Franck Kié
Contributions – Forum de Dakar

L'espace numérique comme champ d'affrontement et espace de cyber-manipulation de puissances étrangères présentes en Afrique :

> *« Si la désinformation prive de tout pouvoir, l'information donne du pouvoir. Ce sont les droits à la liberté d'expression et à l'accès à l'information qui garantissent aux citoyens la possibilité de trouver des informations pertinentes pour prendre des décisions ayant un impact sur leur vie. »*
> **Guy Berger, directeur de la stratégie et de la politique de l'UNESCO dans le domaine de la communication et de l'information.**

En décembre 2020, Facebook a annoncé la suspension de trois réseaux de manipulation totalisant près de 500 comptes et pages, liés à *« l'armée française* » et à la Russie (deux d'entre eux). Pour la première fois, Facebook devenait le théâtre d'opérations d'influence étrangères en confrontation, via des faux comptes se dénonçant mutuellement comme tel."[1] Ces opérations de désinformation visaient principalement la République centrafricaine (RCA), mais aussi l'Algérie, le Cameroun, la Libye et le Soudan – rappelant les intérêts géopolitiques, économiques et militaires des deux pays dans la région.

La désinformation fait référence à la diffusion d'informations fausses et incendiaires, véridiques ou non, par un acteur dans l'intention d'induire en erreur et de causer du tort. Souvent, l'objectif est de créer un paysage informationnel encombré et chaotique – en brouillant les frontières entre ce qui est réel et ce qui ne l'est pas – afin de transformer l'opinion publique, d'influencer les processus démocratiques, d'accroître la discorde, de promouvoir le chaos et la peur, de susciter la méfiance envers les gouvernements et d'entraîner des réactions émotionnelles dans la sphère publique.

Les sociétés démocratiques comptent sur le soutien du public pour faire avancer les initiatives politiques. Un débat informé, rationnel et civique est essentiel pour former une opinion publique favorable, élément vital de la démocratie. Dans un paysage informationnel chaotique, tel que celui produit par la désinformation ciblée, la discussion rationnelle est rendue plus difficile. Ce qui entraîne une diminution de la capacité à construire un consensus public et limite ainsi la capacité des gouvernements démocratiques à mettre en œuvre des changements significatifs (Guge, 2020). Par conséquent, ces campagnes de désinformation en Afrique constituent un défi important pour le libre exercice de la démocratie. Capitalisant sur les caractéristiques inhérentes aux plateformes de messagerie Internet et sur la nature libre des sociétés démocratiques pour diffuser des contenus faux et malveillants, les acteurs mènent une « *guerre de l'information* » [2]contre les citoyens africains. Dès lors, comme le

---

[1] Comme le rappelle Wasserman (2020), les "*fake news*" peuvent être définies comme des contenus "*entièrement faux ou contenant des éléments délibérément trompeurs incorporés dans leur contenu ou leur contexte*" (Bakir et McStay, 2017) ou "*intentionnellement et vérifiablement faux [qui] pourraient induire les lecteurs en erreur"* (Allcott et Gentzkow, 2017).

[2] Selon Robert R. Mackey ("Information Warfare", dans *Oxford bibliographies*) : la guerre de l'information est un terme militaire généralement occidental, datant de la fin du 20e siècle, qui englobe un large éventail de formes non cinétiques de conflits humains. Le cheval de Troie de l'Iliade d'Homère est l'un des exemples les plus connus de guerre de l'information classique dans la littérature, mais l'histoire militaire est remplie d'exemples non fictifs. https://www.oxfordbibliographies.com/view/document/obo-9780199791279/obo-9780199791279-0024.xml#:~:text=La guerre de

rappelle Maylin Fidler du Council on Foreign Relations, ces campagnes de désinformation soulignent les « *défis auxquels les États africains sont confrontés dans l'élaboration d'une politique de l'internet qui réponde à la fois aux menaces extérieures et aux dynamiques politiques internes* ».

Cet article commencera par (a) un examen de la nature de la guerre de l'information dans un contexte africain en tant que laboratoire de micro-ciblage politique, amplifié (b) par une étude de cas sur les opérations russes sur le continent. La conclusion fournira plusieurs recommandations pour lutter à la fois contre les campagnes de désinformation menées par des étrangers et contre la diffusion de *fake news*.

a. La numérisation et l'émergence des « fake news » dans un contexte africain qui constitue un « terreau » fertile pour les ingérences étrangères

Comme le montre une étude de l'Africa Center for Strategic Studies[3], l'émergence des technologies de réseau – en particulier en Afrique – a insufflé l'espoir d'un renforcement de la démocratie grâce à la baisse des coûts d'organisation et d'accès à l'information, avec de meilleurs outils de contrôle de l'action générale (Tufekci, 2014). Pour rappel, la pénétration du mobile est passée de 3 % en 2000 à près de 80 % en 2018 (Banque mondiale, 2020), avec plus de 860 millions d'utilisateurs (Langan, 2020). La pénétration d'Internet est passée de 1 % à 51 % (World Bank Data, 2001 ; Internet Live Stats, 2021).

Mais cet abaissement des barrières à la consommation, à la production et à la diffusion des médias a décuplé la production et la circulation en masse d'outils de désinformation, de mal-information, et de la cyber-propagande (l'utilisation des médias numériques pour diffuser la propagande). L'émergence de « *créateurs de médias* » (Jenkins, 2006), de « *producteurs* » (qui brouillent les frontières entre production et consommation), de « *chambres d'écho* » et de « *bulles de filtrage* » (sur des plateformes privées de médias sociaux aux algorithmes opaques comme Facebook, Messenger, Twitter et WhatsApp) a contribué à la reconfiguration de la sphère publique africaine. Comme partout ailleurs, le passage à une ère « d'*auto-communication de masse* » (Castells, 2009) a marqué la naissance de « *tonnes d'informations non vérifiées et trompeuses qui se disputent l'attention du public sur les plateformes médiatiques traditionnelles et numériques* » (Mare, Mabweazara, Moyo, 2019).

Combiné à la force d'autres outils numériques tels que les *bots* et le *big data*, il a permis à des acteurs opportunistes de favoriser une « *ingénierie du consentement ou de la déstabilisation* » (Bernays, 1947) plus efficace – et moins transparente, dans la sphère publique. Ces « *politiques computationnelles* »[4] ont permis au ciblage d'aller au-delà de l'analyse et du profilage agrégés basés sur des groupes, et de modéliser des individus spécifiques. Elle a transformé la communication en une transaction privée de plus en plus personnalisée et, à ce titre, a remodelé la sphère publique en la rendant de moins en moins

---

l'information%20est%20une%20généralement,cinétique%20des%20formes%20de%20conflit%20humain.&text=La%20invention%20de%20la%20radio%20a%20additionné,les efforts%20dans%20ce%20nouveau%20domaine.

[3] *Africa's Evolving Infosystems: A Pathway to Security and Stability, 2011.*

[4] Selon la chercheuse Zeynep Tufekci, la politique informatique désigne l'application de méthodes informatiques à de grands ensembles de données provenant de sources de données en ligne et hors ligne pour mener des actions de sensibilisation, de persuasion et de mobilisation dans le but d'élire, de promouvoir ou de s'opposer à un candidat, une politique ou une législation.

publique[5] – rappelant ainsi que « *la propension d'Internet à l'autonomisation des citoyens n'est ni unidirectionnelle ni directe »* (Tufekci, 2014).

En Afrique du Sud, par exemple, les bots sont utilisés par un clan politique – les Guptas – pour détourner l'attention des allégations de dévoiement de l'État. Au Zimbabwe ou en Guinée, les partis au pouvoir et d'opposition déploient souvent des cyber-groupes pour défendre des causes spécifiques. Au Kenya, l'élection de 2017 a donné lieu à une cyber-propagande menée par des cyber troupes, des militants citoyens et des influenceurs numériques sur les plateformes de médias sociaux.

Enfin, il faut noter que les réseaux numériques permettent de tester ces méthodes en temps réel et de les déployer immédiatement, ce qui ajoute un niveau de dynamisme et de rapidité jusqu'alors irréalisable dans le façonnage de la sphère publique. La Russie a choisi l'Afrique comme « laboratoire » avant d'étendre ces tactiques à des théâtres plus larges, l'un des acteurs les plus sophistiqués dans ce domaine.

b. *L'Afrique comme laboratoire pour les expérimentations de micro-ciblage politique[6] et d'ingénierie sociale : une étude de cas des tactiques d'influence russes sur le continent*

Selon Mailyn Fidler, chargée de recherche au Harvard Berkman Klein Center for Internet and Society, les opérations menées par la Russie pour façonner la sphère publique numérique africaine (ce qu'elle appelle le « *colonialisme de la désinformation* ») étaient expérimentales et conçues pour être itérées. Les pays et les politiques africains ont été utilisés comme des « *laboratoire* » pour développer des stratégies et des tactiques efficaces ailleurs.

La société militaire privée Wagner Group, fondée en 2014 par l'oligarque russe Yevgueni Prigozhin, est connue pour être le principal acteur russe dans ce domaine. Actif en Libye[7], au Mozambique[8], en Afrique du Sud et en République centrafricaine (RCA)[9], Wagner propose aux politiciens et aux groupes armés de leur bâtir une influence sur le continent en s'appuyant sur un réseau de forces de maintien de la paix, de futurs dirigeants et d'agents d'infiltration, ainsi que sur des cyber-propagandistes et des experts numériques. Par exemple, toutes les pages supprimées par Facebook en octobre 2019 et décembre 2020 étaient liées à Wagner d'après l'enquête de Facebook et d'une organisation d'enquête russe fondée par l'oligarque Mikhaïl Khodorkovski.

Un fait intéressant concernant l'aspect expérimental de ces opérations est leur séquençage. Shelby Grossman, chercheur de l'Observatoire de l'Internet de Stanford, rappelle « qu'*elles ont commencé en 2018, juste après que Facebook et Twitter aient fini de supprimer la majeure partie des comptes de l'Internet Research Agency aux États-Unis* » (Africa Center for Strategic Studies, 2020). Il apparaît donc que les agents de Wagner testaient de nouvelles

[5]Ces approches peuvent être utilisées pour établir des profils et interagir individuellement avec les électeurs en dehors de la sphère publique.
[6] Borgesius et al., Microciblage politique en ligne : Promesses et menaces pour la démocratie, Revue de droit d'Utrecht, Vol. 14, 2018.
[7] Présent sous le couvert du "Fonds pour la défense des valeurs nationales en Libye".
[8] Présents, sous couvert du "Centre international d'anticrise (CIA)" et de "l'Association pour la libre recherche et la coopération internationale (AFRIC)".
[9] Entre 530 et 2 000 forces militaires privées ont été déployées pour soutenir le gouvernement. L'un des membres les plus proches et les plus influents du cabinet du président, son conseiller en matière de sécurité intérieure, est le Russe Valery Zakharov.

stratégies et développaient de nouvelles tactiques qui leur permettraient de rester sous couverture tout en poursuivant leurs intérêts africains[10] : travailler avec des mandataires locaux, utiliser un éventail plus complet de langues (y compris l'arabe), diffuser des informations exactes ou des opinions non falsifiables... (Fidler, 2020).

L'une de ces stratégies, « la *franchise* » (Weiss et Vaux, 2020), s'appuie sur les entreprises médiatiques nationales et les principaux leaders d'opinion comme relais de divers messages : de la promotion des politiques russes au soutien de partis ou de dirigeants particuliers dans la région, en accord avec les intérêts commerciaux, en passant par la critique des politiques françaises et américaines. Alors que la stratégie de l'Internet Research Agency visant les États-Unis en 2016 provenait entièrement de Saint-Pétersbourg, avec des tweets rédigés dans un mauvais anglais, les opérations africaines sont « *externalisées »* à des acteurs locaux. En Libye, Wagner a parrainé Jamahiriya TV, les « *vestiges de l'appareil de télévision d'État de Mouammar Kadhafi* », qui a été « *somptueusement rénovée, le personnel recyclé et a vu ses dettes remboursées* » pour diffuser des nouvelles favorables au fils de Kadhafi, Saîf al-Islam. Autre exemple, Afrique Media TV, qui se présente comme un média panafricaniste anti-impérialiste et qui s'est associé à la filiale AFRIC du groupe Wagner depuis 2018. Leurs émissions défendent régulièrement les intérêts russes en Afrique subsaharienne et organisent des panels composés de leaders africains et de la diaspora cooptés par les Russes, comme l'intellectuelle et polémiste Kemi Seba ou l'activiste Nathalie Yamb. Ironiquement, l'AFRIC s'associe également à des militants d'extrême droite et à des agents néo-nazis pour relayer des discours d'anticolonialisme et de panafricanisme qui trouvent un écho auprès de la population locale et de la diaspora. C'est le cas de Luc Michel, auteur belge et fondateur de l'Observatoire européen de la démocratie et des élections – qui a mené des missions d'observation pro-Kremlin en Crimée et publié une dizaine d'articles pro-russes par semaine sur ses différents sites web : *La Voix de la Guinée Équatoriale*, *PanAfricom-TV*, *WebTV-Tchad*, *Centrafrica News*.

Cette stratégie de franchise permet la création de contenus locaux authentiques et de meilleure qualité qui trouvent un écho auprès des utilisateurs tout en rendant plus difficile la détection de ces campagnes de désinformation.[11] Elle montre également l'ampleur de la guerre de l'information menée par certaines puissances étrangères.

Pour que les gouvernements puissent contrer ces opérations, ils pourraient (i) établir des directives et des procédures pour une stratégie de réponse claire et cohérente (Guge, 2020) ; (ii) augmenter le partage d'informations afin d'identifier rapidement les acteurs de la menace et le contenu qu'ils produisent pour communiquer ces informations aux acteurs de première ligne ; (iii) accroître la responsabilité des plateformes en ligne en mettant à disposition des experts en sécurité nationale pour détecter et retirer les contenus produits par les acteurs de la menace ; (iv) et, globalement, renforcer la résilience du public en sensibilisant les citoyens à l'esprit critique pour limiter l'impact des faux récits, via notamment des initiatives de « fact-checking » telles qu'Africa Check ou encore l'Africa Infodemic Response Alliance (AIRA). Ces initiatives contribueront à renforcer et à maintenir la qualité de l'information relayée – et celle de la démocratie, par conséquent.

---

[10] Selon le Dr Grossman, "*la Russie a des intérêts spécifiques en Afrique. Prigozhin a des intérêts miniers et a des liens étroits avec Poutine, ce n'est donc pas un énorme saut de l'imagination de penser que Poutine est également intéressé par ces investissements miniers*."

[11] Par exemple, il désactive la fonction de transparence des pages de Facebook sur l'organisation qui se cache derrière une page, car cette organisation peut être une organisation locale, cooptée par des acteurs russes.