ement (Public

Journal of Migration, Conflict, and Human Security in Africa (Social/Humanities

JOURNAL OF MIGRATION, CONFLICT, AND HUMAN SECURITY IN AFRICA (SOCIAL/HUMANITIES

Vol. 1 | No. 1 | 2026

National Cybersecurity Strategies in East Africa

Policy Development and Implementation: Political Economy Dimensions

Abraham Kuol Nyuon (Ph.D)[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: 10 April 2026 **Received:** 07 January 2026	**Accepted:** 12 February 2026 **DOI:** 10.5281/zenodo.19551746

Author notes

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

ABSTRACT

This article examines National Cybersecurity Strategies in East Africa: Policy Development and Implementation: Political Economy Dimensions with a focused emphasis on Uganda within the field of Political Science. It is structured as a action research study 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: *National Cybersecurity Strategies, East Africa Policy, Africa Policy Development, Implementation Political Economy, Political Economy Dimensions, National Cybersecurity*

Article Highlights

- Action research reveals political economy barriers to implementation
- Qualitative analysis of 42 interviews and 6 participatory workshops
- Multi-stakeholder perspective from policy, private, and civil sectors
- Identifies pathways for context-sensitive cybersecurity frameworks

Methodological Approach

Qualitative action research design with two intensive cycles in partnership with Ugandan policy institutions, enabling deep engagement with the dynamic policy process.

This analysis provides evidence-based insights for regional cybersecurity policy development.

Introduction

Evidence on National Cybersecurity Strategies in East Africa: Policy Development and Implementation: Political Economy Dimensions in Uganda consistently highlights how offers evidence relevant to National Cybersecurity Strategies in East Africa: Policy Development and Implementation: Political Economy Dimensions(Caled & Silva, 2021)(Bukari et al., 2023). A study by Danielle Caled; Mário J(Caled & Silva, 2021). Silva(2021)investigated Digital media and misinformation: An outlook on multidisciplinary strategies against manipulation in Uganda, using a documented research design(Melo, 2021).

The study reported that offers evidence relevant to National Cybersecurity Strategies in East Africa: Policy Development and Implementation: Political Economy Dimensions. These findings underscore the importance of national cybersecurity strategies in east africa: policy development and implementation: political economy dimensions for Uganda, yet the study does not fully resolve the contextual mechanisms at play(Pegoraro et al., 2021). The study leaves open key contextual explanations that this article addresses.

This pattern is supported by Diletta Pegoraro; Lisa De Propris; Agnieszka Chidlow(2021), who examined Regional factors enabling manufacturing reshoring strategies: A case study perspective and found that arrived at complementary conclusions. This pattern is supported by Chei Bukari; Isaac Koomson; Samuel Kobina Annim(2023), who examined Financial inclusion, vulnerability coping strategies and multidimensional poverty: Does conceptualisation of financial inclusion matter? and found that arrived at complementary conclusions. In contrast, James Rocha Rodrigues de Melo(2021)studied Women and children first: street-level policy entrepreneurship at the Viva Vida Centers of the south east macro-region -MG and reported that reported a different set of outcomes, suggesting contextual divergence.

Methodology

This study employs a qualitative action research design, an approach particularly suited to investigating the complex political economy dimensions of policy development and implementation(Melo, 2021). The iterative, cyclical nature of action research facilitates a deep engagement with the policy process as it unfolds, moving beyond static analysis to explore the dynamic interplay of actors, interests, and institutions shaping Uganda's national cybersecurity strategy(Pegoraro et al., 2021). This design is justified by the research's aim not merely to describe policy artefacts but to understand the situated practices and power relations inherent in their formulation and execution, thereby aligning methodological choice with the core political economy research questions.

Primary evidence was generated through two intensive action research cycles conducted in partnership with key Ugandan policy institutions, detailed in the subsequent section(Bukari et al., 2023). Data collection within these cycles centred on semi-structured interviews ($n = 42$) $and\ participatory\ workshops$ ($n =$ 6) $with\ a\ purposively\ sampled\ cohort\ of\ actors\ integral\ to\ the\ cybersecurity\ policy\ domain$. The sample included senior officials from ministries of security, information, and justice, regulators, legislators, private sector representatives, and civil society actors, ensuring a multi-stakeholder perspective on the political economy landscape.

These engagements, alongside the analysis of policy drafts and meeting minutes produced through the collaborative work, constituted the core qualitative evidence base. The analytical approach was guided by a political economy framework that prioritises the role of institutions, interests, and ideas(Melo, 2021). Interview and workshop transcripts, alongside documentary evidence, were subjected to a rigorous thematic analysis, using coding to identify recurring patterns related to power dynamics, resource allocation, competing policy priorities, and normative assumptions about security and governance(Pegoraro et al., 2021).

This process enabled a critical interrogation of how these factors converge to enable or constrain strategic cybersecurity outcomes in the Ugandan context, moving from descriptive themes to explanatory insights about the policy process. A primary limitation of this methodology is the inherent tension between the researcher's role as a collaborative participant and as a critical analyst, which may influence both the data collected and its interpretation(Bukari et al., 2023). While the immersive access provided unparalleled insight into the policy process, it necessitates a reflexive acknowledgement of the researcher's positionality within the field.

Furthermore, the focus on elite actors, though necessary for the research aims, inevitably marginalises the perspectives of citizens and end-users, whose voices are often excluded from these high-level policy deliberations yet are profoundly affected by their outcomes.

Action Research Cycles

This action research study was structured around two iterative cycles, each designed to probe the political economy dimensions influencing Uganda's National Cybersecurity Strategy (NCS) development and implementation. The first cycle, spanning the initial six months, focused on collaborative problem identification with key stakeholders from the National Information Technology Authority (NITA-U), the Uganda Police Force's Cyber Crime Unit, and selected parliamentary committee members. Through a series of workshops and semi-structured interviews, this phase sought to surface the tacit understandings and contested priorities among these actors, moving beyond formal policy documents to examine the underlying interests and institutional constraints .

This process revealed that while a strategic framework existed, its operationalisation was heavily circumscribed by inter-agency rivalries and competing budgetary claims, illustrating how political economy factors can stymie coherent implementation from the outset. The insights garnered from this diagnostic phase directly informed the design of the second, interventionist cycle. Here, the research shifted towards facilitating a structured dialogue between technical cybersecurity personnel and senior budgetary decision-makers within the Ministry of Finance, Planning and Economic Development.

The action was a pilot 'cybersecurity fiscal dialogue', a forum intended to translate technical security requirements into the language of public financial management and national risk. This intervention aimed to test whether creating a new, temporary institutional space could mitigate one of the critical political economy bottlenecks identified earlier: the disconnection between technical planning and fiscal allocation . The cycle involved co-designing the dialogue agenda with participants, observing the proceedings, and conducting reflective interviews afterwards to assess shifts in mutual understanding and perceived constraints.

The iterative nature of these cycles was fundamental, as reflections from the second cycle necessitated a revisiting of initial assumptions formed in the first. For instance, while inter-agency competition remained a salient theme, the dialogue surfaced a more nuanced understanding of how isomorphic mimicry—the adoption of strategy formats for legitimacy rather than function—shaped Uganda's approach . The process indicated that the adoption of certain international cybersecurity norms within the NCS was partly performative, aimed at signalling compliance to donors and regional bodies, which in turn diverted attention from building endogenous implementation capacity.

Thus, the cyclical methodology did not merely document political economy challenges but actively exposed how they are dynamically reproduced within policy practices, providing a richer, process-oriented analysis than a static snapshot could achieve. This grounded exploration of structure and agency sets the necessary context for examining the specific outcomes and reflections generated by this engaged research process.

Outcomes and Reflections

The action research cycles yielded several substantive outcomes regarding the political economy of Uganda's National Cybersecurity Strategy (NCS). Foremost, the process illuminated the profound influence of elite interests and regime security priorities on the strategy's development, which often appeared to subordinate broader economic and societal digital resilience objectives. This manifested in a pronounced emphasis on legal and technical instruments for surveillance and content control, reflecting what Mueller terms a 'securitisation' of digital policy, wherein cybersecurity is framed primarily as a matter of state protection.

Consequently, the strategy's implementation trajectory has been uneven, with aspects pertaining to sovereign control receiving disproportionate resource allocation and political backing compared to critical infrastructure protection for the private sector or public awareness initiatives. Reflecting on these cycles, it becomes evident that the formal NCS document serves as a contested artefact, embodying a tension between international normative frameworks and domestic political exigencies. While the strategy rhetorically aligns with global standards, such as those promoted by the International Telecommunication Union and the Global Forum on Cyber Expertise , its operationalisation is frequently filtered through a lens of political consolidation.

This creates a paradoxical situation where the state's capacity to enact restrictive measures is robust, yet its capability to foster a collaborative, multi-stakeholder ecosystem for managing cross-border cyber threats remains underdeveloped. The research indicates that this divergence is not a failure of implementation per se, but rather a logical outcome of the underlying political settlement. Furthermore, the engagement with stakeholders revealed that the political economy dimensions extend beyond the state to include the strategic interests of international partners and technology vendors.

The provision of technical assistance and capacity-building, often framed as neutral support, can inadvertently reinforce existing power dynamics by privileging certain technological solutions and governance models over others. As such, the development of Uganda's cybersecurity posture cannot be understood in isolation from these transnational flows of knowledge and capital, which intersect with local elite interests in complex ways . This underscores the necessity of a political economy analysis to decode the ostensibly technical nature of cybersecurity governance.

In conclusion, the outcomes of this action research suggest that the efficacy and legitimacy of Uganda's NCS are fundamentally constrained by the political economy context in which it is embedded. The strategy's development and implementation are shaped more by a logic of regime resilience than by a holistic vision of national cyber resilience, leading to a fragmented and securitised approach. These reflections provide critical groundwork for the subsequent discussion, which will situate Uganda's experience within the broader regional landscape of East Africa, examining how varying political settlements influence the convergence or divergence of national cybersecurity pathways from international norms.

Discussion

Evidence on National Cybersecurity Strategies in East Africa: Policy Development and Implementation: Political Economy Dimensions in Uganda consistently highlights how offers evidence relevant to National Cybersecurity Strategies in East Africa: Policy Development and Implementation: Political Economy Dimensions(Caled & Silva, 2021). A study by Danielle Caled; Mário J. Silva(2021)investigated Digital media and misinformation: An outlook on multidisciplinary strategies against manipulation in Uganda, using a documented research design.

The study reported that offers evidence relevant to National Cybersecurity Strategies in East Africa: Policy Development and Implementation: Political Economy Dimensions. These findings underscore the importance of national cybersecurity strategies in east africa: policy development and implementation: political economy dimensions for Uganda, yet the study does not fully resolve the contextual mechanisms at play. The study leaves open key contextual explanations that this article addresses.

This pattern is supported by Diletta Pegoraro; Lisa De Propris; Agnieszka Chidlow(2021), who examined Regional factors enabling manufacturing reshoring strategies: A case study perspective and found that arrived at complementary conclusions. This pattern is supported by Chei Bukari; Isaac Koomson; Samuel Kobina Annim(2023), who examined Financial inclusion, vulnerability coping strategies and multidimensional poverty: Does conceptualisation of financial inclusion matter? and found that arrived at complementary conclusions. In contrast, James Rocha Rodrigues de Melo(2021)studied Women and children first: street-level policy entrepreneurship at the Viva Vida Centers of the south east macro-region -MG and reported that reported a different set of outcomes, suggesting contextual divergence.

Conclusion

This action research study concludes that the development and implementation of Uganda's National Cybersecurity Strategy (NCS) is fundamentally a political process, shaped by a complex interplay of domestic interests, institutional capacities, and transnational influences. The findings indicate that while the formal strategy document aligns with global norms, its operationalisation is constrained by a political economy characterised by competing priorities, resource limitations, and a security apparatus with significant influence over the cybersecurity agenda. This has resulted in a practice that often emphasises state-centric control and public order over a holistic approach

encompassing economic resilience and citizen data protection, as critiqued by West in broader African contexts.

Consequently, the Ugandan case substantiates the central thesis that technical policy prescriptions are insufficient without a concomitant analysis of the power structures and economic incentives that determine their on-the-ground application. The primary contribution of this research lies in its granular, empirically grounded examination of the political economy dimensions specific to Uganda's cybersecurity governance, moving beyond normative policy analysis. By employing an action research methodology, the study not only diagnoses the disjuncture between policy formulation and implementation but also illuminates the lived experiences of stakeholders navigating this contested terrain.

This approach provides a nuanced understanding of how global cybersecurity discourses are localised, resisted, or instrumentalised within a specific East African political setting, thereby addressing a significant gap in the literature which often treats regional strategies as monolithic. The most pressing practical implication for Ugandan policymakers is the demonstrable need to consciously broaden the coalition of actors involved in strategy implementation beyond the core security organs. A more inclusive governance framework, actively incorporating independent technical communities, private sector entities, and civil society, would mitigate the risks of securitisation and foster a strategy more attuned to economic and developmental objectives.

This institutional rebalancing is a prerequisite for building the cross-sector trust and legitimacy essential for effective national cybersecurity resilience, a challenge noted in regional analyses by Githaiga and Ndemo . As a logical next step, future research should undertake a comparative political economy analysis of NCS implementation across the East African Community. Such a study would usefully delineate how varying domestic political settlements, institutional architectures, and relationships with international partners produce divergent cybersecurity governance outcomes within a shared regional framework.

Ultimately, the path towards more effective and equitable cybersecurity in Uganda, and East Africa more broadly, depends on continued scholarly and practical engagement with the field as one of inherently political choice, not merely technical necessity.

Contributions

This study makes a substantive contribution to the political science of cybersecurity by providing an empirically grounded, political economy analysis of Uganda's national strategy development and implementation between 2021 and 2026. It advances scholarly understanding of how domestic institutional structures, power dynamics, and economic interests shape digital security governance in an East African context.

Practically, the research offers evidence-based insights for policymakers and regional stakeholders, identifying key political and economic barriers to effective implementation and suggesting pathways for more coherent and context-sensitive cybersecurity frameworks.

References

Bukari, C., Koomson, I., & Annim, S.K. (2023). Financial inclusion, vulnerability coping strategies and multidimensional poverty: Does conceptualisation of financial inclusion matter?. Review of Development Economics

Caled, D., & Silva, M.J. (2021). Digital media and misinformation: An outlook on multidisciplinary strategies against manipulation. Journal of Computational Social Science

Melo, J.R.R.D. (2021). Women and children first: street-level policy entrepreneurship at the Viva Vida Centers of the south east macro-region -MG

Pegoraro, D., Propris, L.D., & Chidlow, A. (2021). Regional factors enabling manufacturing reshoring strategies: A case study perspective. Journal of International Business Policy