

L'économie des ransomWare et cyberterrorisme en Afrique.

Par Dr Aimée Laure NJANJO EKOUMKANG

Dans **REVUE AFRICAINE DE PROSPECTIVE STRATÉGIQUE (RAPS)**, volume spécial, N°3, « Retour de la guerre », 2026

Joseph Vincent NTUDA EBODE (Dir)

Éditions **CENTRE DE RECHERCHE D'ÉTUDES POLITIQUES ET STRATÉGIQUES / UNIVERSITÉ DE YAOUNDÉ II**, Page 103 à 123

ISBN : 978-9956-0-2264-9

Article disponible en ligne à l'adresse
<https://www.creps.com>



Distribution électronique

La reproduction ou représentation de cet article, notamment par photocopie, n'est autorisée que dans les limites des conditions générales d'utilisation du site ou, le cas échéant, des conditions générales de la licence souscrite par votre établissement. Toute autre reproduction ou représentation, en tout ou partie, sous quelque forme et de quelque manière que ce soit, est interdite sauf accord préalable et écrit de l'éditeur, en dehors des cas prévus par la législation en vigueur au Cameroun. Il est précisé que son stockage dans une base de données est également interdit.

L'ÉCONOMIE DES RANSOMWARE ET CYBERTERRORISME EN AFRIQUE

Dr Aimée Laure NJANJO EKOUNGKANG

Ph.D Science Politique

Chargée de cours

Université de Bertoua

Résumé

Il est particulièrement intéressant de constater à quel point les TIC et le numérique trouvent toujours un écho favorable dans les études de Science Politique. Si du point de vue de la gouvernance ces derniers tendent à être encadrés par les pouvoirs publics ; ils exercent par ailleurs une influence considérable sur les modes de gestion publique et d'exercice du pouvoir au sein des systèmes politiques. Dans le domaine des relations internationales, ces derniers modifient également les rapports entre les Etats et les différents acteurs sur la scène internationale. Bien que les problématiques dans ce domaine ne soient pas toujours nouvelles ; elles se réinventent au fil des prouesses technologiques qui redynamisent les rapports ainsi que les échanges sur la scène internationale. C'est en effet le cas de la criminalité transfrontalière et internationale qui trouve un souffle nouveau à travers les progrès technologiques et les ransomware en sont le parfait exemple. On observe depuis quelques années de nouvelles formes de cybercriminalité plus agressives qui portent atteinte à la sécurité des Etats, il s'agit des ransomware. A la base des cybercrimes classiques, ces derniers sont devenus une véritable menace selon certains Etats qui les considèrent aujourd'hui comme des actes terroristes.

La présente recherche s'interroge sur l'impact des ransomware sur le terrorisme (cyberterrorisme) et la raison pour laquelle ces derniers tendent à être considérés comme des crimes cyberterroristes ? Cette étude s'inscrit dans une large mesure dans les études sur la gouvernance numérique au niveau national et international englobant des questions purement technologiques et techniques à des analyses sociopolitiques. L'intérêt est d'explorer les mutations en matière de cybercrime qui peuvent porter atteinte à l'intégrité et la sécurité d'un Etat tant dans l'espace physique que dans l'espace « numérique » dans un contexte de gouvernance numérique. Il s'agit d'une analyse à la fois quantitative et qualitative, basée sur une collecte de données de seconde main produites par les rapports des cabinets d'expertise en cybercriminalité et cybersécurité, des données empiriques, ainsi que la littérature qui s'y rapporte. En inscrivant cette étude dans une approche néoréaliste et constructiviste, il en ressort que les ransomware révolutionnent le terrorisme et particulièrement le cyberterrorisme en le radicalisant, tout en faisant surgir un nouveau type d'acteurs sur la scène internationale. Par ailleurs ; les ransomware transforment le financement participatif du terrorisme à travers un double système d'extorsion auprès de la société civile et des gouvernements ce qui le rend aux yeux de certains Etats dangereux pour la sécurité nationale et internationale.

Mots clés : Ransomware, terrorisme, économie, Cybercriminalité, financement.

Abstract

It is particularly interesting to note how ICT and digital technology still find a favorable echo in Political Science studies. While from a governance perspective these tend to be regulated by public authorities, they also exert considerable influence on the methods of public management and the exercise of power within political systems. In the field of international relations, they are also altering the relationships between states and various actors on the international stage. Although the issues in this area are not always new; they are reinvented with technological advances that revitalize relationships and exchanges on the international stage. This is indeed the case with transnational and international crime, which is finding new impetus through technological progress, and ransomware is a perfect example. In recent years, we have observed new, more aggressive forms of cybercrime that threaten the security of states; these are ransomware attacks. At the root of classic cybercrimes, these have become a real threat according to some states which now consider them to be terrorist acts.

This research examines the impact of ransomware on terrorism (cyberterrorism) and why it is increasingly being categorized as a cyberterrorist crime. This study falls largely within the broader context of digital governance research at the national and international levels, encompassing everything from purely technological and technical issues to socio-political analyses. The aim is to explore the evolving nature of cybercrime, which can undermine the integrity and security of a state in both the physical and digital realms, within the framework of digital governance. This analysis combines quantitative and qualitative methods, drawing on secondary data from reports by cybercrime and cybersecurity consulting firms, empirical data, and relevant literature. By adopting a neorealist and constructivist approach, this study reveals that ransomware is revolutionizing terrorism, and particularly cyberterrorism, by radicalizing it and giving rise to a new type of actor on the international stage. Furthermore, ransomware is transforming the crowdfunding of terrorism through a dual system of extortion targeting civil society and governments, making it a threat to national and international security in the eyes of some states.

Keywords: Ransomware, terrorism, economy, cybercrime, financing.