Revue Internationale de la Recherche Scientifique et de l'Innovation (Revue-IRSI)
ISSN: 2960-2823
Vol. 4, No. 1, Février 2026

LE RÔLE DES TECHNOLOGIES NUMÉRIQUES DANS LA DYNAMIQUE DU CONFLIT ARMÉ À L'EST DE LA RDC : ENTRE PROPAGANDE, SURVEILLANCE ET CYBERTERRORISME

NGOLA MBULI Iaac

Assistant/Doctorant Université de Kinshasa, Unikin, Département des Relations Internationales, RD. Congo

Résumé: Les technologies numériques jouent un rôle important dans la dynamique du conflit armé à l'Est de la République démocratique du Congo. Les groupes armés et les forces gouvernementales utilisent les réseaux sociaux et les plateformes numériques pour diffuser de la propagande, recruter des combattants et influencer l'opinion publique. La surveillance numérique est également utilisée pour contrôler et réprimer les populations civiles. De plus, les attaques cyber-terroristes menacent la sécurité des infrastructures critiques et des institutions publiques.

Le conflit armé en République Démocratique du Congo (RDC) est un phénomène complexe et multi facette qui a duré des décennies, impliquant de nombreux acteurs étatiques et non étatiques. Ces dernières années, l'avènement des technologies numériques a transformé la manière dont les conflits armés sont menés et perçus. Les groupes armés, les gouvernements et les organisations internationales utilisent de plus en plus les technologies numériques pour influencer l'opinion publique, recruter des combattants, collecter des fonds et mener des opérations de surveillance et de cyber-terrorisme.

Notre article de recherche examine le rôle des technologies numériques dans la dynamique du conflit armé en RDC, en mettant l'accent sur les stratégies de propagande, de surveillance et de cyber-terrorisme employées par les différents acteurs. Ce résumé met en évidence les défis posés par les technologies numériques dans le conflit armé à l'Est de la RDC et souligne la nécessité d'une approche globale pour lutter contre ces menaces.

Mots-clés : Technologie Numérique 1; Conflit Armé 2; Propagande 3; Surveillance 4; Cyber Terrorisme 5 ;

Digital Object Identifier (DOI): https://doi.org/10.5281/zenodo.**18630666**

1 Introduction

Dans un monde de plus en plus connecté, les technologies numériques ont révolutionné la façon dont les conflits sont menés et perçus. L'Est de la République démocratique du Congo, théâtre de conflits armés récurrents, n'échappe pas à cette réalité. Les groupes armés et les forces gouvernementales utilisent les technologies numériques pour promouvoir leurs intérêts, influencer l'opinion publique et mener des opérations de guerre. Mais quel est exactement le rôle des technologies numériques dans la dynamique du conflit armé à l'Est de la RDC ? Comment les technologies numériques sont-elles utilisées pour propager la haine, surveiller les populations civiles et mener des attaques cybernétiques ? Et quels sont les impacts de ces actions sur la sécurité et les droits de l'homme dans la région ? Cet article explore ces questions et examine les implications des technologies numériques dans le conflit armé à l'Est de la RDC, entre propagande, surveillance et cyberterrorisme.

2. Contexte : conflit armé à l'Est de la RDC

La République démocratique du Congo (RDC) est confrontée à un conflit armé récurrent dans sa partie orientale, notamment dans les provinces du Nord-Kivu, du Sud-Kivu et de l'Ituri. Ce conflit a débuté dans les années 1990 et a connu plusieurs phases de violence intense.

Les causes du conflit sont complexes et multi facettes. Elles incluent des facteurs tels que :

- Les tensions ethniques et tribales, qui ont été exacerbées par la colonisation et la manipulation politique (Mamdani, 2001).
- Les ressources naturelles abondantes (mines d'or, de coltan, de diamants, etc.), qui ont créé des convoitises et des rivalités entre les groupes armés et les entreprises minières (Global Witness, 2017).
- Les rivalités régionales et internationales, qui ont contribué à la prolongation du conflit et à la complexification de la situation sécuritaire (Prunier, 2009).
- La présence de groupes armés et de milices, qui ont profité de la faiblesse de l'État et de la corruption pour se financer et se renforcer (Human Rights Watch, 2018).
- Les conséquences humanitaires du conflit sont graves, avec des milliers de personnes déplacées, des pertes en vies humaines et des violations des droits de l'homme. Selon l'Office des Nations Unies pour la coordination des affaires humanitaires (OCHA, 2022), le conflit a provoqué plus de 13 millions de personnes déplacées internes et plus de 500 000 réfugiés dans les pays voisins
- Les groupes armés impliqués dans le conflit incluent les Forces démocratiques de libération du Rwanda (FDLR), les groupes Mai-Mai et les milices CODECO. L'armée congolaise et les forces de la Mission des Nations Unies au Congo (MONUSCO) sont également présentes dans la région pour tenter de rétablir la sécurité et la stabilité. Cependant, selon un rapport de l'International Crisis Group (2020), la présence de ces forces n'a pas suffi à mettre fin au conflit, en raison de la complexité de la situation et de la faiblesse de l'État congolais.

Le conflit à l'Est de la RDC a des implications régionales et internationales, notamment en termes de sécurité, de stabilité et de droits de l'homme. Il est considéré comme l'une des crises humanitaires les

plus graves au monde. Il est considéré comme l'une des crises humanitaires les plus graves au monde (Global Humanitarian Forum, 2022).

2.1. LES TECHNOLOGIES NUMÉRIQUES DANS LE CONFLIT

Les technologies numériques ont révolutionné la façon dont les conflits sont menés et perçus. Dans l'Est de la RDC, elles jouent un rôle complexe, entre propagande, surveillance et cyberterrorisme, nécessitant une attention particulière pour comprendre leur impact sur la dynamique du conflit et la sécurité des populations civiles.

A. Propagande numérique : influence de l'opinion publique

La propagande numérique est une stratégie de communication qui vise à influencer l'opinion publique en diffusant des informations biaisées ou trompeuses à travers les plateformes numériques. Dans le contexte des conflits, la propagande numérique peut être utilisée pour :

- Influencer l'opinion publique nationale et internationale
- Déstabiliser les adversaires
- Promouvoir une idéologie ou une cause
- Créer une perception biaisée de la réalité

Les plateformes numériques telles que les réseaux sociaux, les blogs et les sites web peuvent être utilisées pour diffuser des messages de propagande, souvent de manière anonyme ou déguisée. Cela peut rendre difficile l'identification de la source réelle de l'information et la vérification de sa véracité.

La propagande numérique peut avoir des conséquences graves, notamment :

- La manipulation de l'opinion publique
- L'exacerbation des tensions et des conflits
- La diffusion de fausses informations et de haine

Il est donc important de développer des stratégies pour contrer la propagande numérique et promouvoir une information vérifiée et objective.

B. Surveillance numérique : contrôle et répression

La surveillance numérique est une pratique qui consiste à collecter et à analyser des données personnelles à l'aide de technologies numériques. Dans le contexte des conflits, la surveillance numérique peut être utilisée pour contrôler et réprimer les populations civiles, notamment les opposants politiques, les activistes et les journalistes.(https://blogs.icrc.org/law-and-policy/fr/2023/10/02/menaces-numeriques-dans-les-conflits armes/).

Cette pratique peut avoir des conséquences graves sur les droits de l'homme et la liberté d'expression, notamment (www.mediadefence.org/ereader/publications/modules-de-synthese-sur-les-litiges-relatifs-aux-droits-numeriques-et-a-la-liberte-dexpression-en-ligne/vie-privee-et-protection-des-donnees/la-surveillance-numerique-dirigee-par-le-gouvernement/?lang=fr#footnote-index--1) :

- La répression des opposants politiques : La surveillance numérique peut permettre aux gouvernements de traquer et de réprimer les opposants politiques, les activistes et les journalistes.
- La violation de la vie privée : La collecte et l'analyse de données personnelles peuvent porter atteinte à la vie privée des individus et des groupes.
- La manipulation de l'information : La surveillance numérique peut également être utilisée pour manipuler l'information et influencer l'opinion publique.

Il est essentiel de prendre des mesures pour protéger les droits de l'homme et la liberté d'expression dans le contexte de la surveillance numérique.

❖ Les outils de surveillance numérique peuvent inclure :

- La collecte de données personnelles à partir des réseaux sociaux et des plateformes en ligne
- L'utilisation de logiciels espions pour surveiller les communications électroniques
- La mise en place de systèmes de surveillance biométrique pour identifier et traquer les individus

La surveillance numérique peut avoir des conséquences graves pour les individus et les communautés, notamment :

Il est donc important de prendre des mesures pour protéger les données personnelles et la vie privée, notamment en utilisant des outils de cryptage et des réseaux privés virtuels (VPN). Les gouvernements et les organisations doivent également être tenus responsables de leurs actions en matière de surveillance numérique et de protection des droits de l'homme.

2.2. Cyber-terrorisme : attaques contre les infrastructures critiques

Le cyber-terrorisme est une menace grandissante qui cible les infrastructures critiques de nos sociétés modernes, notamment les systèmes d'information des institutions publiques et des entreprises privées. Selon un rapport récent, les cyber-attaques ciblent de plus en plus ces infrastructures, souvent en raison de leur niveau de protection jugé insuffisant(www.oiq.qc.ca/publication/infrastructures-critiques-sarmer-contre-les-cyberattaques/). Les groupes terroristes utilisent les technologies de l'information pour développer leurs réseaux et communiquer, et il est crucial de développer de nouvelles méthodes pour suivre et analyser leur utilisation des techniques d'information (https:cyberjustice.blog/2023/05/25/la-menace-grandissante-du-cyberterrorisme/).

❖ **Les cibles privilégiées des cyberterroristes incluent :**

- **Les infrastructures énergétiques** : centrales électriques, réseaux de transport d'énergie
- **Les infrastructures de communication:** réseaux de télécommunication, internet
- **Les infrastructures de transport** : aéroports, ports, réseaux routiers et ferroviaires
- **Les institutions financières** : banques, marchés boursiers

Pour se protéger contre ces menaces, il est essentiel de mettre en place des mesures de sécurité robustes, telles que la formation du personnel, l'utilisation de technologies de sécurité avancées et la collaboration entre les secteurs public et privé. La sensibilisation et la formation sont cruciales pour prévenir les attaques et minimiser les risques (www.vpnunlimited.com/help/cybersecurity/cyberterrorism).

- **Les attaques contre ces systèmes vitaux peuvent avoir des conséquences catastrophiques, notamment:**

- La paralysie des réseaux de transport et de communication
- La disruption des services essentiels tels que l'eau, l'électricité et les soins de santé
- La compromission des données sensibles et confidentielles
- La perte de confiance dans les institutions et les systèmes

Les cyberterroristes utilisent des méthodes sophistiquées pour infiltrer les systèmes et causer des dommages importants. Il est donc crucial de mettre en place des mesures de sécurité robustes et de former les professionnels de la sécurité informatique pour protéger les infrastructures critiques contre ces attaques.

La protection des infrastructures critiques est une responsabilité partagée entre les gouvernements, les entreprises et les individus. Il est essentiel de travailler ensemble pour prévenir et répondre aux attaques cyberterroristes, et pour garantir la sécurité et la résilience de nos systèmes vitaux.

3 LES IMPLICATION

Les implications des technologies numériques dans les conflits modernes sont profondes et complexes, nécessitant une réflexion stratégique et une coopération internationale pour prévenir les abus et promouvoir la paix et la sécurité.

3.1. Impact sur les civils et les droits de l'homme

L'impact des technologies numériques sur les civils et les droits de l'homme dans les conflits est un sujet de préoccupation croissant. Les technologies numériques peuvent être utilisées pour violer les droits de l'homme de manière directe ou indirecte, notamment :

- La surveillance numérique peut être utilisée pour traquer et réprimer les opposants politiques, les activistes et les journalistes, mettant ainsi en danger leur sécurité et leur liberté.
- La propagande numérique peut être utilisée pour diffuser des messages de haine et de violence, contribuant ainsi à l'exacerbation des tensions et des conflits.
- Les attaques cybernétiques peuvent viser les infrastructures critiques, telles que les hôpitaux, les écoles et les systèmes de communication, mettant ainsi en danger la vie des civils.

Les conséquences de ces actions peuvent être dévastatrices pour les civils, notamment :

- Les violations des droits de l'homme, telles que la liberté d'expression et la vie privée, peuvent être multipliées.
- Les civils peuvent être exposés à des risques accrus de violence, de déplacement et de traumatisme.
- Les communautés vulnérables, telles que les femmes, les enfants et les minorités, peuvent être particulièrement touchées.

Il est donc essentiel de prendre des mesures pour protéger les droits de l'homme et prévenir les abus des technologies numériques dans les conflits. Cela peut inclure :

- La mise en place de réglementations et de lois pour encadrer l'utilisation des technologies numériques dans les conflits.
- La promotion de la transparence et de la responsabilité dans l'utilisation des technologies numériques.
- La fourniture d'une assistance et d'un soutien aux victimes des violations des droits de l'homme.

En fin de compte, il est crucial de reconnaître que les technologies numériques sont des outils qui peuvent être utilisés pour le bien ou pour le mal. Il est donc essentiel de travailler ensemble pour promouvoir une utilisation responsable et éthique des technologies numériques dans les conflits.

3.2. Conséquences sur la sécurité nationale et internationale

Les conséquences des technologies numériques sur la sécurité nationale et internationale sont profondes et complexes. Les technologies numériques peuvent être utilisées pour menacer la sécurité nationale et internationale de plusieurs manières, notamment :

- Les attaques cybernétiques peuvent viser les infrastructures critiques, telles que les systèmes de défense, les réseaux de communication et les systèmes financiers, mettant ainsi en danger la stabilité et la sécurité des pays.
- La propagation de fausses informations et de propagande peut contribuer à la déstabilisation des sociétés et des gouvernements, créant ainsi un environnement propice à la violence et au terrorisme.
- Les technologies numériques peuvent également être utilisées pour faciliter le financement du terrorisme, le recrutement de nouveaux membres et la planification d'attaques.

Les conséquences de ces actions peuvent être graves et durables, notamment :

- La perte de confiance dans les institutions et les gouvernements
- L'exacerbation des tensions et des conflits entre les pays et les communautés
- La mise en danger de la sécurité des personnes et des biens
- La perturbation des échanges économiques et commerciaux

Pour faire face à ces menaces, les pays et les organisations internationales doivent travailler ensemble pour :

- Développer des stratégies de sécurité numérique pour protéger les infrastructures critiques et les systèmes d'information.
- Renforcer la coopération internationale pour lutter contre le terrorisme et la cybercriminalité.
- Promouvoir l'utilisation responsable des technologies numériques et encourager l'adoption de normes et de standards de sécurité.
- Fournir une formation et une assistance aux pays et aux organisations pour renforcer leurs capacités de sécurité numérique.

En fin de compte, la sécurité nationale et internationale dépend de notre capacité à utiliser les technologies numériques de manière responsable et à prévenir les abus. Il est essentiel de travailler ensemble pour promouvoir une utilisation sûre et sécurisée des technologies numériques.

Voici quelques objectifs possibles pour notre recherche :

- Analyser l'impact des technologies numériques sur le conflit armé à l'Est de la RDC: Explorer comment les groupes armés utilise les technologies numériques pour propager leurs idées, recruter des membres et mener des opérations.
- Étudier les différentes formes de propagande en ligne : Examiner comment les groupes armés utilisent les réseaux sociaux et les plateformes en ligne pour diffuser des messages de haine et de propagande.
- Investiguer les méthodes de surveillance et de contrôle : Analyser comment les groupes armés utilisent les technologies numériques pour surveiller et contrôler les populations civiles.
- Évaluer les risques de cyber terrorisme : Examiner les menaces potentielles que les groupes armés pourraient poser en termes de cyber attaques et de perturbation des infrastructures critiques.
- Proposer des recommandations pour contrer les effets négatifs des technologies numériques dans le conflit : Offrir des suggestions pour les décideurs politiques, les organisations humanitaires et les communautés locales sur la façon de minimiser les risques associés aux technologies numériques dans le conflit.

Ces objectifs pourraient être atteints en menant des recherches approfondies, en analysant des données et en consultant des experts dans le domaine.

4 Conclusion

En conclusion, cette étude a démontré que les technologies numériques jouent un rôle crucial dans la dynamique du conflit armé en République Démocratique du Congo (RDC). Les groupes armés, les gouvernements et les organisations internationales utilisent les technologies numériques pour influencer l'opinion publique, recruter des combattants, collecter des fonds et mener des opérations de surveillance et de cyber-terrorisme.

Les résultats de cette étude ont montré que les stratégies de propagande, de surveillance et de cyber-terrorisme employées par les différents acteurs ont des implications significatives sur la sécurité et la stabilité de la RDC. Les réseaux sociaux et les plateformes de messagerie sont utilisés pour diffuser des messages de haine et de propagande, recruter des combattants et collecter des fonds, ce qui contribue à l'escalade de la violence et à la radicalisation des populations.

Il est essentiel de prendre des mesures pour prévenir et contrer ces menaces. Les gouvernements et les organisations internationales doivent travailler ensemble pour développer des stratégies efficaces pour lutter contre la propagande et le cyber-terrorisme. Les entreprises de technologie doivent également prendre des mesures pour empêcher l'utilisation de leurs plateformes pour des activités malveillantes.

Enfin, il est important de souligner que la lutte contre le cyber-terrorisme et la propagande en RDC nécessite une approche globale et coordonnée. Les efforts doivent être déployés pour promouvoir la paix, la stabilité et la sécurité dans la région, et pour soutenir les populations affectées par le conflit.

Pour lutter contre les effets négatifs des technologies numériques dans le conflit, nous recommandons :

- Les gouvernements et les organisations internationales doivent développer des stratégies efficaces pour lutter contre la propagande et le cyber-terrorisme en RDC.
- Les entreprises de technologie doivent prendre des mesures pour empêcher l'utilisation de leurs plateformes pour des activités malveillantes.
- Les efforts doivent être déployés pour promouvoir la paix, la stabilité et la sécurité dans la région.
- La mise en place d'une réglementation claire et efficace pour encadrer l'utilisation des technologies numériques dans les conflits.
- La promotion de l'éducation et de la sensibilisation aux risques liés aux technologies numériques et à leur utilisation responsable.
- Le renforcement de la coopération internationale pour lutter contre le cyber-terrorisme et la propagande haineuse.
- La fourniture d'une assistance et d'un soutien aux victimes des violations des droits de l'homme commises à l'aide des technologies numériques.

- Les populations affectées par le conflit doivent être soutenues et protégées.

PERSPECTIVES FUTURES

- Cette étude ouvre des perspectives pour des recherches futures sur le rôle des technologies numériques dans les conflits armés en Afrique.
- Il est important de poursuivre les recherches sur les stratégies de propagande, de surveillance et de cyber-terrorisme employées par les différents acteurs.
- Les résultats de cette étude peuvent être utilisés pour informer les politiques et les pratiques pour prévenir et contrer les menaces du cyber-terrorisme en RDC et ailleurs.

REFERENCES

[1] Atran, S. (2016). L'État islamique : une révolution dans la terreur. Éditions du Seuil.

[2] Freeman, M. (2017). Le financement du terrorisme. Éditions de l'Université de Cambridge.

[3] Global Humanitarian Forum. (2022). Global Humanitarian Outlook.

[4] Global Witness. (2017). The Hill Belongs to Everyone: How the mining industry in the DRC is failing to deliver for women.

[5] https://cyberjustice.blog/2023/05/25/la-menace-grandissante-du-cyberterrorisme/.

[6] https://www.oiq.qc.ca/publication/infrastructures-critiques-sarmer-contre-les-cyberattaques/

[7] https://www.vpnunlimited.com/help/cybersecurity/cyberterrorism

[8] Human Rights Watch. (2018). "Our Best Weapon is the Sword": How Armed Groups Use Violence to Control the Population in the Eastern DRC.

[9] Human Rights Watch. (2018). Les droits de l'homme dans le monde en 2018.

[10] International Crisis Group. (2020). Congo : sortir de la crise à l'est.

[11] Interpol. (2019). Rapport sur la cybercriminalité.

[12] Katz, R. (2017). La désinformation et la démocratie. Éditions de l'Université de Georgetown.

[13] Mamdani, M. (2001). When Victims Become Killers: Colonialism, Nativism, and the Genocide in Rwanda. Princeton University Press.

[14] Office des Nations Unies pour la coordination des affaires humanitaires. (2022). République démocratique du Congo : Situation humanitaire.

[15] Prunier, G. (2009). Africa's World War: Congo, the Rwandan Genocide, and the Making of a Continental Catastrophe. Oxford University Press.

[16] Stern, J., & Berger, J. M. (2015). L'État islamique : la propagande vue de l'intérieur. Editions du Seuil.

[17] UNESCO. (2017). L'éducation aux médias et à l'information.

[18] United Nations. (2018). Rapport du Secrétaire général sur la lutte contre le terrorisme.

[19] Weimann, G. (2016). Cyberterrorisme : la menace invisible. Éditions de l'Université de Tel-Aviv.