ZAINA FOUNDATION

THE GENDERED BLACKOUT

Impacts of the October 2025 Internet Shutdown on Women in Tanzania

A Comprehensive Research and Advocacy Report

Prepared by **Zaina Foundation**
Published: **September 2026**

Executive Summary

This report provides an extensive and analytical critique of the nationwide internet shutdown enforced by the Government of Tanzania and coordinated through the Tanzania Communications Regulatory Authority (TCRA) during the general election period from October 29, 2025, to early November 2025. While state apparatuses systematically defended the digital blackout through public safety paradigms, national security directives, and the necessity to manage post-election narrative friction, this report reveals that the socio-technical fallout was structurally gendered, falling disproportionately and heavily on Tanzanian women.

Using rigorous desk research, secondary data synthesis, and technical indicators provided by global digital watchdogs such as NetBlocks and regional policy centers like the Collaboration on International ICT Policy for East and Southern Africa (CIPESA), Zaina Foundation maps out the deep human and macroeconomic damage caused by this 126-hour total shutdown. The economic metrics alone reveal a staggering national loss exceeding $238 million USD due to the combined impacts of the election week blackout ($72.3M) and the long-term, pre-election suspension of platform X ($165.8M). However, the real tragedy lies in the severe social and physical cost: the immediate isolation of Women Human Rights Defenders (WHRDs), the silencing of female journalists reporting from volatile field locations, the abrupt collapse of informal micro-e-commerce networks sustained by thousands of low-income female traders, and the complete severing of crisis response and medical lifelines for rural women and women with disabilities.

> Key Insufficiency: The traditional gender-blind approach to analyzing internet shutdowns obscures the specific systemic vulnerabilities forced upon women, who already experience a 24% lower rate of mobile internet access across Sub-Saharan Africa.

This document serves as an urgent advocacy tool, designed to provide civil society organizations, legal professionals, and international oversight bodies with the technical, human, and legal evidence necessary to push for absolute anti-shutdown guarantees, judicial oversight protocols, and structural reforms within Tanzania's telecommunications architecture.

CONTENTS

Executive Summary	2
1. Introduction	4
2. Methodology and Theoretical Approach	5
Primary Analytical Pillars:	5
3. Tanzania's Digital Rights Landscape	6
4. Timeline and Chronology of the Shutdown	7
5. Technical Evidence and Quantitative Economic Damage	8
6. Human Rights Framework and International Standards	11
7. Women Human Rights Defenders (WHRDs)	13
8. Women Journalists and Media Workers	13
9. Women Entrepreneurs and Informal Micro-Traders	14
10. Political Participation and Electoral Equity	14
11. Gender-Based Violence and Crisis Response	15
12. Rural Women and Smallholder Farmers	15
13. Women with Disabilities and Accessibility Barriers	16
14. International and Regional Responses	16
15. Comparative African Lessons and Legal Precedents	17
16. Detailed Policy Recommendations	18
To the Government of Tanzania and TCRA	18
To the Judiciary	18
To Civil Society Organizations and International Donors	18
17. Conclusion	18
References:	19

1. Introduction

Zaina Foundation is a registered Non-Governmental Organization established under the Non-Governmental Organizations Act [CAP 56 RE 2023] of the Laws of the United Republic of Tanzania. Founded with a vision to rectify historical gender imbalances within the tech industry, our mandate focuses strictly on promoting digital rights, inclusion, and safety by empowering women across all areas of technology and digital communication. As an advocacy entity, Zaina Foundation reviews, critiques, and challenges domestic legal provisions that infringe upon freedom of expression, digital safety, and press freedom, ensuring that marginalized genders are not left behind in the expanding East African information landscape.

In October 2025, Tanzania entered a highly tense political landscape during its general elections. On the morning of October 29, 2025, as voters began queuing at polling stations across both the mainland and Zanzibar, the state implemented an absolute, unannounced, and coordinated nationwide digital blockade. The complete cut-off of mobile data, social platforms, and basic messaging applications persisted for exactly 5 days and 6 hours (126 hours), continuing through the critical vote-counting and post-election periods.

For Tanzanian women, who already face a structural digital divide due to lower device ownership rates, higher data costs, and lower digital literacy, this blackout was not a temporary technical inconvenience. It was a profound structural crisis. This report moves past basic connectivity tracking to document the real human impact of this event. It shows how state-directed technical blackouts act as a multiplier of gendered oppression, exposing women to economic shocks, physical dangers, and political exclusion.

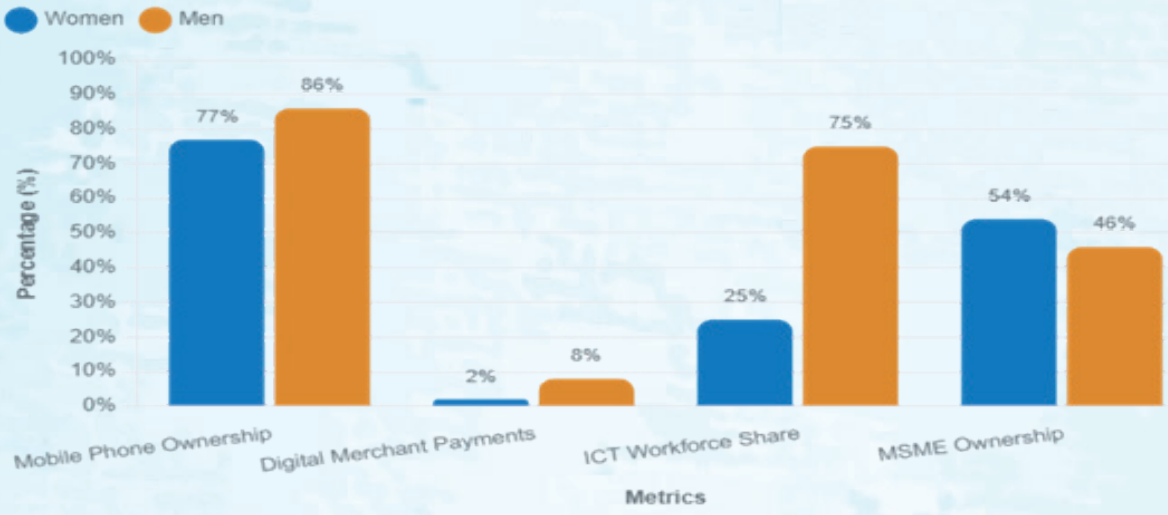


Figure 1: Breakdown of the digital and economic ownership data comparing women and men in Tanzania

2. Methodology and Theoretical Approach

Zaina Foundation utilized an exhaustive desk-based research methodology and qualitative data synthesis framework from late 2025 to mid-2026. This approach deliberately avoids generic, single-point surveys to focus instead on aggregating, validating, and cross-referencing expansive public records, technical whitepapers, civil society logs, and regional policy studies.

Primary Analytical Pillars:

Zaina Foundation utilized an exhaustive desk-based research methodology and qualitative data synthesis framework from late 2025 to mid-2026. This approach deliberately avoids generic, single-point surveys to focus instead on aggregating, validating, and cross-referencing expansive public records, technical whitepapers, civil society logs, and regional policy studies.

- Network Measurement and Telemetry Triangulation: Analysis of border gateway protocol (BGP) routing tables, domain name system (DNS) tampering data, and server response logs provided by NetBlocks, the Open Observatory of Network Interference (OONI), and localized censorship probes.

- Regional Policy and Civil Society Fact-Checking: Deep textual integration of policy briefings, global situational updates, and legal research issued by CIPESA, the Paradigm Initiative, Access Now, and the #KeepItOn coalition.

- Legal and Framework Synthesis: A complete statutory review comparing the Tanzanian state's administrative actions against the provisions of the Constitution of the United Republic of Tanzania (1977), the East African Community (EAC) Treaty, the African Charter on Human and Peoples' Rights (ACHPR), and the International Covenant on Civil and Political Rights (ICCPR).

3. Tanzania's Digital Rights Landscape

Prior to the severe events of October 2025, Tanzania's broader civic space had experienced a steady, decade-long contraction driven by restrictive legislative frameworks. These laws were ostensibly passed to manage online safety and national security but have increasingly been used to police and suppress independent public discourse.

to police and suppress independent public discourse.

The primary legal instruments used to control the internet landscape include:

a) The Cybercrimes Act [CAP 443 R.E 2023]: This statute introduces vague, highly punitive criminal definitions for offences such as 'publication of false information' or 'misleading data.' Because the text lacks objective legal parameters, it grants law enforcement wide authority to detain, interrogate, and intimidate citizens who voice online dissent or share independent statistics regarding public affairs.

b) The Electronic and Postal Communications (Online Content) Regulations (GN No. 158i published on 30/6/2026): These regulations impose expensive mandatory registration fees, licensing conditions, and strict compliance duties on digital creators, bloggers, online podcasters, and forum administrators. Non-compliance results in immediate site takedowns and criminal liability, forcing widespread self-censorship.

As detailed by the joint report of CIPESA, Jamii Africa and PALU in its analytical submissions during Tanzania's Universal Periodic Review (UPR-2026), this legislative environment creates a severe structural imbalance. The state allocates vast resources to technical tracking, user surveillance, and platform blocking, yet fails to establish enforceable legal definitions or safety resources to counter Technology-Facilitated Gender-Based Violence (TFGBV). As a result, women operate in a high-risk digital landscape where they are vulnerable to unpoliced online extortion, stalking, and harassment, while remaining exposed to sudden state actions that can sever their connection to the global economy entirely.

4. Timeline and Chronology of the Shutdown

The digital blockade of October 2025 was not an isolated incident, but rather the climax of a long-term strategy of information control deployed by the state throughout the electoral cycle. The progression of this timeline outlines the systematic isolation of the country:

- May 21, 2025 (Long-Term Platform Suspension): Five months prior to the election, the government issues an indefinite restriction on X (formerly Twitter). Because X serves as the primary platform for civil society mobilization, real-time human rights alerts, and political debate, its suspension intentionally crippled independent tracking and decentralized organizing early in the election cycle.
- October 28, 2025 (Strategic Throttling Phase): On the eve of the general election, major mobile network operators begin aggressive bandwidth throttling across major population hubs, intentionally degrading the transmission of media assets (images, audio notes, video feeds) to block the rapid spread of opposition rallies.
- October 29, 2025 (The General Blackout - 05:00 EAT): As polling centers open across the country, a complete, nationwide blackout is initiated. All major mobile and fixed internet service providers (including Vodacom, Airtel, Tigo, Halotel, and TTCL) drop connectivity. Universal messaging platforms—WhatsApp, Instagram, Telegram, and Facebook—become completely unreachable.
- October 30 – November 2, 2025 (Total Digital Isolation): For 126 continuous hours, the country remains in a complete digital blackout. This critical phase directly overlaps with the counting of ballots, localized protests, and subsequent state crackdowns in urban centers like Mwanza, Arusha, and Zanzibar, hiding human rights conditions from international eyes.
- November 3, 2025 (Gradual, Monitored Restoration): Basic data connections are slowly restored, though major social communication tools remain blocked at the core ISP gateways, forcing citizens to rely on commercial Virtual Private Networks (VPNs) to communicate.

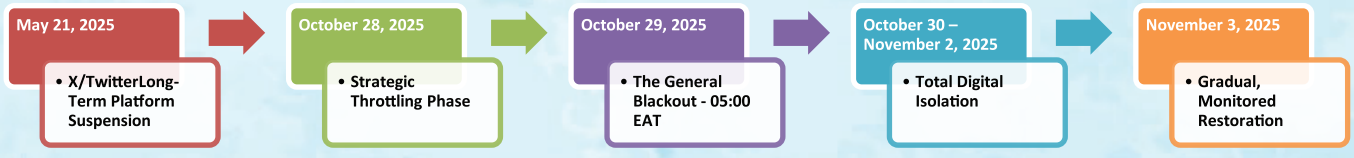


Figure 2: Internet Blackout Chronology towards and after October 29th in Tanzania

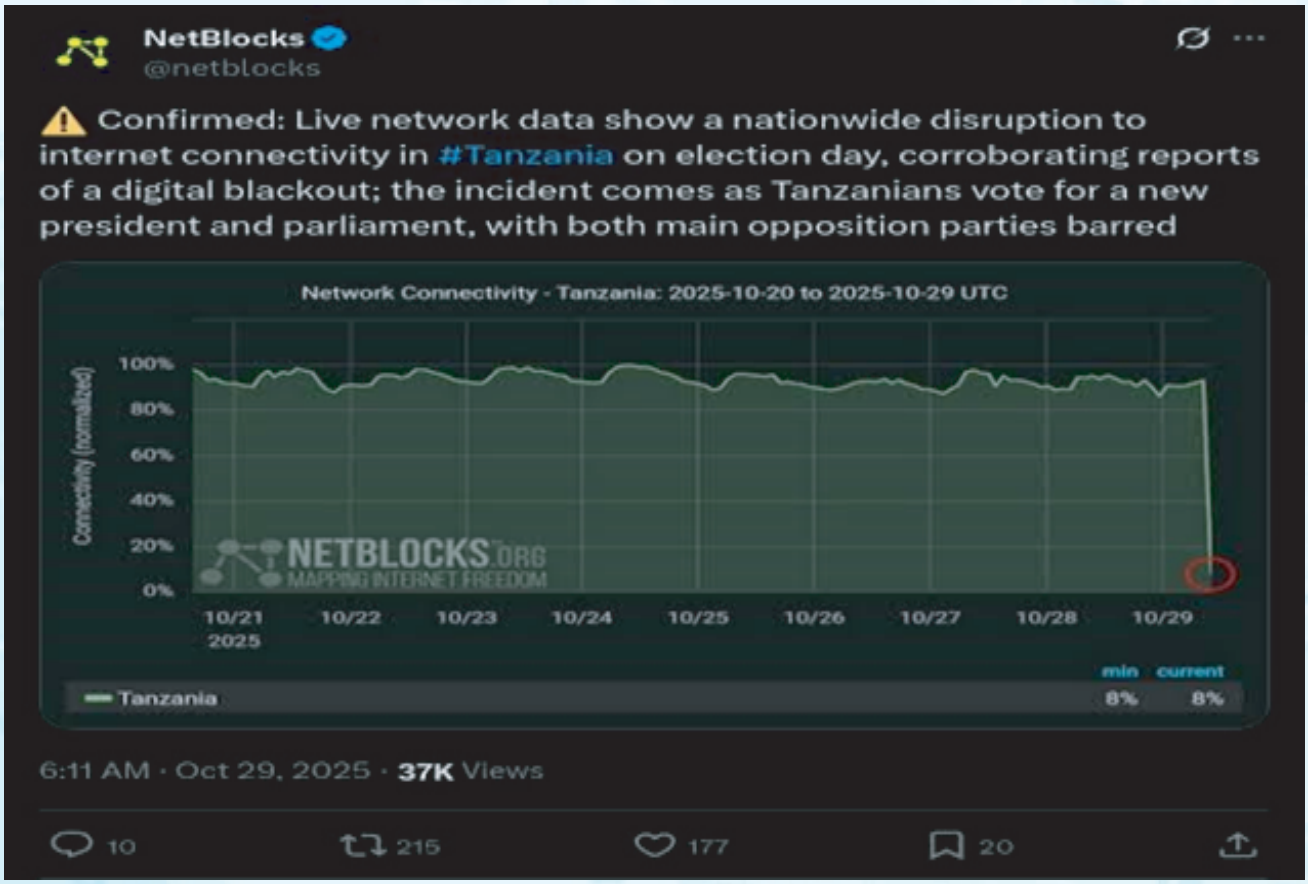


Figure 3: NetBlocks-an internet measuring and advocacy organization reporting on the Incident in Tanzania

5. Technical Evidence and Quantitative Economic Damage

Network logs compiled by NetBlocks prove that the disruption was a deliberate, top-down intervention executed at the border gateway and Internet Service Provider (ISP) levels, completely invalidating any claims of random physical infrastructure breakdown. The blocking utilized Server Name Indication (SNI) filtering combined with localized DNS spoofing to ensure that even when basic IP layers appeared active, data transmission to communication platforms was blocked.

Using the NetBlocks Cost of Shutdown Tool (COST) framework—which estimates macroeconomic impact by integrating indicators from the World Bank, the International Telecommunication Union (ITU), and Eurostat—the financial damage was profound. The 126-hour total shutdown resulted in a direct domestic loss of $72,333,826 USD. When combined with the economic damage caused by the structural ban on X since May 2025 ($165,817,059 USD), the total cost to the Tanzanian economy exceeded $238 million USD.

Metric / Target Group	Disruption Type	Primary Technical Method	Impact Severity
Social Media and Messaging	Total Protocol Block	SNI Filtering and DNS Spoofing	Complete failure of peer-to-peer data lines
Mobile Data Infrastructure	Severe Bandwidth Throttling	Gateway packet drop and capping	Inability to upload/download media
Commercial VPN Platforms	IP and Endpoint Blocking	Server IP address blacklisting	Delayed and degraded circumvention lines

This economic devastation hit the informal, female-led business sectors hardest. Unlike formal corporations with corporate lease lines, female entrepreneurs rely completely on open mobile networks and accessible digital wallets to survive.



Figure 4: One of the News coverages on the Loss incurred by Tanzania due to Internet Shutdown



Figure 5: the Citizen Newspapers captured the Government's view and commitment to future internet shutdowns

6. Human Rights Framework and International Standards

The execution of the 2025 internet shutdown stands as a direct breach of the United Republic of Tanzania's domestic constitutional promises and its international treaty commitments:

- **The African Charter on Human and Peoples' Rights (ACHPR):** Principle 38 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa explicitly prohibits state parties from disrupting access to the internet, particularly during sensitive national processes like elections. The African Commission has noted that arbitrary shutdowns violate the fundamental right to civic participation.

- **The International Covenant on Civil and Political Rights (ICCPR):** Under Article 19, any restriction on expression must pass strict international legal tests: it must be explicitly provided by clear law, must pursue a legitimate public interest, and must be strictly necessary and proportional. The 2025 blackout completely failed these tests, operating as an absolute form of collective punishment that harmed innocent citizens.

- **The Constitution of Tanzania (1977):** Article 18 explicitly states that every citizen has the right to look for, receive, and share information without interference. By cutting off access to the web, the executive branch implemented an unconstitutional barrier that restricted the public's ability to engage with the state or access essential news.

- However, in the constitutional petition challenging the government internet shutdown actions, the High Court of Tanzania ruled in favor of the government actions that, there must be a balance between individual liberty with social control during periods of unrest. The Court accepted the State's argument that the shutdown was justified due to violence and unrest allegedly disseminated through digital platforms. The Court ultimately held that the shutdown was constitutionally justifiable under Article 30(2) of the Constitution (Refer; Elvis John Makumbo v Minister for Communications and Information Technology & Others, Constitutional Case No. 4831 of 2026).

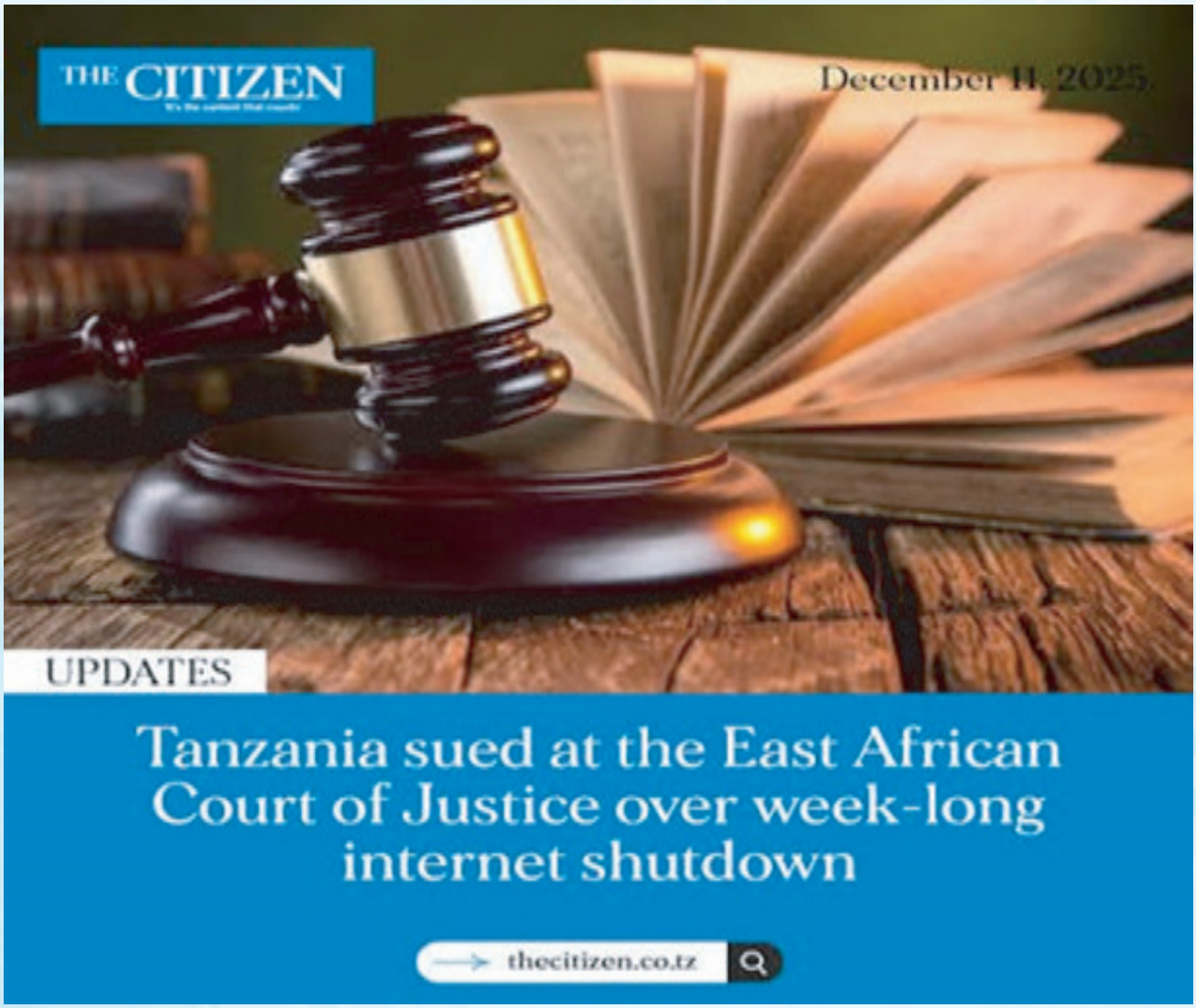


Figure 6:Internet Rights Advocacy bodies' reactions on the occurred internet shutdown

7. Women Human Rights Defenders (WHRDs)

This section demonstrates how the digital cutoff directly targeted specific groups of women. The intersection of gender, social standing, and technical reliance meant that the 126-hour blackout amplified existing vulnerabilities across the country.

- **Collapse of Rapid Response Operations:** For WHRDs operating across highly volatile urban centers, the internet is an essential tool for physical safety. The sudden cutoff of secure, encrypted apps like Signal and WhatsApp completely fractured emergency protection networks, leaving activists unable to flag imminent safety threats or request legal help.
- **Unmonitored State Crackdowns:** As post-election protests met with security forces, the digital blackout prevented the documentation of human rights abuses against female organizers. Without access to live streaming or cloud storage, abuses remained hidden, shielding state actors from accountability.
- **Psychological Exploitation and Isolation:** Cut off from regional networks and unsure if their colleagues had been detained, WHRDs faced intense psychological stress and isolation, forcing many into hiding.

8. Women Journalists and Media Workers

This section exposes how the digital cutoff weaponized connectivity gaps against targeted groups of women. Operating at the intersection of gender, social standing, and technical reliance, the 126-hour blackout severely amplified pre-existing marginalization nationwide.

- **Inability to Transmit Field Reports:** Female field journalists found it impossible to transfer video logs, audio files, or text updates to central newsrooms, effectively erasing women's perspectives from the national election narrative.
- **Information Ecosystem Breakdown:** Deprived of real-time internet verification tools, women reporters were exposed to state accusations of spreading 'fake news' if they relied on word-of-mouth reports, making investigative journalism highly dangerous.
- **Physical Vulnerability:** Without access to live-location sharing or instant security check-ins with their newsrooms, female field reporters faced heightened physical vulnerabilities during street protests and localized unrest.

9. Women Entrepreneurs and Informal Micro-Traders

This section exposes how the digital blackout disproportionately weaponized access against women entrepreneurs and informal micro-traders, plunging this sector into acute economic vulnerability and causing devastating financial losses as hereunder demonstrated.

- **Destruction of Micro-e-Commerce Platforms:** Thousands of women who sell clothing, food, and handmade goods through WhatsApp groups and Instagram saw their businesses vanish overnight.
- **Paralysis of Mobile Money Systems:** As highlighted by CIPESA, the wider digital halt disrupted mobile commerce and informal payment platforms. Women were unable to complete basic M-Pesa or Airtel Money transfers to buy stock or receive payments, forcing micro-businesses into a standstill.
- **Perishable Product Losses:** Small-scale women vendors dealing in fresh produce or fish could not coordinate delivery routes, leading to spoiled inventory and the loss of their primary capital.

10. Political Participation and Electoral Equity

This section exposes how the digital blockade directly disenfranchised women during the 2025 general election, driving severe electoral gender inequity and silencing female voices in the democratic process.

- **Destruction of Micro-e-Commerce Platforms:** Thousands of women who sell clothing, food, and handmade goods through WhatsApp groups and Instagram saw their businesses vanish overnight.
- **Paralysis of Mobile Money Systems:** As highlighted by CIPESA, the wider digital halt disrupted mobile commerce and informal payment platforms. Women were unable to complete basic M-Pesa or Airtel Money transfers to buy stock or receive payments, forcing micro-businesses into a standstill.
- **Perishable Product Losses:** Small-scale women vendors dealing in fresh produce or fish could not coordinate delivery routes, leading to spoiled inventory and the loss of their primary capital.

11. Gender-Based Violence and Crisis Response

This section exposes how the digital cutoff directly and indirectly exacerbated Gender-Based Violence (GBV) and crippled lifesaving GBV crisis response networks nationwide.

- Disabled Crisis Helplines: Local GBV hotlines and digital case management services that rely on cloud-connected routing went down completely, preventing women from reaching out for medical or legal help.
- Interrupted Protection Logistical Networks: Human rights groups could not coordinate emergency transport to relocate victims of violence away from abusive households during curfew hours.
- Trapped in Isolation: Deprived of data networks, women facing domestic abuse could not send quick alerts to neighbors or relatives, isolating them alongside their abusers in a closed information loop.

12. Rural Women and Smallholder Farmers

This section exposes how the digital cutoff weaponized connectivity gaps against rural women and smallholder farmers. The intersection of gender, marginalized social standing, and agricultural digital reliance meant that the 126-hour blackout severely amplified pre-existing economic and geographic vulnerabilities nationwide.

- Complete News Deprivation: For many rural women, basic mobile web access is their sole window into national events. The blackout left them dependent on unverified rumors, inducing panic during post-election unrest.
- Agricultural Market Exploitation: Female farmers in regions like Kilimanjaro or coastal Zanzibar were unable to verify current market values for their produce, forcing them to sell to predatory middlemen at a loss.
- Interruption of Essential Remittances: Family members working in urban centers could not send mobile financial transfers back home, leaving rural matriarchs without funds for food or healthcare emergencies.

13. Women with Disabilities and Accessibility Barriers

This section exposes how the digital cutoff weaponized lack of connectivity against women with disabilities, cutting off vital lifelines. The intersection of gender, marginalized social standing, and reliance on digital accessibility tools meant that the blackout severely amplified pre-existing exclusion and vulnerability nationwide.

- Failure of Assistive Technologies: Visually impaired women using screen-reading software linked to online processing tools found their systems suddenly inoperable, leaving them digitally isolated.
- Total Disconnection for the Deaf: Deaf women rely almost exclusively on internet-based video calls for sign language communication. The blocking of these platforms cut them off from emergency updates and peer support networks.
- Disrupted Medical Supply Chains: Women with physical dependencies who use basic digital platforms to manage or request medication deliveries saw their support systems fail due to widespread logistical disruptions.

14. International and Regional Responses

The unannounced execution of the 2025 digital blackout drew immediate and strong condemnation from international human rights watchdogs and regional bodies. The African Commission on Human and Peoples' Rights (ACHPR) issued an official statement emphasizing that access to information is an essential part of democratic legitimacy, and urged the Tanzanian state to restore all communications networks without delay.

Concurrently, United Nations Special Rapporteurs focused on freedom of expression warned that deliberate internet blocks during election cycles often serve to obscure state-sponsored violence and electoral fraud. Global digital rights coalitions, led by Access Now, CIPESA, and the #KeepItOn network, launched joint campaigns to hold the Tanzanian government accountable, demanding the removal of the ban on X and the establishment of legal protections for users.

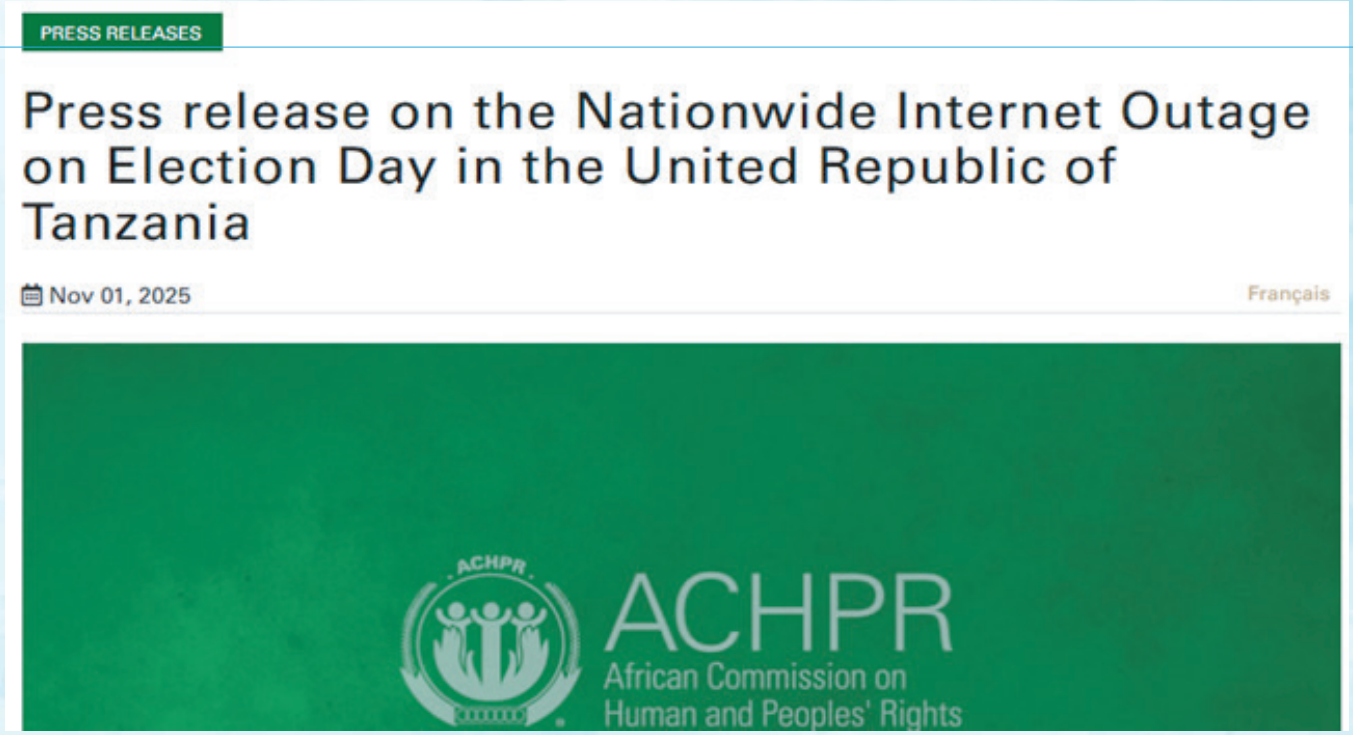


Figure 7: the African Commission on Peoples and Human Rights coverage about Tanzania Election and internet Shutdown

15. Comparative African Lessons and Legal Precedents

Tanzania's 2025 digital blackout reflects a broader, worrying trend of technological control across Africa. However, successful responses from civil society across the continent offer valuable lessons for the future:

- Uganda and Strategic Litigation: Past blackouts in Uganda show that constitutional challenges filed in regional courts, like the East African Court of Justice (EACJ), can create international legal precedents that make arbitrary state censorship politically costly.
- Kenya and Decentralized Infrastructure: To counter potential network shutdowns, Kenyan digital rights organizations have initiated community mesh networks and offline documentation applications, ensuring that human rights monitoring continues even without commercial internet access.
- Nigeria and Civic Preparedness: The public resistance to platform blocks in Nigeria demonstrates that training community groups in VPN configurations and encrypted storage systems prior to elections mitigates the impact of sudden state censorship.

16. Detailed Policy Recommendations

To protect the digital landscape and ensure that internet communication is never weaponized as a tool of gendered oppression again, Zaina Foundation presents the following policy recommendations:

To the Government of Tanzania and TCRA

- Legislate an Anti-Shutdown Guarantee: Enact explicit statutory bans preventing total or partial internet shutdowns, platform blocking, and bandwidth throttling during national elections.
- Repeal and Amend Restrictive Statutes: Reform the Cybercrimes Act and the Online Content Regulations to align with international human rights benchmarks, focusing on protecting user expression rather than expanding state control.

To the Judiciary

- Enforce Prior Judicial Review: Mandate that any emergency restriction on public telecommunications networks requires explicit, public authorization from the High Court, removing arbitrary executive power.

To Civil Society Organizations and International Donors

- Fund Digital Security tailored for Women: Allocate resources to train WHRDs, female politicians, and women journalists in advanced digital security, circumvention tools, and secure communication.
- Invest in Decentralized Connectivity: Support the deployment of community-governed internet infrastructure and offline tools to protect marginalized groups, particularly rural women and women with disabilities, during national crises.

17. Conclusion

- The October 2025 internet shutdown in Tanzania demonstrates how state-directed digital blockades compound gender inequality. By disconnecting the nation, the state compromised women's safety, interrupted their economic livelihoods, and excluded their voices from public discourse. Protecting these rights requires an active commitment from state actors, legal bodies, and civil society. Zaina Foundation calls on all stakeholders to implement these recommendations immediately, ensuring that the digital platforms driving women's empowerment across Tanzania are never silenced again.

References:

- African Commission on Human and Peoples' Rights (ACHPR). (2019). Declaration of Principles on Freedom of Expression and Access to Information in Africa.
CIPESA. (2025). 'Tanzania's Internet Disruption Undermines Electoral Integrity and Imperils Livelihoods.' Policy Briefing Series.

  Elvis John Makumbo v Minister for Communications and Information Technology & Others, Constitutional Case No. 4831 of 2026)

  NetBlocks. (2025). 'Internet disrupted in Tanzania on eve of presidential elections.' Technical Telemetry Log Report.

  OONI. (2025). 'Tanzania: Social media platforms and VPN endpoints blocked during general election.' Open Observatory of Network Interference.

  The African Charter on Human and Peoples' Rights (ACHPR), 1981:
The International Covenant on Civil and Political Rights (ICCPR), 1966:

  United Republic of Tanzania. (1977). Constitution of the United Republic of Tanzania, Article 18. Government Printer.

  Zaina Foundation. (2026). 'The Shrinking Digital Space for Tanzanian Women: An Evaluation of TFGBV and Policy Hurdles.' Internal Research Archive.

Websites:
https://datareportal.com
https://ippmedia.co.tz
https://dailynews.co.tz
https://www.gsma.com
https://www.forbesafrica.com
https://www.fsdt.or.tz
https://academic.oup.com

ZAINA
FOUNDATION

Address

P.O.Box 75757, Dar es Salaam
Hotline: +255 676 586 199

Web

info@zainafoundationtz.org
www.zainafoundationtz.org

Social Media

facebook.com/Zaina Foundation
x.com/@Zainafoundation