rythme. On s'y connecte vite, on s'y protège lentement. Les services publics se numérisent, les registres d'état civil deviennent biométriques, les résultats électoraux transitent par des portails en ligne, alors que la majorité des États africains restent classés dans les catégories les plus faibles de l'indice mondial de cybersécurité de l'UIT.

Le deuxième tient à la langue. Les grandes plateformes investissent d'abord là où se trouvent leurs marchés publicitaires. Les documents internes de Facebook divulgués en 2021 ont révélé que 87 % de son budget de lutte contre la désinformation allait aux États-Unis, contre 13 % pour le reste du monde. Le français parlé en Afrique y est mal couvert, et le mooré, le bambara, le fulfuldé ou le lingala le sont sans doute encore moins, les plateformes ne publiant pas les moyens qu'elles consacrent à ces langues. Or l'Afrique compte désormais près des deux tiers des 396 millions de francophones recensés par l'OIF en 2026.

Le troisième tient à la politique. L'espace francophone africain est aujourd'hui fragmenté. Le Burkina Faso, le Mali et le Niger ont quitté la CEDEAO en janvier 2025, puis annoncé en mars leur retrait de l'Organisation internationale de la Francophonie. Ces pays restent francophones par l'usage, mais ils sortent des cadres de coopération qui auraient pu aider à gérer ces menaces, au moment même où le Sahel en concentre plusieurs.

Les pages qui suivent examinent cinq menaces : la vulnérabilité d'États qui se numérisent sans se protéger, la désinformation, l'usage malveillant de l'intelligence artificielle, la transformation des conflits armés et la dépendance aux infrastructures étrangères. L'argument de cet article est que les systèmes africains d'alerte précoce doivent désormais intégrer les signaux informationnels, au même titre que les indicateurs politiques, sécuritaires et humanitaires. Conçus pour un monde où la rumeur voyageait moins vite, ils passent aujourd'hui à côté d'une partie des signaux faibles qui annoncent les crises.

1. Des États qui se numérisent plus vite qu'ils ne se protègent

Au début du mois de février 2026, la Direction de l'automatisation des fichiers (DAF) du Sénégal, qui gère les cartes d'identité, les passeports et les données biométriques de toute la population, a dû fermer temporairement ses services après une cyberattaque. Un groupe se faisant appeler Green Blood a revendiqué l'opération et affirmé détenir 139 téraoctets de données. Selon le média spécialisé The Record et Africa Cybersecurity Magazine, les autorités ont confirmé l'incident et suspendu la production des cartes d'identité, sans confirmer l'ampleur de la fuite revendiquée ; un responsable policier a même assuré que les données des citoyens restaient intactes. L'affaire est survenue alors que l'État et son prestataire, la société malaisienne IRIS Corporation, s'opposaient sur des paiements.

On ne sait pas encore ce qui a réellement quitté les serveurs de la DAF. Mais l'épisode suffit à montrer le problème. Un an plus tôt, Dakar lançait son « New Deal technologique » pour moderniser l'administration. Le Sénégal n'a rien d'un cas isolé : partout, les États centralisent des données très sensibles, dépendent souvent d'un prestataire étranger unique et découvrent leurs failles au moment où elles sont exploitées.

La cybercriminalité ordinaire prospère sur le même terrain. Selon le rapport d'INTERPOL et d'AFRIPOL publié en juin 2025, elle représente désormais plus de 30 % de la criminalité signalée en Afrique de l'Ouest et de l'Est. Escroqueries en ligne, rançongiciels, fraude au président, sextorsion : les schémas sont connus, les capacités d'enquête beaucoup moins.

En quoi est-ce une question de paix, et pas seulement de police ? Parce que les données les plus exposées sont aussi les plus politiques. Un fichier électoral compromis, une base biométrique détournée ou une panne le soir d'un scrutin peuvent suffire à faire basculer une contestation. Le Nigeria l'a vécu en février 2023. Le portail qui devait publier les résultats de l'élection présidentielle bureau par bureau a connu de longs dysfonctionnements. La commission électorale a parlé d'un problème technique ; le ministre des Communications, lui, a fait état d'environ 12 millions de tentatives d'attaque pendant le scrutin. Personne n'a pu trancher de façon convaincante, et l'opposition s'est engouffrée dans le doute.

C'est là que le retard institutionnel coûte le plus cher. Un État qui ne dispose pas d'une équipe nationale de réponse aux incidents informatiques (CERT), disponible jour et nuit et capable d'expliquer publiquement ce qui s'est passé, laisse le terrain aux récits concurrents. La cybersécurité devient alors une affaire de confiance publique autant que de technique.

2. Désinformation et guerre cognitive

En mars 2024, l'Africa Center for Strategic Studies a recensé 189 campagnes de désinformation documentées visant des publics africains, soit près de quatre fois plus qu'en 2022. Près de 60 % d'entre elles étaient parrainées par des États étrangers. Le centre précise que ce décompte est sans doute inférieur à la réalité.

Les chiffres disent l'ampleur. Les cas disent les conséquences. Dans l'Est de la RDC, en 2022, des rumeurs accusant la MONUSCO de vendre des armes aux groupes rebelles ont nourri des manifestations violentes contre ses bases ; elles ont fait cinq morts parmi les Casques bleus et plus de trente parmi les manifestants. Dans les régions anglophones du Cameroun, des réseaux liés aux belligérants ont diffusé des informations personnelles sur des civils, une pratique qui a peut-être conduit à des exécutions sommaires. Et il y a Bouaké. Dans les trois cas, le contenu n'a pas eu besoin d'être sophistiqué. Il lui a suffi de toucher une tension déjà là.

Des influences extérieures mieux documentées

Une partie de ces campagnes vient de l'extérieur, et l'on commence à en savoir plus sur leur fonctionnement. En février 2026, le consortium Forbidden Stories a publié une enquête fondée sur 1 431 pages de documents internes russes. D'après l'enquête, le réseau d'influence autrefois animé par l'entourage d'Evgueni Prigojine est désormais supervisé par le renseignement extérieur russe (SVR). Il aurait disposé d'environ 7,3 millions d'euros entre janvier et octobre 2024 pour des opérations dans une trentaine de pays du Sud, notamment en Afrique. D'autres acteurs utilisent des leviers différents. Les analyses du MERICS et de Freedom House décrivent par exemple le poids de Huawei dans les réseaux africains et dans des projets de « villes intelligentes » équipés de reconnaissance faciale. Ces stratégies n'ont ni les mêmes moyens ni les mêmes objectifs, et il serait trompeur de les confondre.

L'angle mort des langues

C'est ici que la dimension francophone devient décisive. La désinformation qui fait des dégâts circule rarement en anglais, et pas toujours en français. Le haoussa compte plus de 70 millions de locuteurs. Au Sahel, la propagande des groupes jihadistes passe en bonne partie par les langues locales, le fulfuldé ou le bambara notamment ; dans l'Est de la RDC, les messages qui attisent les tensions circulent souvent en swahili ou en lingala. Ces langues sont celles des messages vocaux sur WhatsApp et des émissions de radio, et ce sont aussi celles pour lesquelles la modération automatisée est la moins développée. Une plateforme qui modère mal le français d'Abidjan a peu de chances de bien modérer le mooré de Bouaké.

Le problème ne s'arrête pas à la modération. Il touche aussi la découvrabilité, c'est-à-dire ce que les moteurs de recherche, les algorithmes de recommandation, les plateformes de streaming et les magasins d'applications rendent visible ou laissent dans l'ombre. Un média local, un podcast en wolof ou un service public d'information en lingala existent parfois, mais remontent rarement dans les résultats et les fils d'actualité, faute d'audience suffisante aux yeux des algorithmes.

Or un espace où l'information fiable en langue nationale est introuvable laisse le champ libre à ceux qui produisent du faux. La question dépasse alors la désinformation: elle touche à la souveraineté culturelle et informationnelle, c'est-à-dire à la capacité d'une société à se voir et à s'entendre dans ses propres langues.

Quand les États manipulent aussi

Il faut enfin regarder du côté des gouvernements eux-mêmes. Plusieurs régimes africains utilisent des réseaux de comptes coordonnés pour discréditer l'opposition ou la société civile. Selon les enquêtes du Citizen Lab, d'Amnesty International et du Pegasus Project en 2021, le logiciel espion Pegasus aurait servi à cibler des journalistes et des militants dans plusieurs pays, dont le Maroc, le Rwanda et le Togo, ce que les gouvernements concernés contestent.

Cette réalité a une conséquence directe pour quiconque veut renforcer les capacités numériques des États : les outils de cybersécurité peuvent servir à surveiller. Tout programme d'appui devrait donc comporter au minimum trois garanties : une clause d'usage exclusivement civil et non répressif, un mécanisme de contrôle indépendant, et la suspension automatique de l'aide en cas de détournement avéré.

Les diasporas jouent ici un rôle ambivalent. Depuis Paris, Bruxelles ou Montréal, certains attisent des conflits qu'ils ne vivent pas et relaient des récits partisans avec une liberté que leurs proches restés au pays n'ont pas toujours. D'autres financent la reconstruction, servent de médiateurs informels ou démentent les rumeurs. Les politiques de résilience gagneraient à les traiter comme des acteurs, pas seulement comme un risque.

3. L'intelligence artificielle au service de la manipulation

Au printemps 2025, des chansons générées par intelligence artificielle ont envahi les réseaux sociaux en Afrique de l'Ouest. On y entendait des voix imitant Beyoncé ou Rihanna chanter les louanges du capitaine Ibrahim Traoré, chef de la junte burkinabè. Personne, ou presque, ne croyait vraiment que Beyoncé s'était mise à la politique sahélienne. Ce n'était pas le but. Il s'agissait de saturer l'espace, de rendre un récit omniprésent et sympathique. La propagande devenait un divertissement.

L'intelligence artificielle générative a fait chuter le coût de la manipulation. Ce qui demandait autrefois une équipe, des studios et du temps peut se faire aujourd'hui avec un ordinateur portable et quelques heures. Au Soudan, en 2023, une enquête de la BBC a mis au jour des enregistrements attribués à l'ancien président Omar el-Béchir, fabriqués par clonage vocal, vus des centaines de milliers de fois sur TikTok en pleine guerre civile, ajoutant à la confusion sur qui parlait au nom de qui.

Le danger le plus subtil n'est pourtant pas le faux qui trompe. C'est le doute qui paralyse. Le Gabon l'a montré avant même la diffusion massive de ces outils. Fin décembre 2018, le président Ali Bongo, affaibli par un AVC, est apparu dans une vidéo de vœux que ses adversaires ont jugée suspecte. Certains y ont vu un montage, voire un deepfake. Le 7 janvier 2019, un groupe de militaires tentait un coup d'État en invoquant notamment cette vidéo. Les experts consultés par la suite n'y ont trouvé aucune trace de manipulation. Les juristes américains Robert Chesney et Danielle Citron ont donné un nom à ce phénomène : le « dividende du menteur ».

Quand tout peut être faux, le vrai lui-même devient contestable, et chacun peut rejeter une preuve gênante en criant au trucage.

Cette menace prend une forme particulière en Afrique, où la parole politique et religieuse circule largement par l'audio : messages vocaux sur WhatsApp, radios communautaires, prêches enregistrés. Un faux message d'un chef religieux, d'un commandant ou d'un ministre peut déclencher une réaction collective avant qu'un démenti n'ait la moindre chance d'arriver. Or il n'existe pratiquement pas d'outils publics de détection adaptés aux langues dans lesquelles ces contenus circulent. Le faux n'a d'ailleurs pas besoin d'être parfait. Il lui suffit d'être plausible au bon moment.

4. Des conflits armés augmentés

Pendant longtemps, la maîtrise du ciel a été un privilège d'État. Ce n'est plus le cas. Au Sahel, le JNIM, affilié à al-Qaïda, et l'État islamique au Sahel utilisent désormais des drones commerciaux modifiés, d'abord pour observer, puis de plus en plus pour larguer des charges explosives ou mener des attaques kamikazes. Selon les chercheurs et les données de conflit cités par la revue Africa Defense Forum, plus d'une dizaine de frappes de ce type ont été recensées au Burkina Faso depuis février 2025. En Libye, le Groupe d'experts des Nations unies a décrit dès 2021 l'emploi d'une munition rôdeuse capable de frapper sans intervention humaine directe.

Les États s'équipent aussi. Selon l'Atlantic Council, plusieurs armées sahéliennes ont acquis des drones turcs Bayraktar TB2 à partir de 2022, puis des appareils plus lourds de type Akıncı en 2024. Ces transferts s'accompagnent de formations, de maintenance et donc de liens durables avec les fournisseurs. Les conflits africains deviennent ainsi des espaces de déploiement rapide de technologies militaires nouvelles, souvent avec l'accord de gouvernements pressés de monter en puissance, et dans des contextes où la pression diplomatique internationale reste faible.

La connectivité elle-même devient un enjeu militaire. Selon l'armée nigériane et des chercheurs de la Global Initiative against Transnational Organized Crime, cités par Africa Defense Forum, des groupes comme le JNIM ou l'État islamique en Afrique de l'Ouest utilisent des terminaux Starlink pour communiquer hors des réseaux surveillés, du lac Tchad au Liptako-Gourma. Le même service permet aussi à des populations de contourner les coupures d'Internet décidées par leurs gouvernements. Une connectivité privée, pilotée depuis l'étranger, est à la fois une ressource pour les civils et un défi pour les États, et aucune doctrine africaine ne dit encore comment la traiter.

La guerre des récits et l'espace humanitaire

C'est sans doute dans la guerre de l'information que le changement est le plus profond. Au Tigré, entre 2020 et 2022, chaque camp disposait de son propre écosystème médiatique en ligne et diffusait sa version des faits en continu. Les humanitaires en ont payé le prix. Fin juillet 2021, les autorités éthiopiennes ont suspendu les activités de MSF Hollande et du Conseil norvégien pour les réfugiés, accusés de « diffusion de désinformation ». En septembre, sept hauts responsables onusiens étaient déclarés persona non grata. Un an plus tard, quand des combattants du TPLF ont saisi du carburant dans un entrepôt du Programme alimentaire mondial à Mekele, des campagnes en ligne ont aussitôt accusé l'agence de complicité.

Ce schéma se retrouve aujourd'hui au Sahel et dans l'Est de la RDC. Quand il devient impossible de s'accorder sur des faits de base, la médiation se grippe. Quand les médiateurs et les humanitaires sont discrédités en ligne, leur accès se réduit sur le terrain. La désinformation n'accompagne plus seulement la guerre : elle en façonne le déroulement.

5. La géopolitique des infrastructures

Le 14 mars 2024, un glissement sous-marin au large de la Côte d'Ivoire a endommagé quatre câbles qui relient l'Afrique de l'Ouest au reste du monde : WACS, MainOne, SAT-3 et ACE. En quelques heures, une dizaine de pays ont vu leur connexion s'effondrer ou ralentir fortement. Banques, administrations, opérateurs de mobile money ont tourné au ralenti pendant des jours. Un mois plus tôt, en mer Rouge, l'ancre d'un cargo touché par une attaque des Houthis avait sectionné plusieurs câbles, dont Seacom et AAE-1, qui desservent l'Afrique de l'Est.

Ces deux épisodes n'avaient rien de malveillant envers l'Afrique. Ils ont pourtant montré à quel point la connectivité du continent repose sur quelques points de passage, et combien un accident ou un conflit lointain peut avoir des effets immédiats. L'Afrique abrite par ailleurs moins de 1 % de la capacité mondiale de centres de données. L'essentiel de ses données, y compris des données publiques, est hébergé ailleurs.

La dépendance ne s'arrête pas aux câbles. Les équipements de réseau, les systèmes d'identité, les plateformes de gestion électorale sont souvent fournies et maintenues par des entreprises étrangères. Le cas de la DAF sénégalaise l'a rappelé : quand un État et son prestataire unique sont en conflit, c'est la sécurité de toute la population qui se trouve fragilisée. Ces dépendances ne sont pas forcément exploitées. Mais elles créent des leviers de pression que des fournisseurs, ou les États qui les soutiennent, peuvent être tentés d'utiliser.

L'intelligence artificielle ajoute une couche nouvelle. Les grands modèles de langage sont entraînés pour l'essentiel sur des textes anglais produits dans les pays riches, et très peu sur les langues nationales de l'espace francophone africain. À mesure que les administrations, les médias et les écoles s'appuient sur ces outils pour produire ou résumer l'information, la question de savoir qui les conçoit, et dans quelles langues, cesse d'être technique. Elle devient une question de souveraineté.

6. Faire entrer la menace informationnelle dans l'alerte précoce

Ce que les systèmes d'alerte ne voient pas

L'Afrique n'a pas attendu le numérique pour se doter d'outils d'anticipation. Le Système continental d'alerte rapide de l'Union africaine, prévu par le protocole de 2002 qui institue le Conseil de paix et de sécurité, s'appuie sur une salle de veille à Addis-Abeba et sur les mécanismes des communautés économiques régionales, dont ECOWARN pour la CEDEAO et CEWARN pour l'IGAD. Ces dispositifs ont été pensés pour suivre ce qui se voit : mouvements armés, déplacements de population, flambées de prix, tensions autour d'un scrutin.

Ils captent mal la phase qui précède souvent le passage à l'acte. Dans l'Est de la RDC, on l'a vu, les rumeurs contre la MONUSCO ont circulé pendant des semaines avant les attaques contre ses bases. En Éthiopie, après l'assassinat du chanteur Hachalu Hundessa en juin 2020, les appels à la violence se sont propagés en ligne en quelques heures, avant que les autorités ne coupent Internet pendant plus de trois semaines. Dans les deux cas, le signal existait. Il était public, souvent daté, parfois localisable. Il n'entrait simplement dans aucune grille d'indicateurs.

Cinq signaux à suivre

Intégrer l'information dans l'alerte précoce ne veut pas dire surveiller tout ce qui se dit en ligne. Il faut au contraire choisir peu d'indicateurs, bien définis, que des analystes peuvent suivre dans la durée. Cinq familles de signaux nous paraissent prioritaires.

1. La montée rapide de discours de haine visant un groupe identifiable, mesurée en langues nationales et pas seulement en français. Ce qui compte n'est pas le volume mais l'accélération, surtout à l'approche d'une date sensible.
2. Les campagnes coordonnées, que trahissent des comptes créés en série, des messages identiques publiés en rafale ou des contenus repris mot pour mot d'un pays à l'autre.
3. Les rumeurs visant ceux qui protègent ou apaisent : Casques bleus, humanitaires, médiateurs, observateurs électoraux. Leur discrédit précède souvent leur mise à l'écart, le Tigré l'a montré.

4. Les coupures et ralentissements d'Internet. Une coupure accompagne souvent une répression ou une offensive, et elle aveugle au passage ceux qui observent.
5. Les contenus synthétiques visant des figures centrales (dirigeants, chefs religieux, commandants) en période de tension. Un faux audio diffusé la veille d'un scrutin ou au lendemain d'un coup de force ne pèse pas le même poids qu'en temps ordinaire.

Qui collecte, qui vérifie, qui décide

Le maillon faible n'est pas la technologie, c'est la chaîne humaine. Les outils de détection automatique fonctionnent mal en langues africaines, et l'essentiel des échanges sensibles passe par WhatsApp ou Telegram, où rien n'est visible de l'extérieur. L'accès des chercheurs aux données des plateformes s'est d'ailleurs réduit : Meta a fermé CrowdTangle en août 2024, et l'accès à l'interface de programmation de X est devenu payant en 2023.

La collecte doit donc s'appuyer sur ceux qui entendent déjà ces signaux. Les réseaux de vérification comme BenbereVérif au Mali, ou les radios communautaires du Nord-Kivu, reçoivent chaque jour des messages d'auditeurs qui leur transfèrent ce qui circule. Le Kenya a montré qu'on pouvait organiser ce flux. La plateforme Uwiano, portée par la Commission nationale pour la cohésion et l'intégration (NCIC) et le PNUD, combine signalements citoyens par SMS, moniteurs de terrain et comités de paix locaux ; la NCIC a même publié en 2022, avant les élections générales, un lexique des expressions codées employées pour inciter à la haine.
Vient ensuite la vérification. Un signal brut ne vaut rien sans quelqu'un qui comprend la langue, le contexte et l'histoire locale, et qui sait distinguer une insulte ordinaire d'un appel au meurtre. Les centres nationaux d'alerte, là où ils existent, sont le bon niveau pour ce travail, à condition d'y recruter des analystes qui parlent les langues concernées.
Reste la réponse. Une alerte informationnelle n'a d'intérêt que si elle déclenche quelque chose: un démenti diffusé par une radio de confiance, une démarche d'un médiateur auprès des leaders communautaires, une demande de retrait accéléré adressée aux plateformes, ou la saisine de la salle de veille continentale quand le risque dépasse les frontières.

Le risque de dérive

Une telle proposition a un revers évident. Un système capable de repérer des discours de haine est aussi capable de repérer des opposants. On l'a vu plus haut avec les logiciels espions : il serait naïf de croire qu'une veille informationnelle échapperait à cette tentation.
Trois garde-fous nous semblent indispensables. Le premier tient à l'objet : on suit l'incitation à la violence contre des groupes et la manipulation coordonnée, jamais la critique politique. Le deuxième tient à l'institution : la veille doit être confiée à des structures indépendantes des services de sécurité, avec une place réelle pour la société civile. Le troisième tient aux données : aucune collecte nominative au-delà de ce qu'exige la vérification, et une durée de conservation limitée.

Un chantier à la portée des organisations régionales

Rien de tout cela n'exige de créer une institution. Les briques existent déjà : la salle de veille de l'UA, les mécanismes régionaux, les centres nationaux, les réseaux de vérification. Ce qui manque, c'est une grille commune d'indicateurs informationnels, des analystes formés aux langues concernées et des protocoles qui disent qui fait quoi quand un signal est confirmé.
La géographie complique la tâche. Depuis le départ du Burkina Faso, du Mali et du Niger de la CEDEAO, une partie des signaux sahéliens échappe aux mécanismes ouest-africains. Il faudra passer par d'autres canaux : l'UA, les médias et les réseaux de vérification qui travaillent par-delà les frontières, la société civile. C'est là qu'un espace francophone, qui partage une langue de travail, peut réellement apporter quelque chose.

Conclusion

quatre chantiers prioritaires

Les cinq menaces décrites ici ont un point commun : elles exploitent le décalage entre la vitesse à laquelle l'Afrique francophone se connecte et la lenteur avec laquelle elle se dote de garde-fous. Ce décalage ne se comblera pas d'un coup. Mais certains chantiers peuvent avancer vite, parce qu'ils s'appuient sur des institutions qui existent déjà.

1. **Pour l'Union africaine et les communautés économiques régionales** : adopter une grille commune d'indicateurs informationnels et l'intégrer au Système continental d'alerte rapide comme aux mécanismes régionaux, avec des analystes formés aux langues nationales. La Position africaine commune sur l'application du droit international au cyberespace, adoptée en 2024, offre une base politique ; il reste à la traduire en protocoles opérationnels.
2. **Pour les États** :
   doter chaque pays d'une équipe nationale de réponse aux incidents informatiques réellement opérationnelle, capable de communiquer publiquement en cas de crise, et ratifier la Convention de Malabo, entrée en vigueur en juin 2023 mais encore peu ratifiée.
3. **Pour les plateformes** :
   recruter des modérateurs dans les langues africaines les plus parlées, publier des rapports de transparence par langue et par pays, et rétablir un accès raisonnable aux données pour les chercheurs et les vérificateurs.
4. **Pour les bailleurs** :
   conditionner tout appui en matière de cybersécurité aux trois garanties décrites plus haut, et financer dans la durée, et non projet par projet, les réseaux de vérification et les radios communautaires qui constituent aujourd'hui la première ligne de défense.

Les espaces de coopération linguistique, francophone mais aussi lusophone ou arabophone, peuvent appuyer ces chantiers, notamment en portant auprès des plateformes la question des langues africaines, que les États isolés ont peu de poids pour imposer.

Cette première ligne a un visage : celui d'une jeunesse connectée que l'on décrit trop souvent comme une cible, de la radicalisation, de la manipulation, du recrutement. Elle est aussi celle qui vérifie, dément et corrige, en bambara, en wolof ou en lingala, bien avant que les institutions ne s'en mêlent. Toute stratégie de résilience numérique qui ne la traiterait pas en partenaire passerait à côté de sa principale ressource.

Références

Africa Center for Strategic Studies, Mapping a Surge of Disinformation in Africa, 13 mars 2024.

- Africa Cybersecurity Magazine, Réponse à l'incident informatique à la DAF au Sénégal, février 2026.
- Africa Defense Forum, Cheap Drones Multiply Terrorist Threats in Sahel, 12 août 2025.
- Africa Defense Forum, Starlink Becomes Communication Tool of Choice for Sahel Terrorists, 12 août 2025.
- African Arguments (M. Suliman), The deepfake is a powerful weapon in the war in Sudan, 23 octobre 2024, qui rend compte de l'enquête de la BBC d'octobre 2023.
- Africanews, Mali withdraws from the International Organisation of La Francophonie, 19 mars 2025.
- AIP Fact-checking, démenti de la vidéo de Bouaké, relayé par Abidjan.net, janvier 2024.
- Atlantic Council, The Sahel is pivoting toward Turkey.
- BusinessDay, INEC server records 12m cyber-attacks during presidential poll, 2023.
- Chesney, R. et Citron, D., « Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security », *California Law Review*, vol. 107, 2019.
- Conseil de sécurité des Nations unies, Rapport final du Groupe d'experts sur la Libye, S/2021/229, 8 mars 2021.
- Forbidden Stories, Propaganda Machine: Secret documents reveal Russia's foreign influence strategy across three continents, 14 février 2026.
- France 24 Observers, Deepfake music videos praising Ibrahim Traoré, 30 mai 2025.
- INTERPOL/AFRIPOL, Africa Cyberthreat Assessment Report 2025, juin 2025.
- MERICS, African networks, smartphones and surveillance.
- NetBlocks, Internet cut in Ethiopia amid unrest following killing of singer, juin 2020.
- NPR, Meta shutters tool used to fight disinformation, despite outcry, 14 août 2024.
- OIF, *La langue française dans le monde*, Observatoire de la langue française, 2026 (synthèse).
- The Record, Senegal confirms breach of national ID card department after ransomware claims, 9 février 2026.
- The Star, List of hate speech words blacklisted by NCIC, 8 avril 2022.
- Time, The 5 Most Important Revelations From the Facebook Papers, octobre 2021.
- UIT, Global Cybersecurity Index 2024, septembre 2024.
- Union africaine, Conseil de paix et de sécurité, Position africaine commune sur l'application du droit international à l'utilisation des technologies de l'information et de la communication dans le cyberespace, communiqué de la 1196e réunion, 29 janvier 2024.
- Union africaine, Convention sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo), 2014, entrée en vigueur le 8 juin 2023.
- Washington Post, How a sick president's suspect video helped spark an attempted coup in Gabon, 13 février 2020.

MISSIONS :

Thinking Africa est un think tank panafricain non partisan, créé dans le but de produire des savoirs innovants au sujet du devenir africain. Ces savoirs sont diffusés à travers les partages d'expériences, le renforcement des capacités, les plaidoyers et l'appui aux institutions publiques, privées et aux sociétés civiles (www.thinkingafrica.org). L'Observatoire des enjeux géopolitiques, sécuritaires et sociopolitiques au Sahel de Thinking Africa constitue un cadre unique d'échange d'idées et d'expertises, un laboratoire de réflexion pluridisciplinaire sur les problématiques complexes qui déstabilisent le Sahel (www.thinkingafrica.org/V2/observatoire-du-sahel/)

OBJECTIFS :

L'Observatoire du Sahel a vocation à créer des synergies de compétences pour entreprendre dans une approche holistique, des recherches pluridisciplinaires à toutes les échelles (internationale, régionale et locale). Il vise également à produire des études originales apportant une analyse novatrice sur les problématiques névralgiques du Sahel, offrant un regard local et formulant des recommandations concrètes basées sur des données récentes de terrains fournies par des acteurs locaux

Une note produite dans le cadre d'un partenariat avec le soutien de l'Organisation internationale de la Francophonie (OIF) Depuis 2014, Thinking Africa collabore avec l'OIF. La présente collaboration porte sur la réalisation de notes d'analyse politique, par l'Observatoire du Sahel de Thinking Africa, à propos des enjeux géopolitiques, stratégiques et sécuritaires liés à la gouvernance, à la stabilité politique et au développement durable au Sahel.

« Avec le soutien de l'Organisation internationale de la Francophonie (OIF) ». « Les propos énoncés dans la présente publication ne sauraient en rien engager la responsabilité de l'OIF, pas plus qu'ils ne reflètent une prise de position officielle de l'Organisation »

Contacts Email: contact@thinkingafrica.org

Web: www.thinkingafrica.org