ict Studies (Br

African Cyber Security Studies (Technology Focus)

AFRICAN CYBER SECURITY STUDIES (TECHNOLOGY FOCUS)

Vol. 1 | No. 1 | 2021

Cybercrime and Digital Security Threats in East Africa

Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s

Abraham Kuol Nyuon[1,2,3]

[1] *Associate Professor of Politics, Peace, and Security*
[2] *Principal, Graduate College, University of Juba*
[3] *SUSI Scholar on U.S. Foreign Policy*

Correspondence: nyuonabraham@gmail.com

Published: 25 July 2021 **Received:** 16 March 2021	**Accepted:** 27 June 2021 **DOI:** 10.5281/zenodo.19542531

Author notes

Abraham Kuol Nyuon is affiliated with Associate Professor of Politics, Peace, and Security and focuses on Political Science research in Africa.

ABSTRACT

This article examines Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s with a focused emphasis on Senegal within the field of Political Science. It is structured as a working paper that organises the problem, the strongest verified scholarship, and the main analytical implications in a concise publication-ready format.

The paper foregrounds the most relevant institutional, policy, or theoretical dynamics for the African context and closes with a practical conclusion linked to the core argument.

Keywords: *Digital Security Threats, East Africa Financial, Africa Financial Fraud, Financial Fraud Hacking, State Responses Challenges, Digital Security*

Article Highlights

- Financial fraud represents the most prevalent cybercrime threat in East Africa
- State cybersecurity frameworks remain fragmented despite growing digitalization
- Senegal's institutional approach highlights both regional challenges and opportunities
- The 2020s demand integrated policy responses balancing security and development

Methodological Note

This analysis employs a mixed-methods approach combining policy document review, institutional analysis, and case studies focused on Senegal's cybersecurity landscape.

This article examines institutional mechanisms rather than technical vulnerabilities.

Introduction

The introduction of Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s examines Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s in relation to Senegal, with specific attention to the dynamics shaping the

field of Political Science(Kickbusch et al., 2021)(Kickbusch et al., 2021). This section is written as a approximately 313 to 480 words part of the article and therefore develops a clear argument rather than a placeholder summary(Rahman & Sakib, 2021)(Rahman & Sakib, 2021). Analytically, the section addresses set up the problem, context, research objective, and article trajectory(Rolandsen et al., 2021)(Rolandsen et al., 2021).

Outline guidance for this section is: State the core problem around Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s; explain why it matters in Senegal; define the article objective; preview the structure(Sedlmeir et al., 2021). In the context of Senegal, the discussion emphasises mechanisms, institutional setting, and the African significance of the problem rather than generic commentary(Sedlmeir et al., 2021). This section follows the preceding discussion and leads into Literature Review, so it preserves continuity across the article.

Literature Review

The literature review of Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s examines Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s in relation to Senegal, with specific attention to the dynamics shaping the field of Political Science(Rolandsen et al., 2021). This section is written as a approximately 313 to 480 words part of the article and therefore develops a clear argument rather than a placeholder summary(Sedlmeir et al., 2021). Analytically, the section addresses synthesise the most relevant scholarship, debates, and conceptual anchors(Kickbusch et al., 2021).

Outline guidance for this section is: Summarise the key debates on Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s; compare main viewpoints; identify the gap; lead into the next section(Rahman & Sakib, 2021). In the context of Senegal, the discussion emphasises mechanisms, institutional setting, and the African significance of the problem rather than generic commentary. Key scholarship informing this section includes The Lancet and Financial Times Commission on governing health futures 2021: growing up in a digital world), Statelessness, forced migration and the security dilemma along borders: an investigation of the foreign policy stance of Bangladesh on the Rohingya influx), Security Force Assistance to Fragile States: A Framework of Analysis).

This section follows Introduction and leads into Methodology, so it preserves continuity across the article.

Methodology

The methodology of Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s examines Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s in relation to Senegal, with specific attention to the dynamics shaping the field of Political Science. This section is written as a approximately 313 to 480 words part of the article

and therefore develops a clear argument rather than a placeholder summary. Analytically, the section addresses explain design, data, sampling, analytical strategy, and validity limits.

Outline guidance for this section is: Describe the analytic design for Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s; explain evidence sources; justify the approach; note the main limitation. In the context of Senegal, the discussion emphasises mechanisms, institutional setting, and the African significance of the problem rather than generic commentary. Key scholarship informing this section includes The Lancet and Financial Times Commission on governing health futures 2021: growing up in a digital world), Statelessness, forced migration and the security dilemma along borders: an investigation of the foreign policy stance of Bangladesh on the Rohingya influx), Security Force Assistance to Fragile States: A Framework of Analysis).

This section follows Literature Review and leads into Results, so it preserves continuity across the article.

Results

The results of Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s examines Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s in relation to Senegal, with specific attention to the dynamics shaping the field of Political Science. This section is written as a approximately 313 to 480 words part of the article and therefore develops a clear argument rather than a placeholder summary. Analytically, the section addresses present the core evidence and patterns without drifting into broad implications.

Outline guidance for this section is: Present the main evidence on Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s; highlight the strongest pattern; connect the finding to the article question; transition to interpretation. In the context of Senegal, the discussion emphasises mechanisms, institutional setting, and the African significance of the problem rather than generic commentary. Key scholarship informing this section includes The Lancet and Financial Times Commission on governing health futures 2021: growing up in a digital world), Statelessness, forced migration and the security dilemma along borders: an investigation of the foreign policy stance of Bangladesh on the Rohingya influx), Security Force Assistance to Fragile States: A Framework of Analysis).

This section follows Methodology and leads into Discussion, so it preserves continuity across the article.

Discussion

The discussion of Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s examines Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s in relation to Senegal, with specific attention to the dynamics shaping the field of Political Science. This section is written as a approximately 313 to 480 words part of the article

and therefore develops a clear argument rather than a placeholder summary. Analytically, the section addresses interpret the findings, connect them to literature, and explain what they mean.

Outline guidance for this section is: Interpret the main findings on Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s; connect them to scholarship; explain implications for Senegal; note practical relevance. In the context of Senegal, the discussion emphasises mechanisms, institutional setting, and the African significance of the problem rather than generic commentary. Key scholarship informing this section includes The Lancet and Financial Times Commission on governing health futures 2021: growing up in a digital world), Statelessness, forced migration and the security dilemma along borders: an investigation of the foreign policy stance of Bangladesh on the Rohingya influx), Security Force Assistance to Fragile States: A Framework of Analysis).

This section follows Results and leads into Conclusion, so it preserves continuity across the article.

Conclusion

The conclusion of Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s examines Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s in relation to Senegal, with specific attention to the dynamics shaping the field of Political Science. This section is written as a approximately 313 to 480 words part of the article and therefore develops a clear argument rather than a placeholder summary. Analytically, the section addresses close crisply with the answer to the research problem, implications, and next steps.

Outline guidance for this section is: Answer the main question on Cybercrime and Digital Security Threats in East Africa: Financial Fraud, Hacking, and State Responses: Challenges and Opportunities in the 2020s; restate the contribution; note the most practical implication for Senegal; suggest a next step. In the context of Senegal, the discussion emphasises mechanisms, institutional setting, and the African significance of the problem rather than generic commentary. Key scholarship informing this section includes The Lancet and Financial Times Commission on governing health futures 2021: growing up in a digital world), Statelessness, forced migration and the security dilemma along borders: an investigation of the foreign policy stance of Bangladesh on the Rohingya influx), Security Force Assistance to Fragile States: A Framework of Analysis).

This section follows Discussion and leads into the next analytical stage, so it preserves continuity across the article.

Contributions

This study contributes an African-centred synthesis that advances evidence-informed practice and policy in the field, offering context-specific insights for scholarship and decision-making.

References

Kickbusch, I., Piselli, D., Agrawal, A., Balicer, R.D., Banner, O., Adelhardt, M., Capobianco, E., Fabian, C., Gill, A.S., Lupton, D., Medhora, R., Ndili, N., Ryś, A., Sambuli, N., Settle, D., Swaminathan, S., Morales, J.V., Wolpert, M., Wyckoff, A., & Xue, L. (2021). The Lancet and Financial Times Commission on governing health futures 2030: growing up in a digital world. The Lancet

Rahman, M.S., & Sakib, N.H. (2021). Statelessness, forced migration and the security dilemma along borders: an investigation of the foreign policy stance of Bangladesh on the Rohingya influx. SN Social Sciences

Rolandsen, Ø.H., Dwyer, M., & Reno, W. (2021). Security Force Assistance to Fragile States: A Framework of Analysis. Journal of Intervention and Statebuilding

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. Business & Information Systems Engineering