

STAR WARS AU SAHEL

COMMENT ELON MUSK RECOMPOSE DISCRÈTEMENT
LA FRONTIÈRE NUMÉRIQUE EN AFRIQUE

JENNY OUÉDRAOGO



**ROSA
LUXEMBURG
STIFTUNG**

WEST AFRICA OFFICE

STAR WARS AU SAHEL

COMMENT ELON MUSK RECOMPOSE DISCRÈTEMENT LA FRONTIÈRE
NUMÉRIQUE EN AFRIQUE

—— JENNY OUÉDRAOGO





IMPRINT

Published by the Rosa-Luxemburg-Stiftung West Africa Regional Office

Author : Jenny Ouédraogo

Cover Illustration & Editorial design : Yessine Ouerghemmi



ROSA LUXEMBURG STIFTUNG

WEST AFRICA OFFICE

Une nouvelle frontière numérique a émergé au Sahel, cette ceinture de 6 000 kilomètres qui s'étend à travers l'Afrique, de l'océan Atlantique à la mer Rouge. Des antennes blanches de Starlink parsèment désormais les villes, les localités et même les villages les plus reculés, promettant une connexion là où les infrastructures numériques sont quasi inexistantes.

Starlink, le fournisseur d'accès Internet par satellite détenu par SpaceX, l'entreprise d'Elon Musk, s'est rapidement implanté pour répondre à la demande locale d'une connexion fiable dans les zones mal desservies par l'État. Ce déploiement a mis en lumière les failles structurelles de la région : les opérateurs nationaux s'appuient sur des réseaux vieillissants, tandis que Starlink offre un haut débit mondial à grande vitesse. Commerçants et entrepreneurs déplacent les terminaux d'un pays à l'autre à travers des circuits informels, des transports personnels ou de la petite contrebande. En étendant ainsi la connectivité jusqu'aux zones rurales, ces réseaux informels ont créé une infrastructure de facto qui façonne la vie quotidienne et alimente les tensions autour de la sécurité et de l'accès non étatique. Très vite, écoles, cliniques, entreprises — et même groupes armés — se sont connectés à un système privé échappant presque totalement à la supervision de l'État.

Au Niger, par exemple, le signal est apparu avant la réglementation. Les terminaux fonctionnaient déjà dans des administrations provinciales et des écoles plusieurs mois avant l'autorisation officielle du gouvernement en 2024. Le Mali, après avoir d'abord ouvert l'accès à Starlink, l'a suspendu brusquement dans un flou réglementaire, tandis que le service devrait être [autorisé](#) au Burkina Faso d'ici la fin de l'année. Dans la plupart des cas, les autorités n'ont jamais formellement interdit l'usage de Starlink, et l'absence de cadre clair a créé une zone grise où ONG, journalistes et commerçants pouvaient opérer librement. Le Tchad et le Nigeria, [à l'inverse](#), ont choisi d'assumer ouvertement la technologie, en octroyant des licences et en la présentant comme un outil de connectivité nationale.

Il en résulte une mosaïque juridique à l'échelle régionale - une zone d'autonomie numérique où les frontières entre communication, conflit et contrôle se brouillent quelque part entre l'orbite terrestre et les caprices d'un milliardaire.

REDÉFINIR LE CHAMP DE BATAILLE NUMÉRIQUE

Le Jama'at Nusrat al-Islam wal-Muslimin (JNIM) est l'organisation jihadiste la plus [durable](#) du Sahel, principalement active au Mali, au Burkina Faso et au Niger. Formé en 2017 en tant qu'affilié d'Al-Qaïda, le groupe exploite depuis longtemps les frontières poreuses, la faiblesse de la gouvernance et les frustrations locales pour étendre son influence et s'enraciner dans des territoires où l'État-nation s'est presque effondré.

Au cours de l'année écoulée, il est entré dans une phase d'expansion rapide, marquée par des offensives simultanées dans le centre du Mali, la zone des trois frontières du Tchad, du Cameroun et de la République centrafricaine, ainsi que dans le nord du Bénin et du Togo.

Cette expansion s'explique par la convergence de plusieurs facteurs. Le retrait progressif des forces internationales, notamment l'opération Barkhane menée par la France et la mission onusienne MINUSMA, a favorisé l'émergence de vastes zones de faible autorité étatique que les combattants ont cher-

ché à [exploiter](#). Le passage progressif du JNIM d'une stratégie de guérilla à une forme de gouvernance locale - collecte d'impôts, contrôle des routes commerciales et arbitrage des différends - a renforcé sa légitimité dans certaines régions. Comme l'a observé l'International Crisis Group au début de l'année 2025, la capacité du JNIM à adapter sa structure et à s'ancrer dans les [communautés](#) locales lui a permis de survivre aux campagnes antiterroristes qui ont anéanti ses rivaux.

La technologie a amplifié la résilience du groupe. [Selon](#) des analystes régionaux, le JNIM utilise désormais des drones commerciaux pour la surveillance et a expérimenté des explosifs aériens improvisés. Mais le changement le plus subtil réside dans la communication. Le commandement du JNIM, autrefois dépendant de messagers, de radios et de réseaux mobiles instables, était souvent fragmenté. Starlink a largement supprimé cette contrainte, offrant une connectivité rapide, abordable et non surveillée à un niveau jusqu'alors inatteignable.

Souvent achetés à l'étranger puis revendus sur les marchés locaux, les terminaux sont acheminés à travers des réseaux informels reliant la Libye, le Nigeria et le Sahel. Un [rapport](#) de mai 2025 de la Global Initiative Against Transnational Organized Crime documente plusieurs saisies de terminaux Starlink dans les régions de Tillabéri et de Tahoua, bastions du JNIM au Niger. En juin 2024, [Le Monde](#) a identifié un terminal Starlink dans une vidéo de propagande du groupe tournée près de Gao, tandis que les services de sécurité nigériens ont depuis confisqué

plusieurs appareils lors d'opérations antiterroristes.

Le système d'enregistrement de Starlink, dépourvu de toute vérification d'identité spécifique à la région, permet aux appareils de fonctionner loin de l'adresse déclarée par l'abonné, créant ainsi une [zone grise](#) numérique échappant à la visibilité de l'État. Les analystes [avertissent](#) que cette connectivité satellitaire améliore considérablement les capacités logistiques et de commandement des acteurs non étatiques - une inquiétude partagée par les services de renseignement sahéliens, qui estiment que le réseau crypté et à faible latence de Starlink affaiblit la capacité de l'État à surveiller la coordination de ces groupes.

LE DILEMME DE LA RÉGULATION

L'exploitation de Starlink par le JNIM met en lumière un problème structurel plus profond dans la région : les gouvernements du Sahel disposent de très peu de moyens pour superviser ou réguler les réseaux dont dépendent aussi bien les civils que les groupes armés.

L'architecture de Starlink place l'autorité opérationnelle loin de toute portée locale. Les terminaux doivent être enregistrés aux États-Unis, d'où ils sont également opérés à distance : c'est là que sont effectuées les mises à jour des micrologiciels et que le réseau est contrôlé dans son ensemble. Si les licences locales confèrent une autorisation légale d'utilisation, elles n'impliquent aucun véritable pouvoir de supervision. Des utilisateurs affirment que les terminaux restent [actifs](#) dans de nombreux pays où Starlink n'a pourtant reçu aucune approbation réglementaire formelle. De plus, bien que SpaceX conserve

la capacité technique de désactiver le service, cela se produit rarement et demeure difficile à tracer, laissant l'accès - et ses implications stratégiques - largement sous le contrôle du fournisseur plutôt que des autorités locales.

Les États ne peuvent ni surveiller qui utilise le service, ni quand, ni à quelles fins. Ils sont donc incapables d'en prévenir les détournements, permettant à des acteurs non étatiques comme le JNIM d'exploiter cette connectivité cryptée pour coordonner leurs opérations, déplacer des ressources et maintenir des communications transfrontalières. Obtenir un droit de regard nécessiterait une coopération technique avec SpaceX qui, même si elle était accordée, exigerait des infrastructures sophistiquées et un personnel hautement qualifié pour analyser les flux. Les règles américaines sur les [technologies](#) à double usage limitent par ailleurs ce

que les gouvernements peuvent légalement faire avec les terminaux Starlink, ajoutant un obstacle supplémentaire.

Mais même si cet accès était acquis, un second dilemme apparaîtrait aussitôt. Dans les États dominés par des régimes militaires, le contrôle de Starlink pourrait servir à espionner des journalistes, des militants ou des opposants politiques. Les mêmes outils capables de révéler les activités d'un groupe armé pourraient tout aussi bien devenir des instruments de répression et de consolidation du pouvoir autoritaire.

Il en résulte une impasse réglementaire. La connectivité, si essentielle à la gouvernance, à l'éducation et au commerce, devient à la fois un vecteur de coordination pour les groupes armés et un potentiel levier de contrôle autoritaire. Tant qu'un cadre de gouvernance équilibrant supervision technique et garanties civiles n'aura pas été mis en place - ce qui exigerait une coopération sans précédent entre SpaceX, les autorités américaines et les États sahéliens -, Starlink restera une zone d'ambiguïté opérationnelle.

LE GARDIEN MILLIARDAIRE

Au Sahel comme ailleurs, Starlink opère sous l'autorité d'une seule entreprise privée. Si les gouvernements africains peuvent en autoriser l'usage, la gestion du réseau demeure centralisée à l'étranger, avec des décisions clés concentrées entre les mains d'Elon Musk. Cette structure confère à un acteur économique - et, par extension, à un seul individu - une influence considérable sur une part croissante des infrastructures de communication de la région.

Le parcours de Musk illustre les dangers d'une telle concentration de pouvoir. En 2022, alors que les forces ukrainiennes reprenaient du territoire à la Russie, Musk aurait ordonné la coupure du service Starlink dans des zones contestées, notamment à Kherson. Au moins une centaine de terminaux auraient été affectés, perturbant les communications des drones, de l'artillerie et des troupes - démontrant ainsi qu'une entreprise privée peut exercer une influence sans précédent sur des opérations militaires. Reuters a décrit la situation comme « un scénario où le sort d'une guerre se retrouve entre les mains d'Elon Musk ». Des schémas similaires se retrouvent dans sa gestion du réseau social anciennement connu sous le nom de Twitter, où des revirements soudains de politique affectent des millions d'utilisateurs sans véritable responsabilité.

L'activisme politique de Musk accentue encore ces risques : soutien affiché à la réélection de Donald Trump en 2024, interventions répétées dans le débat médiatique et politique, et prises de position marquées par un mélange d'impulsions libertariennes, d'alliances sélectives et de volte-face spectaculaires. Autant de traits qui font de lui tout sauf l'autorité idéale pour superviser une infrastructure critique. Dans le Sahel, cette dépendance est particulièrement préoccupante : le précédent ukrainien démontre qu'une décision unilatérale d'un opérateur privé peut avoir des conséquences stratégiques majeures.

L'expansion de Starlink au Sahel n'est pas simplement un progrès technologique, comme ses promoteurs aiment à le présenter. C'est bien davantage : un transfert de contrôle, des institutions publiques vers des intérêts privés. Elon Musk parle d'innovation ; la réalité, c'est que des pans entiers des infrastructures de communication essentielles dépendent désormais des caprices d'un seul individu. Ce qui avait commencé comme un exploit d'ingénierie est devenu un instrument de pouvoir, plaçant le ciel numérique hors de portée des gouvernements et des populations qu'il est censé servir. Alors que la technologie continue de devancer la gouvernance, ce sont les plus vulnérables qui paient le prix de ce nouvel ordre numérique.