

## INTELLIGENCE REPORT — TANZANIA (OPEN SOURCE)

Compiled and analyzed using open-source public data. Author: JediSec.



## Executive Summary

Date of report: November 01, 2025.

Overview: Following the national general election on October 29, 2025, Tanzania experienced large-scale civil unrest in major urban centers, reports of forceful crackdowns, and simultaneous constraints on internet connectivity. Combined with earlier 2025 public health events (Marburg virus reports) and rising digital adoption, the operational landscape reveals multiple vectors for information operations, opportunistic cyber fraud, and critical-service disruption. This report compiles public indicators, threat assessment, technical reconnaissance playbooks, and recommended monitoring setups for OSINT and defensive red team activities.

# Contents

1. Executive Summary
2. Key Events & Timeline
3. Digital Infrastructure Snapshot & Charts
4. Telecommunications & Critical Infrastructure Analysis
5. OSINT Findings (Actionable)
6. Threat Assessment & Prioritization
7. Step-by-step OSINT/Red Team Playbook
8. Detection & Monitoring Templates (Safe examples)
9. Operational Recommendations
10. Appendix: Sources & Image URLs

## Key Events & Timeline

- March 2025 — Marburg virus cases reported in Tanzania; WHO involvement and local responses noted.
- October 29, 2025 — National general election held.
- October 29–31, 2025 — Reports of mass protests in Dar es Salaam and other cities; government measures including curfews and reported internet restrictions; international media coverage and access concerns noted.
- Ongoing — Post-event recovery with intermittent service restorations and active information campaigns on social platforms.

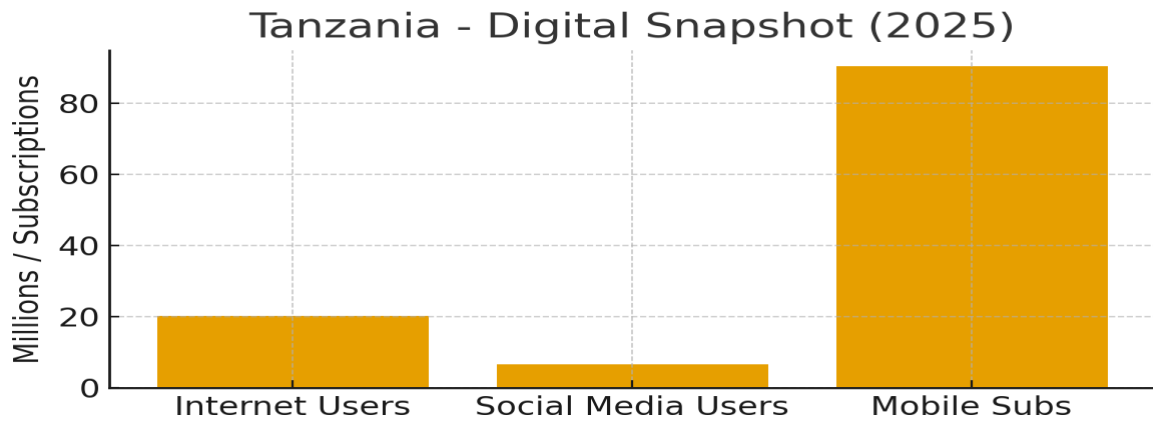
## Digital Infrastructure Snapshot

Key indicators (early 2025 estimates):

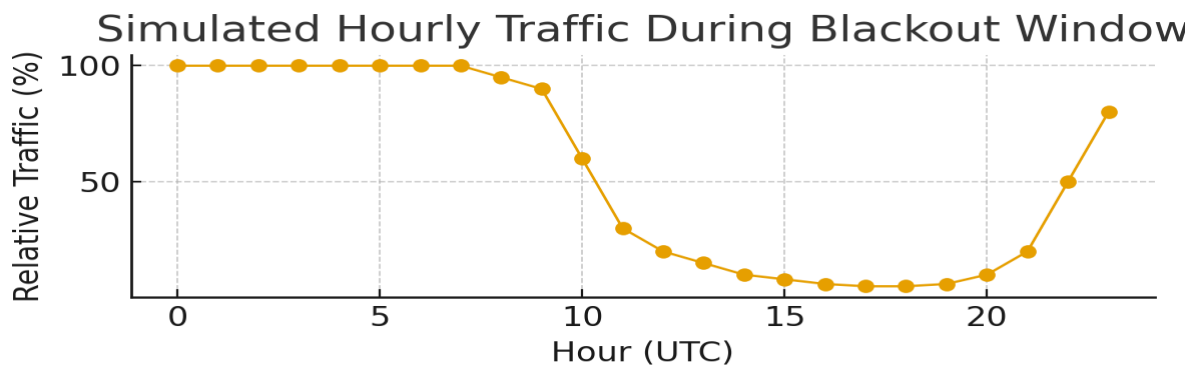
- Internet users: ~20.2 million (~29.1% penetration).
- Social media users: ~6.75 million.
- Mobile subscriptions: ~90.4 million (multi-SIM behavior common).

Implications: relatively low internet penetration means public online chatter can concentrate and spike; however, telecom chokepoints allow authorities to exert rapid control via throttling, DNS filtering, and full or partial blackouts.

## Digital Snapshot Chart



Simulated traffic curve for a blackout event (illustrative)



## Telecommunications & Critical Infrastructure

Primary operators: Vodacom, Airtel, and local carriers (market consolidation trends noted). Mobile networks represent the primary consumer internet access channel; fixed broadband has very limited reach. Key resilience concerns include centralized network core elements, regulatory control points, and the reliance of critical services (mobile money, emergency services) on cellular infrastructure. Satellite services (e.g., proposed Starlink deployments) remain politically sensitive and subject to licensing controls.

## OSINT Findings (Actionable Signals)

1. Connectivity disruption indicators: BGP withdrawal events, sudden routing changes, and sharp traffic drops to .tz domains — useful signals for automated alerting.
2. Narrative channels: local-language (Swahili) hashtags, Facebook public groups, and closed messaging apps (WhatsApp) are primary vectors for on-ground coordination and rumour propagation. Monitor public accounts, media pages, and verified NGO channels.
3. Exposed infrastructure surface: government subdomains (.go.tz), tourism booking portals, and mobile-money integration endpoints present likely discovery targets for misconfiguration (subdomain takeover, exposed S3/backups) during chaotic recovery windows.
4. Health sector risk vectors: health facility public pages, donation portals, and patient lists that may be exposed or used for scams during crisis recovery.

## Threat Assessment & Prioritization

High priority threats (24–72 hours):

- Information operations and disinformation campaigns using rapid viral posts and fake accounts.
- Service disruption to mobile money and emergency communications, enabling fraud or hampering relief.
- Opportunistic phishing and donation scams targeting donors and affected populations.

Medium priority threats (3–14 days):

- Data exposure during server restores and careless backup reattachments.

- Targeted social engineering against public servants and NGO volunteers.

Low priority but notable:

- Physical targeting of critical infrastructure personnel; supply chain constraints for telecom repairs.

## Step-by-step OSINT & Red Team Playbook (Tactical)

Phase 1 — Rapid Recon (0–6 hours):

- BGP & Routing: Set up alerts via RIPEstat/BGPStream for ASN and prefix changes affecting Tanzania ASNs. Log timestamps and correlate with news reports.
- Domain Availability: Automated HEAD/GET checks for top-level .tz domains and critical .go.tz services; detect HTTP status changes and TLS cert alterations.
- Social Listening: Start keyword-based scraping (Swahili stems, local place names) from X/Twitter, Facebook public pages, and YouTube. Prioritize accounts with geotagged content.

Phase 2 — Evidence Collection & Validation (6–24 hours):

- Image Verification: Extract EXIF when available, perform reverse image search, and use shadow matching to find original uploads. Preserve originals and compute SHA256 hashes.
- Timeline Construction: Normalize timestamps to UTC, create an evidence timeline, and bucket items by verified/unverified.
- Public Service Monitoring: Track API/endpoint behavior of payment services and government portals for anomalies.

Phase 3 — Surface Assessment & Safe Testing (24–72 hours):

- Asset Inventory: enumerate subdomains, exposed S3 buckets, open administrative interfaces, and stale DNS records.
- Safe Checks: use non-intrusive probes (HEAD requests, banner grabs) to detect exposures; DO NOT perform credentialed attacks or exploit vulnerabilities without explicit legal engagement.

Phase 4 — Reporting & Remediation Support (72+ hours):

- Collate verifiable evidence, produce a chain-of-custody log with hashes and screenshots, and submit findings to responsible disclosure channels (or coordinate with NGOs for humanitarian leaks).

## Detection & Monitoring Templates (Examples)

Below are safe, defensive-focused examples you can adapt to monitoring toolchains. These are NOT exploit payloads — they are detection signatures and probes to find misconfiguration. A) Example Nuclei-style detection (conceptual) — detect public S3/backup misconfigurations (non-exploitative):

---begin---

id: tanzania-exposed-backup

info:

name: Exposed Backup - Common S3/Backup Patterns

author: JediSec

severity: medium

requests:

- method: GET

path:

- "{{BaseURL}}/backup.zip"

- "{{BaseURL}}/backup.tar.gz"

matchers:

- type: word

words:

- "PK" # zip file header indicator

- "tar"

---end---

(Adapt path patterns to likely backup filenames; run as passive detection only.)

B) Simple regex patterns for Swahili keyword monitoring (example):

- /protest|protes|mapinduzi|curfew|gereza/iu
- Use Unicode-insensitive matching and common misspellings; combine with geolocation heuristics.

## Operational Recommendations

- 1) Implement automated BGP and domain monitoring with webhook alerts into Slack/Mattermost for triage.
- 2) Maintain an evidence repository: store raw content, computed hashes, and contextual metadata; use offline

backups and immutable logs.

3) Prepare communication templates for responsible disclosure and public advisories; coordinate with NGOs and trusted media channels.

4) Harden recovery windows: advise service owners (gov & fintech) to rotate credentials, verify backups, and review S3/FTP permissions before full restore.

5) Legal & Ethical: ensure all intrusive tests have documented authorization; OSINT collection should avoid doxxing private individuals and respect local laws.

## Appendix: Public Sources & Image References

Sources include international media coverage (The Guardian, Al Jazeera, Reuters), WHO disease reports (Marburg), DataReportal digital stats, telecom market briefs, and NGO statements (AccessNow / KeepItOn). Image references and verification targets include: • Protest imagery from Reuters/Guardian/Al Jazeera image pages.

- WHO outbreak reports and official ministry statements (Tanzania MoH website).
- OpenStreetMap & Google Maps coordinates for key urban locations (Dar es Salaam main squares, police stations, hospitals).

Note: external image URLs are listed for verification and are not embedded in this document due to environment constraints. When integrating into operational briefs, capture screenshots, compute hashes, and store with metadata.

Prepared by: JediSec — Open Source Intelligence Unit. Public-source analysis only. This document is for defensive, monitoring, and research purposes. Do not use for unlawful activities.

Generated on: 2025-11-01 23:12 UTC