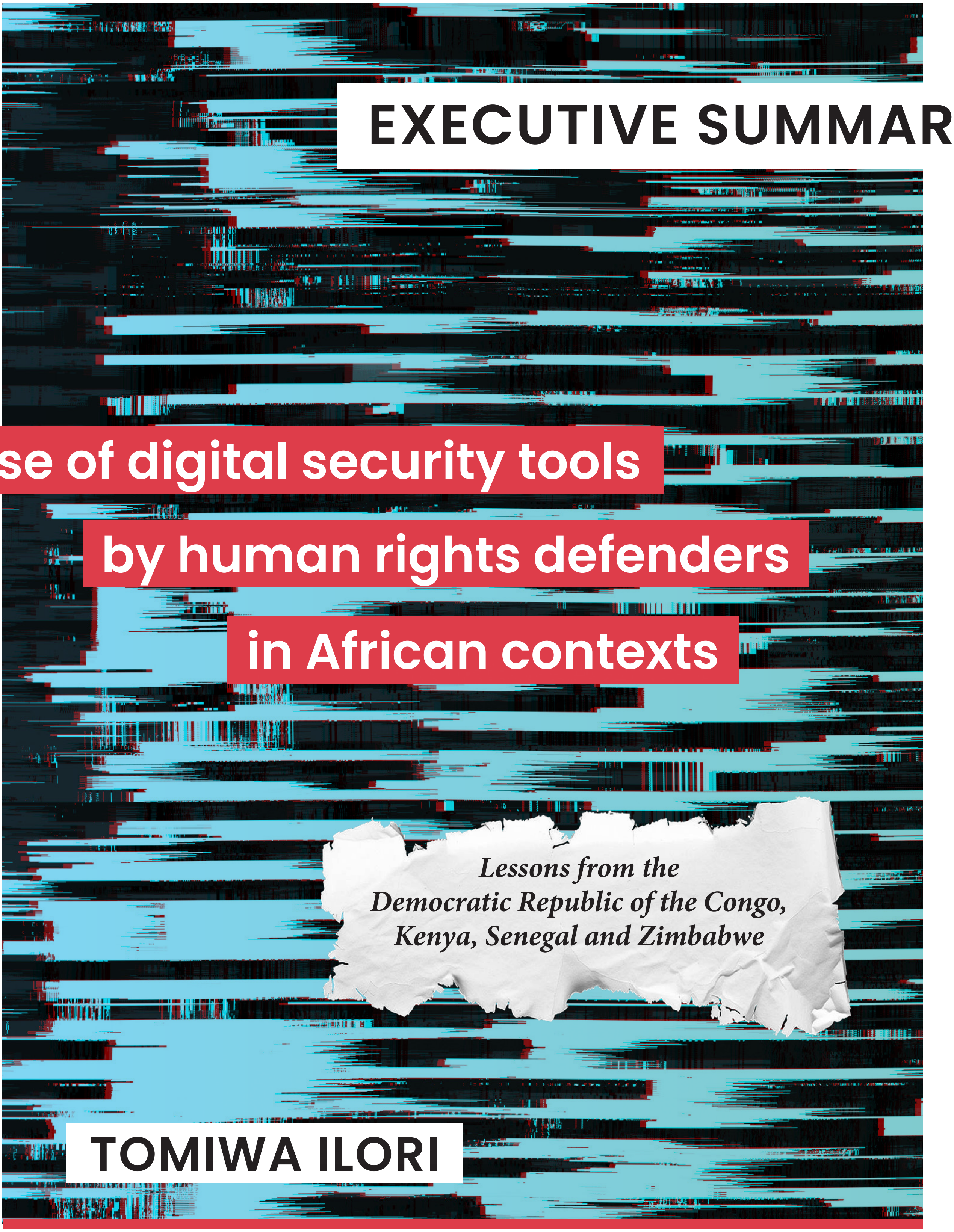


EXECUTIVE SUMMARY

Use of digital security tools by human rights defenders in African contexts

Lessons from the Democratic Republic of the Congo, Kenya, Senegal and Zimbabwe

TOMIWA ILORI

*A report of a fellowship project
supported by Open Technology Fund and hosted by HURIDOCS*

OPEN TECHNOLOGY FUND

huridocs

Executive Summary

This report examines how human rights defenders (HRDs) in African contexts including the **Democratic Republic of the Congo**, **Kenya**, **Senegal**, and **Zimbabwe** use digital security tools to protect themselves in high-risk political and digital environments.

It uses existing literature, survey responses and interviews with HRDs and developers of digital security tools to highlight key challenges such as **pervasive state surveillance**, **limited access to digital infrastructure**, **low digital literacy**, and the **technical complexity** of existing digital security tools.

However, both HRDs and tools developers expressed strong interest in **collaboration**, **co-design**, and **digital security training** to improve usability. The report recommends a comprehensive approach to digital security which includes co-design, continuous training support, and reform to ensure HRDs are capacitated and protected in their work.

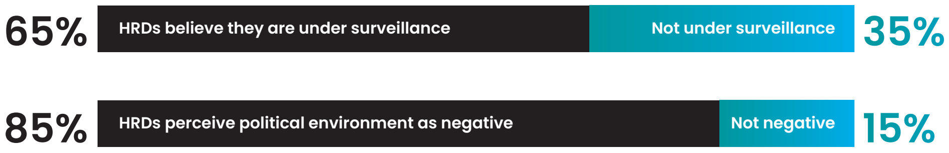
Tomiwa Ilori
July 2025

Key findings of the report

KEY FINDING 1

Pervasive state surveillance threatens HRDs' safety and work

The majority (65%) of HRDs across the countries studied believe they are under surveillance by state actors and 85% of HRDs believe that their political environment has a negative impact on their work. This surveillance is not only real but also perceived which creates a climate of fear that leads to self-censorship, psychological stress, and operational constraints. These threats are compounded by repressive laws and government practices that criminalise dissent and restrict internet freedoms, which severely impact HRDs' ability to advocate safely and effectively.



KEY FINDING 2

Limited access to digital infrastructure and resources hampers tool adoption

More than half of HRDs in these countries face significant digital and systemic infrastructural challenges such as unreliable internet, high data costs, outdated devices, and power outages.

These issues are pronounced in rural and conflict-affected areas where connectivity is poor or non-existent. Women human rights defenders (WHRDs) in these regions face additional gender-based forms of violence such as doxing, sexual harassment, and non-consensual sharing of intimate images. As a result, many HRDs rely on platforms like WhatsApp and Facebook due to their accessibility. The lack of affordable, secure, and locally adapted digital tools limits HRDs' ability to protect themselves and their work in high-risk political environments.

KEY FINDING 3

Digital security skills and usability gaps limit effective tool use

The report reveals that only 20% of HRDs possess advanced digital security skills, while 40% have basic and intermediate skills. This skills gap, combined with the technical complexity of many digital security tools leads to underutilisation of digital security tools. Some of these tools are often seen as too complicated without proper training and access to affordable and reliable internet. Peer adoption is also low which makes secure communication difficult. WHRDs in rural areas face compounded challenges due to limited access to training and digital literacy. These findings demonstrate the need for user-friendly, context-specific tools and continuous capacity-building efforts.

KEY FINDING 4

Tool developers are willing to engage but face challenges

Most (90%) digital security tool developers express strong interest in collaborating with HRDs even though most HRDs have never interacted with a developer. Developers mentioned that they face constraints such as limited funding and small teams, which hinder their ability to localise tools and respond to user feedback effectively. Language barriers and lack of structured engagement platforms further limit collaboration. In spite of these challenges, developers are committed to improving usability, expanding language support, and building tools that reflect the realities of HRDs in African contexts.

KEY FINDING 5

Strong demand for co-design, training, and inclusive digital security ecosystems

The digital security risks that HRDs face have become complex. This is why they articulated a clear need for regular and hands-on training programmes tailored to varying skill levels and local contexts. They emphasised the importance of tools that are affordable, offline-capable, and available in local languages. There is also a strong desire for co-design opportunities with developers to ensure tools are relevant and responsive. Both HRDs and developers support the creation of multi-stakeholder platforms for continuous collaboration.

These findings point to the need for a comprehensive and inclusive approach to digital security that goes beyond technology to include continuous training and support.