SUB-SAHARAN AFRICA INTERNET FREEDOM LANDSCAPE

ARTHUR GWAGWA

JUNE 4, 2018

Presentation to the

Bureau of Democracy, Human Rights, United States Department of State

ACKNOWLEDGEMENTS

FUNDED BY THE OPEN TECHNOLOGY FUND
https://www.opentech.fund/page/open-technology-fund

Projects and Reports.

- https://www.opentech.fund/project/sub-saharan-africa-cyber-threat-modeling
- https://www.opentech.fund/article/angola-emerging-battleground-digital-rights
- https://www.opentech.fund/article/new-report-investigates-internet-censorship-during-rwandas-2017-presidential-election
- https://www.opentech.fund/article/new-report-analyzes-internet-censorship-during-lesothos-2017-general-elections

Agenda

- **Internet Governance Environment**
- **Regional Forums, standard-setting/norm sharing**
- **Domestic Information Controls**
- **Deliberate Network Interference (OONI/Shutdowns)**
- **Network Landscape**
- **Legal and Regulatory Frameworks**

Mapping the Internet Governance Environment

- States preference of multilateralism versus multistakeholder (ism).
- Lack of clarity in government department, public and private sector roles
- Side-lining of civil society, weakened leverage
- Government preference of political economy and other lesser security issues

Regional Forums, standard-setting/norm sharing

- Coordinate policies and practices, and are vehicles through which repressive countries learn from each other
- Details about what goes on in ‘security’ forums is difficult to discern from outside
- Policing, militarisation and securitisation of the internet.
- Practices reflected at National levels

Domestic Information Controls

- Technically aided by the increasing cyber espionage and the market for surveillance
- Legally aided by the proliferating cybercrime laws
- Politically-motivated information security threats
- CSOs, unlike corporate entities, have little or no capacity to deal with the problem
- These capabilities are proving particularly attractive to many regimes that face on-going insurgencies & popular protests.

Domestic Information Controls

- “Surveillance-by-design” infrastructure development projects
- Political intent –v- human rights & security in app design, data centre, IXP & network protocols.
- Opportunities and risks of digital economies for Africa
- Log but don’t block: Surveillance & computational propaganda
- Application of non-technical measures
- “Downloading” policing of the Internet to the private sector

Deliberate Network Interferences

- Blocking and Filtering of Content
- The work of the Open Network Observatory for Network Interference (OONI)
- What OONI measurements tell us about network interference
- Internet shutdowns: Causes, motivations, impact, campaigns

Mapping Network Landscape

- Institutional and policy mapping (government, IXPs, ISPs/telcos, GAFAM, SMEs, policy, entrepreneurs)
- Political economy of African national cybersecurity policies (including funding, tech flows)
- Monopoly, convergence and downloading

The Legal and Regulatory Frameworks

- Growing national security awareness and other cyber risks
- Cybersecurity capacity is generally limited in Africa
- Implementation is a significant challenge with governments and law enforcement
- Fear to engage academics and technologists

Specific laws of concern

- Anti-terrorism laws: Ethiopia, Kenya
- Criminalisation of hate speech, slander, defamation and other forms of critical speech
- Penalising/imposing fees for social media use
- Cyber security legislation

Sub-Saharan Africa Threat Modelling Current project

- Who do you think I should talk to?
- What information do you think I should get?
- What support can I get from the USG towards my research, e.g, in-country contacts?
- What do the USG and other stakeholders need?