2026

DEFENDERS
PROTECTION INITIATIVE

THE ARCHITECTURE OF SURVEILLANCE

DIGITAL RIGHTS, CIVIC SPACE, AND UGANDA'S 2026 ELECTIONS.

DEFENDERS PROTECTION INITIATIVE (DPI)

Special Research Report • March 2026

DEFENDERS PROTECTION INITIATIVE

TABLE OF CONTENTS

ORGANIZATION OVERVIEW

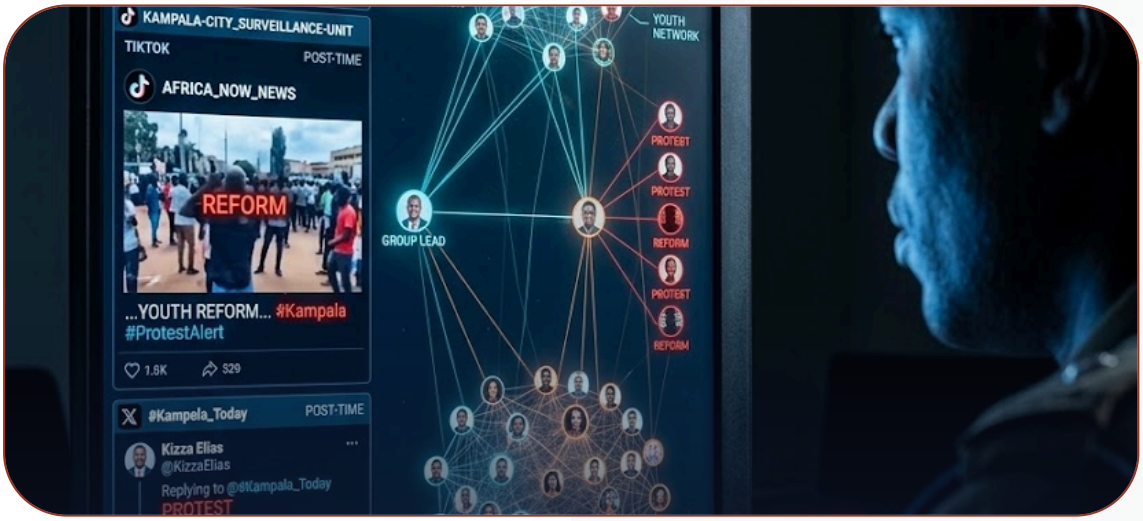
DEFENDERS PROTECTION INITIATIVE

OUR VISION

A safer working environment for humanity.

OUR MISSION

- Provide contextualized and tailored security options.
- Deliver innovative safety solutions to humanity.
- Strengthen human rights defenders' protection capacity.
- Integrate safety into core organizational workflows.



CORE APPROACH

Defenders Protection Initiative contributes to promoting and protecting human rights by strengthening defenders' capacity to integrate security and safety into their work through continuous learning and tailored training.

STATEMENT FROM A CIVIL SOCIETY REPRESENTATIVE

Across Uganda, civil society organizations continue to operate in an environment shaped by increasing digital risks, regulatory pressure, and direct security threats. From targeted cyber-attacks and data breaches to physical intimidation and surveillance, the space for civic engagement is becoming more constrained.

At the frontline, human rights defenders are not only advocating for accountability and justice—they are also managing complex security challenges that affect their daily work and personal safety. Many organizations have had to adapt quickly, investing in digital protection, risk assessments, and emergency response mechanisms just to sustain their operations.

Initiatives led by organizations such as Defenders Protection Initiative highlight the scale of this reality. Civil society actors now rely on structured security support systems, including rapid response interventions, digital security training, and coordinated protection networks, to respond to threats as they arise.

At the same time, evolving regulatory frameworks—particularly around financial compliance and anti-money laundering measures—have introduced additional operational pressure. While these frameworks aim to strengthen accountability, they also risk limiting the flexibility and independence of civil society work if not carefully balanced.

What emerges is a clear picture: civic space is not only shaped by policy, but by lived experience. Behind every report, there are organizations navigating uncertainty, protecting their teams, and continuing to serve communities under constraint.

This report reflects those realities. It brings forward the voices, risks, and resilience of civil society actors who continue to operate, adapt, and persist—despite the challenges.

INTRODUCTION & CONTEXT

THE HISTORICAL ORIGINS AND EVOLUTION OF SURVEILLANCE

1.1 SURVEILLANCE AS A CONCEPT AND GLOBAL PHENOMENON

Surveillance, broadly defined as the systematic observation, monitoring, and collection of information about individuals or groups, is neither a new phenomenon nor one exclusive to authoritarian regimes. Theorists such as Michel Foucault, drawing on Bentham's Panopticon model, have long argued that surveillance is an intrinsic mechanism of modern state power; a tool through which institutions manage, classify, and discipline populations. In the modern era, however, the architecture of surveillance has evolved from the physical registers, informants, and watchtowers of colonial administrations into an extraordinarily complex web of digital systems capable of monitoring billions of people simultaneously.

Historically, the origins of formalized state surveillance in Africa are inseparable from the project of European colonialism. Surveillance practices were first used by colonial governments, then continued by post-colonial governments, and are now being digitalized and accelerated across the continent. This trajectory from pass books and fingerprinting to facial recognition and commercial spyware represents a continuum of control in which the actors and technologies have changed, but the fundamental purpose has remained: the monitoring and suppression of populations deemed threatening to those in power.

1.2 COLONIAL ROOTS: THE FOUNDATIONS OF SURVEILLANCE ON THE AFRICAN CONTINENT

The foundations of surveillance infrastructure on the African continent were laid by European colonial powers between the late nineteenth and mid-twentieth centuries. Colonial powers used surveillance to enable the extraction of taxes and to monitor the struggle for independence. This surveillance was both physical and documentary in nature. In Southern Africa, passing laws requiring Black workers to carry identification documents at all times constituted one of the most invasive and pervasive surveillance systems in history. Under apartheid South Africa, the National Party imported computers specifically to impose a regime of fixed racial classification and to maintain detailed records on the African population.

In East Africa, British colonial administrators constructed elaborate networks of informants, tribal registers, and population census mechanisms to manage territories and identify potential dissidents. In Rwanda, the Belgian colonial administration introduced ethnic identity cards a system of categorical surveillance that would have tragic consequences in the 1994 genocide, as these documents became instruments of identification and targeting during the mass killings.

In South Africa, the state's biometric surveillance capabilities evolved from skin branding and fingerprinting of mine workers at the turn of the twentieth century into a sophisticated national identification infrastructure. A critical feature of colonial surveillance, extensively documented in academic literature, is what scholars have termed the 'bequeathed legacy': the institutional and technological infrastructure of surveillance was not dismantled at independence but was retained and frequently expanded by post-independence governments.

In many cases, the same Special Branch units that had spied on anti-colonial independence movements were incorporated wholesale into the security apparatuses of new African states, repurposed to monitor the very political opposition movements and civil society organisations that independence had promised to liberate.

DIGITAL SURVEILLANCE METHODS AND TECHNOLOGIES IN AFRICA.

2.1 The Technology Supply Chain: Who Sells Surveillance to Africa?

A defining characteristic of the contemporary African digital surveillance landscape is its dependence on externally supplied technology. Rather than developing indigenous surveillance capabilities, most African governments procure surveillance tools from a global market dominated by companies from China, Israel, France, the United Kingdom, Germany, and the United States.

China has been particularly prominent, providing surveillance technology through a model that bundles infrastructure lending with technology transfer. Beijing has provided billions of dollars in loans to African governments to procure its 'safe city' package of CCTV cameras with facial recognition and vehicle licence plate recognition capabilities. Huawei and ZTE are the two principal Chinese companies delivering these surveillance technologies, along with associated training and ongoing support. Nigeria, Ghana, Malawi, Zambia, Uganda, Kenya, and Zimbabwe are among the countries that have implemented Chinese-supplied urban surveillance systems under this model.

Critics have raised serious concerns about the geopolitical and sovereignty implications of African governments becoming dependent on Chinese surveillance infrastructure. Scholars argue that this reliance mirrors colonial dynamics, where external powers impose their technologies and governance models, often disregarding local contexts and needs. This has led some analysts to characterize the proliferation of Chinese surveillance technology in Africa as a form of neo-colonialism not through territorial occupation but through technological and data dependency.

GLOBAL SUPPLIERS

CHINA
Huawei (Safe City), ZTE (Infrastructure)

ISRAEL
NSO Group (Pegasus), Cellebrite

EUROPE
Thales (Biometrics), Nexa (Interception)

UNITED STATES
Palantir (Predictive Policing), Cisco

2.2 CATEGORIES OF DIGITAL SURVEILLANCE METHODS

METHOD 2.2.1

SOCIAL MEDIA MONITORING AND OPEN-SOURCE INTELLIGENCE (OSINT)

Social media monitoring is the most pervasive form of digital surveillance in Africa. Intelligence agencies utilize Open Source Intelligence (OSINT) techniques to harvest data from platforms like Facebook, X (Twitter), and TikTok. Specialized software tools enable real-time keyword tracking, sentiment analysis, and deep profiling of individuals based on their digital footprint.

Case Study: During Nigeria's 2020 #EndSARS movement, social media surveillance was used to identify protest leaders, track mobilization patterns, and profile activists for subsequent legal or extra-legal targeting.

METHOD 2.2.2

COMMERCIAL SPYWARE: THE PEGASUS PARADIGM

Commercial spyware software sold by private companies to government clients for the covert compromise of mobile devices and computers has emerged as one of the most powerful and concerning surveillance tools available to African governments. NSO Group's Pegasus software represents the most sophisticated and widely documented example of this category. Pegasus is capable of silently accessing a target device's calls, messages, emails, contacts, microphone, camera, and location data all without the user's knowledge or consent.

The 2021 Pegasus Project, a collaborative investigation by 17 international media organisations, revealed the extraordinary breadth of Pegasus deployment across Africa. Of the 14 world leaders identified on the list of suspected Pegasus targets, half were African, including two sitting heads of state. Among the five African countries identified as likely Pegasus operators are Rwanda, Morocco, Togo, and Uganda. Rwanda has been reported to have used NSO software to target as many as 3,500 activists, journalists, political opponents, and diplomats.

THE PEGASUS PROJECT AND AFRICA

?

The 2021 Pegasus Project investigation revealed that commercial surveillance technology has been weaponized across Africa at a scale that defies earlier assumptions about the geographic and financial limitations on advanced spyware use. The findings demonstrate that powerful surveillance capabilities are no longer limited to well-resourced intelligence agencies in high-income countries but are commercially available to any government with the budget and political will to procure them, with devastating consequences for civil society, journalists, and political opposition across the continent.

2.2.3 TELECOMMUNICATIONS INTERCEPTION AND SIM CARD REGISTRATION

NETWORK INTERCEPTION

Network-level surveillance, including the interception of mobile and internet communications at the telecommunications infrastructure level, is practiced widely across Africa and is often mandated by law. Governments require telecommunications companies and internet service providers to install lawful interception capabilities that allow intelligence agencies to monitor communications in real time or access stored communications data.

SIM REGISTRATION

SIM card registration requirements now nearly universal across African countries have significantly expanded governments' ability to link digital communications to individual identities. In Uganda, for instance, SIM card registration became mandatory in March 2012 under the Regulation of Interception of Communications Act. While proponents argue that registration reduces crime and terrorism, critics note that it creates a comprehensive database linking phone numbers to biometric data, enormously facilitating targeted surveillance of specific individuals.

2.2.4 CCTV NETWORKS WITH FACIAL RECOGNITION

Urban surveillance infrastructure, including extensive closed-circuit television (CCTV) networks integrated with artificial intelligence-powered facial recognition software, has been deployed in major African cities. In South Africa, the private security company Vumacam has built a network of over 6,600 cameras in Johannesburg alone, with the footage feeding into security control rooms using AI tools including licence plate recognition to track population movement. In Kenya, collaboration with Chinese firms has resulted in the installation of facial recognition systems across urban areas. In Uganda, significant Chinese investment in CCTV infrastructure in Kampala has raised concerns about the integration of urban surveillance systems with the national intelligence apparatus

2.2.5 PHISHING ATTACKS, MALWARE, AND CYBER INTRUSION

Beyond commercial spyware, African civil society organizations (CSOs) and journalists face constant threats from phishing attacks and malware distribution. These campaigns use deceptive emails or messages to trick targets into revealing credentials or installing malware, providing attackers with persistent access to sensitive organizational data.

Email compromise is a primary vector. By gaining unauthorized access, attackers can impersonate staff, monitor internal deliberations, and compromise relationships with donors and partners. The lack of robust technical capacity in many CSOs makes them particularly vulnerable to these low-cost, high-impact intrusions.

METHOD 2.2.6

Insider Threats and Human Intelligence Operations

Alongside technical surveillance methods, African intelligence services regularly deploy traditional human intelligence (HUMINT) techniques, including the recruitment or coercion of individuals within civil society organizations to report on their colleagues, programs, and communications. The effectiveness of technical surveillance can be dramatically amplified when combined with insider access: a recruited informant can provide encryption keys, physical access to devices, advance warning of planned activities, and intelligence about internal deliberations that no remote technical system can replicate.

The prevalence of insider threats represents a particularly difficult challenge for CSOs because it requires not merely technical solutions but institutional and cultural responses. Organizations must develop trust frameworks, information-sharing protocols, and confidential reporting mechanisms while simultaneously avoiding the corrosive paranoia that a fear of infiltration can generate within teams.

THE INSTITUTIONAL CHALLENGE

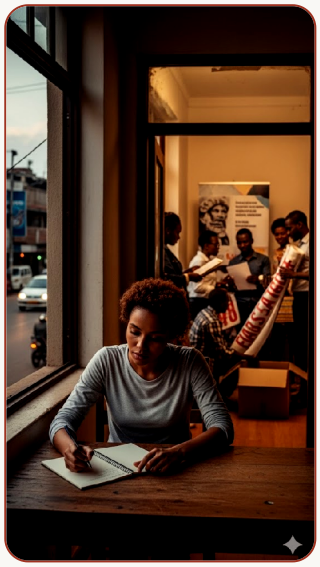
Addressing insider threats requires more than technical patches; it demands institutional trust frameworks and secure information-sharing protocols. Organizations must balance vigilance with the need to maintain a collaborative, non-paranoid working environment.

The Surveillance Nexus: The most potent threat arises from the combination of digital and human surveillance. A recruited informant can provide the encryption keys or physical access needed to deploy spyware, while digital monitoring validates the informant's reports. This hybrid approach creates a comprehensive surveillance net that is nearly impossible to evade.

2.3 THE CHILLING EFFECT: HOW SURVEILLANCE SUPPRESSES CIVIL SOCIETY

THE CHILLING EFFECT

One of the most significant and insidious effects of digital surveillance is the chilling effect it produces on civil society activity even in the absence of direct repression. Research conducted across African contexts consistently demonstrates that when individuals and organizations know or believe that their communications are being monitored, they modify their behaviour in ways that serve the interests of those conducting surveillance.



The chilling effect manifests in multiple ways: journalists self-censor reporting on sensitive subjects; civil society organizations avoid working on issues that attract government attention; activists use less effective communication channels to evade surveillance; donors and international partners reduce their engagement with surveilled organizations; and sources and whistleblowers decline to share information out of fear of identification.

The Uganda Communications Act of 2013 established the Uganda Communications Commission (UCC) as the primary regulatory body. Section 5(u) provides an exceptionally broad mandate, including the establishment of 'an intelligence-gathering capability.' Critics argue this creates a structure where the regulator and surveillance apparatus are effectively fused, allowing directives that directly affect civil society organizations' ability to communicate freely.

3.2.5 THE DATA PROTECTION AND PRIVACY ACT, 2019

Uganda's Data Protection and Privacy Act, enacted on February 25, 2019, represents the most significant legislative development in favour of privacy rights in Uganda's recent history. The Act was the first of its kind in East Africa and was designed to give effect to Article 27 of the Constitution and Uganda's obligations under international human rights instruments.

The Act establishes important rights for data subjects, including the right to consent to collection and processing, the right to access personal data held about them, and the right to seek correction or deletion. It imposes obligations on data controllers and processors to implement appropriate security measures and to obtain consent before collecting or processing personal data. Criminal sanctions apply for unlawful obtaining, disclosing, or destroying personal data.

THE LEGAL CONTEXT OF SURVEILLANCE IN UGANDA

3.1 3.1 The Constitutional Framework: Privacy as a Fundamental Right

The constitutional protection of privacy in Uganda is grounded in Article 27 of the Constitution of the Republic of Uganda (1995, as amended). Article 27(1) states that no person shall be subjected to unlawful search of the person, home, or other property of that person, and Article 27(2) provides that 'no person shall be subjected to interference with the privacy of that person's home, correspondence, communication or other property.'

ANALYSIS

This constitutional guarantee establishes the foundational right upon which all surveillance law in Uganda must be grounded. However, the constitutional provision's effectiveness as a check on state surveillance is substantially undermined by a matrix of overlapping statutory instruments that confer broad surveillance powers on state agencies with inadequate oversight, limited judicial authorization requirements, and minimal avenues for civil society or individual redress.

ARTICLE 27 (1995)

27(1): No person shall be subjected to — (a) unlawful search of the person; or (b) unlawful entry. 27(2): No person shall be subjected to interference with the privacy of home, correspondence or communication.

KEY LEGISLATIVE INSTRUMENTS GOVERNING SURVEILLANCE SEC 3.2

REGULATION OF INTERCEPTION OF COMMUNICATIONS ACT, 2010 (RICA)

The RICA (2010) is the primary legislative instrument governing communications surveillance. It establishes a framework for lawful interception requiring intelligence officials to seek judicial authorization.

RICA 2010 (SEC. 8)

Requires all telecommunications companies and ISPs to ensure their services are technologically capable of allowing lawful interception unknowingly to the target. Failure results in sanctions.

THE LEGAL CONTEXT OF SURVEILLANCE IN UGANDA

RICA 2010 | COMPUTER MISUSE | ANTI-TERRORISM | UCC ACT

THE COMPUTER MISUSE ACT, 2011 AND THE 2022 AMENDMENT

The Computer Misuse Act of 2011 established Uganda's primary legal framework for cybercrime and computer-related offences. While ostensibly designed to protect individuals and organizations from cyber attacks, the Act has been extensively criticized for its weaponization against political opponents, journalists, activists, and civil society representatives.

The most notorious provision was Section 25, which criminalized 'offensive communication' and was declared unconstitutional by Uganda's Constitutional Court on January 10, 2023. Justice Kenneth Kakuru, writing the lead judgment, found that Section 25 was 'vague, overly broad and ambiguous' and gave 'law enforcement unfettered discretion to punish unpopular or critical protected expression.'

Rather than addressing structural deficiencies, however, the government enacted the Computer Misuse (Amendment) Act on October 14, 2022. The Amendment introduced new offences with broad formulations that CSOs argue replicate and expand the repressive potential of the provisions struck down.

CMA (2011/2022)

2022 offences: Ridiculing or demeaning any person, tribe, or gender (7 yrs); Misuse of social media-publishing with disguised identity; Unauthorized recording of an individual (10 yrs).

ANTI-TERRORISM ACT

Sec. 9: Offence to publish info connected to terrorism. Sec. 10: Minister can designate terrorist suspects. Sec. 19: Digital and physical surveillance against designated suspects.

THE ANTI-TERRORISM ACT, 2002 (AS AMENDED 2022)

The Anti-Terrorism Act provides sweeping surveillance powers. Section 19 authorizes interception of communications through wiretapping, digital surveillance, and physical stake-outs. Section 10 grants the Interior Minister broad authority to designate terrorist suspects, triggering full surveillance protocols.

THE UGANDA COMMUNICATIONS COMMISSION ACT, 2013

The Act's implementation has been hampered by delays and lack of oversight. The Data Protection Office under NITA-U raises independence concerns. Government has intensified mandatory collection of sensitive personal data through national ID systems, sharing information without transparent legal authority.

DATA PROTECTION ACT (2019)

Sec. 3, 10, 17, 35: Prohibits processing of personal data that infringes on privacy. Criminalizes unauthorized disclosure of personal info.

MANDATORY SIM REGISTRATION

Since 2012, all SIM cards require biometric registration, linking phone numbers to identities. This eliminates anonymity in mobile communication.

PEGASUS SPYWARE & ECMU OPERATIONS

THE PEGASUS SCANDAL: UGANDA'S USE OF COMMERCIAL SPYWARE

The 2021 'Pegasus Project' investigation by Amnesty International and Forbidden Stories revealed that Pegasus spyware, developed by NSO Group, has been used globally to target over 50,000 phone numbers, including those of heads of state, activists, and journalists. In Africa, usage has been documented in Rwanda, Morocco, Togo, and Uganda. Documents accessed by the Financial Times confirmed that the Ugandan government spent in excess of UGX 35 billion on the acquisition.

PEGASUS ACQUISITION

- Year of acquisition: 2019
- Cost: Over UGX 35 billion
- First confirm: 2021 Apple notifications
- Recent: 2025 selection season targeting
- *Full remote access to messages, microphone, camera, and GPS.*

PEGASUS CAPABILITIES

- Live Call Interception
- Ambient Mic Recording
- GPS Location Tracking
- Remote Camera Activation
- Full Data Access (WhatsApp/Signal)
- Zero-Click Infection

The targeting of journalists and activists represents the most severe risk. In late 2021, Apple notified at least nine US State Department employees in Uganda of state-sponsored attacks. This technology allows for 'total surveillance,' turning a personal device into a 24-hour monitoring tool.

THE ELECTRONIC COUNTER MEASURE UNIT (ECMU)

The Uganda Police Force has established a specialized Electronic Counter Measure Unit (ECMU) with a mandate to detect and investigate crimes committed using online platforms and electronic communications. The ECMU is the unit responsible for overseeing the implementation of the Computer Misuse Act.

More recently, in 2025, ahead of the 2026 elections, Ugandan investigative journalist Canary Mugume publicly disclosed receiving Apple notifications warning of targeted mercenary spyware attacks on his device. This pattern of spyware use against journalists during electoral periods is a direct and serious threat to press freedom and civil society operations in Uganda.

Civil society organizations in Uganda have consistently identified the ECMU as a major instrument of digital surveillance directed at their activities. The gap between the formal legal requirements for surveillance authorization and the practical reality of how surveillance is conducted represents one of the most significant rule-of-law concerns in Uganda's digital rights landscape.

SECTION 4: INTERNATIONAL STANDARDS

INTERNATIONAL HUMAN RIGHTS LAW AND SURVEILLANCE

UNIVERSAL AND REGIONAL HUMAN RIGHTS FRAMEWORKS

Uganda's surveillance practices must be assessed not only against domestic law but against the international human rights obligations to which Uganda is a party. These obligations establish baseline standards for the conditions under which surveillance may be lawfully conducted and the protections that must be in place to prevent abuse.

The Universal Declaration of Human Rights (UDHR, 1948), Article 12, establishes that 'no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence.' Uganda ratified the International Covenant on Civil and Political Rights (ICCPR) on June 21, 1995. Article 17 of the ICCPR provides that 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.'

The African Charter on Human and Peoples' Rights (Banjul Charter, 1981), to which Uganda is a party, protects related rights including freedom of expression (Article 9), freedom of association (Article 10), and freedom of assembly (Article 11). Digital surveillance that chills these freedoms by deterring individuals from associating with civil society organizations constitutes a prima violation of Uganda's obligations under the African Charter.

THE NECESSITY AND PROPORTIONALITY STANDARDS

Under international human rights law, restrictions on the right to privacy are permissible only where they meet three cumulative criteria: they must be prescribed by law, necessary to achieve a legitimate aim, and proportionate to that aim. UN General Comment No. 16 (1988) on Article 17 of the ICCPR stated that surveillance, interceptions of telephonic and other communications, wire-tapping, and recording of conversations may be authorized only in cases meeting the strictest standards.

An honest assessment of Uganda's surveillance legal framework against these standards reveals significant deficiencies. The broad scope of the Anti-Terrorism Act's designated suspects category, the mandatory interception capabilities of RICA, the vague formulations of the Computer Misuse Act, and the absence of meaningful independent oversight collectively fail to meet required international law standards.

THE RIGHT TO COMMUNICATE ANONYMOUSLY AND USE ENCRYPTION

International human rights law has increasingly recognized that the right to privacy in the digital age encompasses the right to communicate anonymously and to use encryption. UN Special Rapporteurs have affirmed that states should not require the removal, weakening, or backdooring of encryption technologies.

Uganda's legal framework does not explicitly prohibit encryption. However, Section 10 of RICA, which authorizes compelling individuals to provide encryption keys and decryption codes under penalty of criminal sanction, substantially undermines the practical protection that encryption provides. The provision creates a legal obligation to surrender the very tools that individuals rely upon to protect their communications.

PRIMARY SURVEY FINDINGS: THE LIVED EXPERIENCE OF SURVEILLANCE AMONG UGANDAN CSOS

This section introduces a qualitatively distinct form of evidence: the direct testimony of 74 civil society practitioners across Uganda, collected through a structured survey administered in March 2025. These findings are original, unpublished, and exclusive to this research. They represent the first systematic primary data collection from Ugandan CSOs on the lived experience of digital surveillance in the pre-2026 election period.

The survey sought to document: the extent of concern about surveillance; practitioners' awareness of surveillance tactics; which forms of surveillance have been encountered; the operational impacts on CSO activities; existing mitigation strategies; support needs; and priority actions ahead of the 2026 elections. Responses came from 74 individuals representing 68 or more organisations spanning human rights, governance, minority advocacy, health, environment, women's rights, anti-corruption, media, and community development work.

CONCERN AND AWARENESS: A SECTOR UNDER PRESSURE

The response is unambiguous: 82% of respondents described themselves as 'very concerned' or 'extremely concerned' about digital surveillance affecting their work or personal lives. A further 7% described themselves as 'moderately concerned.' Only one respondent indicated no concern.

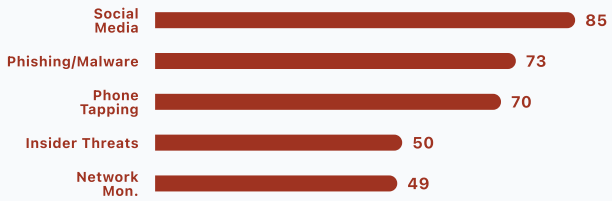
82% SURVEY STAT

are very or extremely concerned

Research on 68+ CSOs across Uganda (March 2025).

On awareness: 73% described themselves as 'somewhat aware,' with only 18% 'very aware.' This gap between high concern and partial knowledge is significant: it suggests practitioners respond to generalised fear of surveillance rather than technical threat assessments.

FORMS OF SURVEILLANCE ENCOUNTERED: WHAT PRACTITIONERS HAVE EXPERIENCED



Social media monitoring (85%) and phishing/malware (73%) top the list. Phone tapping (70%) reflects mandated interception infrastructure. The insider threat figure (50%) is striking.

OPERATIONAL IMPACTS: THE DAMAGE ALREADY BEING DONE

IMPACT AREA	COMBINED RESULT
Targeting of key individuals	85%
Digital communication	84%
Partner/Funding relationships	81%
Compromised staff safety	77%
Leakage of confidential info	77%
Self-censorship	68%

VERBATIM TESTIMONIES

"Someone hacked into my email address and began sharing my private photos on Facebook while demanding a two million shilling ransom."
— RESPONDENT A

"Theft of computers by suspected security operatives."
— RESPONDENT B

"Break-ins to access perceived assets (Info)."
— RESPONDENT C

"Anonymous calls requesting for sensitive information."
— RESPONDENT E

The single highest impact (85%) is for the targeting of key individuals. This is the endangerment of journalists and advocates.

The 81% impact on donor relationships has profound systemic implications. Association becomes too risky.

PRIMARY SURVEY FINDINGS (FINAL)

PREPAREDNESS AND MITIGATION: A CRISIS OF CAPACITY

97%

PREPAREDNESS GAP

Only 3% of respondents reported a comprehensive security strategy. 97% range from partially prepared to entirely unprotected. This gap is the defining vulnerability of the sector.

SUPPORT NEEDS: WHAT PRACTITIONERS ARE ASKING FOR

SUPPORT REQUESTED	RESP.	PERCENTAGE
Digital security training for staff	65	88%
Financial support for cybersecurity infrastructure	58	78%
Provision of secure communication tools	53	72%
Legal support for cases of digital harassment	41	55%

PRIORITY ACTIONS

Digital literacy (95%) reflects capacity needs. Secure networks (85%) and emergency response (81%) suggest practitioners think in collective terms.

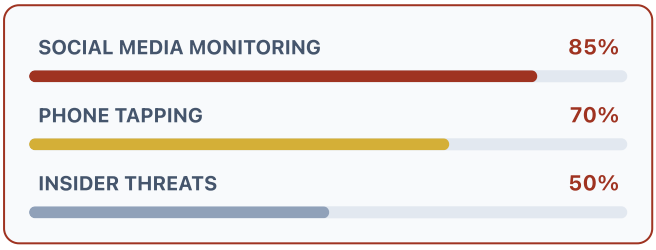
THE UNIQUE EVIDENTIARY VALUE OF THIS SURVEY

The findings represent the first systematic primary data collection on digital surveillance in the pre-2026 election period. Engaging with this evidence is essential for an accurate picture of reality.

SYNTHESIS: THE ARCHITECTURE OF SURVEILLANCE AND ITS IMPLICATIONS FOR UGANDAN CSOS

THE LEGAL-TECHNICAL SURVEILLANCE NEXUS

The legal framework analysed in Section 4 and the technical capabilities described in Section 2 do not operate independently. They function as complementary components of an integrated architecture of surveillance in which each element reinforces the others. RICA mandates that the national communications infrastructure be interception-ready. Mandatory SIM registration ensures that all mobile communications can be attributed to specific individuals.



The primary findings provide evidence that this legal-technical architecture is operational and producing measurable harm: 85% experience social media monitoring; 70% report phone tapping; 50% encounter insider threats; and only 3% have comprehensive protective strategies.

SPECIFIC VULNERABILITIES OF CSOS

GOVERNANCE & HUMAN RIGHTS

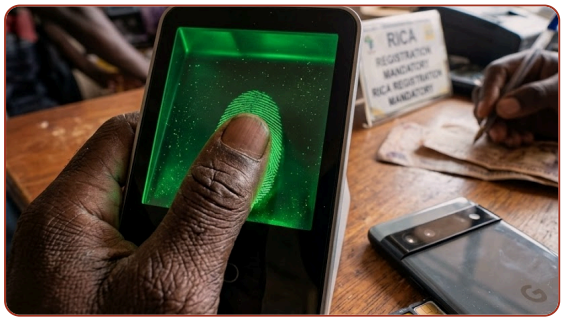
Organizations working on governance, human rights documentation, or political advocacy are at heightened risk of characterization as security threats.

INTERNATIONAL DONOR RELATIONS

CSOs face risks related to financial surveillance and the characterization of foreign funding as foreign interference.

SIM CARD REGISTRATION VULNERABILITY

Mandatory SIM registration leaves CSOs acutely vulnerable. All staff communications are fully traceable, yet the phone numbers used to conduct surveillance and send threats frequently turn out to be untraceable. This creates a severe security gap, exacerbated by the fact that both Telcos and the UCC routinely fail to take action against these threat actors.



MARGINALIZED GROUPS & ACTIVISTS

Organizations working with marginalized groups operate where legal risks of exposure are acute giving records.

CONCLUSION & STRATEGIC TAKEAWAYS

CONCLUSION

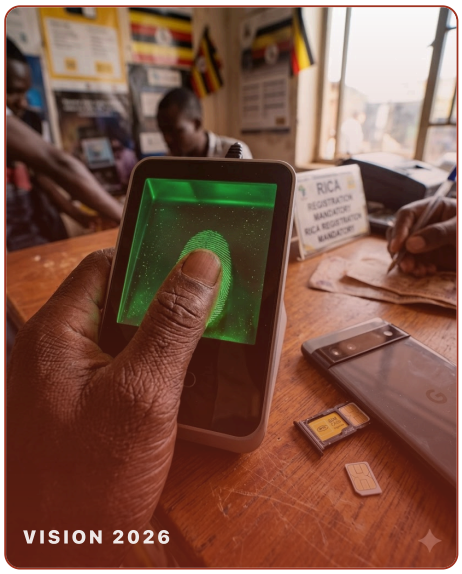
The intersection of a deeply rooted colonial tradition of surveillance, a contemporary technology market that makes sophisticated digital surveillance tools commercially available to resource-constrained governments, and a legal framework in Uganda that normalizes and enables surveillance while providing inadequate protection for privacy rights creates a formidable challenge for civil society organizations seeking to carry out their work safely and effectively.

The primary findings ground this structural analysis in reality: behind every percentage point is a practitioner, an organisation, and a community whose capacity to contribute to Uganda's civic life is being constrained by the surveillance environment. The 2026 elections make the urgency of action acute.

KEY TAKEAWAY

The data confirms that the surveillance architecture is active and active, producing harm, and confronting a civil society sector that is aware of the threat but comprehensively under-resourced to meet it. Effective responses must be systematic, combining capacity building with advocacy and international engagement.

- TECHNICAL CAPACITY BUILDING
- LEGAL & POLICY ADVOCACY
- SECURITY CULTURE
- INTERNATIONAL ACCOUNTABILITY



Addressing this requires engagement at multiple levels: technical, organizational, legal, and international.

SECURE THE FUTURE OF DIGITAL RIGHTS

PARTNER WITH US TO BUILD A RESILIENT, SECURE, AND FREE CIVIL SOCIETY IN UGANDA.

CALL: +256 392 201102

EMAIL: communications@defendersprotection.org

VISIT: Plot 5, Kintu Alley, Kulambiro Ring Rd, Kampala, Uganda

Image Credits: Some images in this report were generated using Google Gemini AI, based on prompt-guided design. These visuals are intended to support conceptual representation and do not depict real individuals or events. Other images, where applicable, are credited to their respective sources.