Cybersecurity and Civil Liberties: The Hard Tension

AiCE Africanism & Pan-African Studies — When security becomes repression

When Security Becomes Repression

The most difficult dimension of cybersecurity for African democracies is the tension between security and freedom. Effective cybersecurity requires surveillance capabilities — the ability to monitor network traffic for threats, to intercept criminal communications, to identify attackers and track their activities. These capabilities, if controlled by accountable democratic governments and governed by robust legal frameworks, can protect citizens from genuine threats. If controlled by unaccountable governments or used without adequate legal oversight, the same capabilities become instruments of political repression.

Africa's history of governance failure, examined in an earlier unit, gives particular urgency to this tension. A government that uses COVID-19 contact tracing apps to track political opponents is not providing public health protection — it is using public health infrastructure for political surveillance. A government that blocks social media platforms during elections is not protecting cybersecurity — it is suppressing political speech. A government that uses cybercrime laws to prosecute journalists for publishing leaked documents is not fighting crime — it is criminalising journalism.

These are not hypothetical scenarios. Internet shutdowns — the deliberate disabling of internet access by governments, typically during elections or protests — have become a recurring feature of African political life. Ethiopia, Sudan, Cameroon, Chad, Guinea, Zimbabwe, and many other countries have implemented internet shutdowns in recent years, typically at moments of political crisis. These shutdowns are justified by governments as security measures. They are understood by their targets — citizens trying to organise, journalists trying to report, businesses trying to operate — as political attacks dressed in security language.

Internet Shutdowns in Africa: Key Facts
Scale: Africa accounts for the largest number of internet shutdowns of any global region.

Internet Shutdowns in Africa: Key Facts
Common triggers: elections, protests, security operations, and exam periods (to prevent cheating).
Economic cost: the African Union estimates internet shutdowns cost African economies approximately $2 billion per year.
Human rights cost: shutdowns prevent citizens from accessing emergency services, organising for safety, and exercising free expression.
Legal basis: most shutdowns are ordered by executive authority without judicial oversight, violating due process requirements.
#KeepItOn coalition: a global campaign with strong African civil society participation, documenting and opposing internet shutdowns.
Sudan 2019: a 68-day shutdown imposed by the military following the civilian uprising that overthrew al-Bashir — one of the longest in history.
Cameroon 2017: a shutdown in Anglophone regions lasting over 90 days, directly exacerbating the Anglophone crisis.

Cybercrime Laws as Instruments of Repression

Many African countries have enacted cybercrime laws that, while ostensibly designed to combat criminal hacking, fraud, and harassment, contain provisions so broad that they can be — and have been — used to prosecute journalists, bloggers, and social media users for publishing political content that governments dislike. The criminalisation of 'spreading false information online,' 'cyberstalking' of public officials, and 'content likely to cause public panic' under vague and broadly worded provisions has become a mechanism for prosecuting legitimate political speech.

In Nigeria, the Cybercrimes Act has been used to arrest social media users for posts critical of government officials. In Tanzania, the Electronic and Postal Communications Act imposed severe restrictions on online content that effectively prohibited political criticism. In Egypt, dozens of journalists and bloggers have been prosecuted under cybercrime provisions for their reporting. These laws weaponise cybersecurity language against democratic participation.

The appropriate response is not to abandon cybercrime legislation — genuine cybercrime causes real harm and must be addressed legally. The appropriate response is to require that cybercrime laws meet international human rights standards: clear and precise definitions of prohibited conduct; proportionate penalties; judicial oversight of prosecutions; specific protections for journalism and political speech; and independent review mechanisms to prevent abuse. African civil society organisations working on digital rights — including Paradigm Initiative, the Collaboration on International ICT Policy for East and Southern Africa (CIPESA), and the African Declaration on Internet Rights and Freedoms — are doing critical work in this space.

Key Takeaways

Internet shutdowns and overly broad cybercrime laws are the two clearest ways cybersecurity language has been used to justify political repression across Africa — costing an estimated $2 billion annually while denying citizens emergency services, safe organising, and free expression. The solution is not abandoning cybersecurity law but designing it to international human rights standards, with judicial oversight and specific protections for journalism. The next lesson examines what it takes to build the capacity to do cybersecurity right in the first place.