DEFENDERS
PROTECTION INITIATIVE

SECURE & DEFEND

A TOOLKIT FOR ACTIVISTS & DEFENDERS

Contents

Foreword

In today's increasingly complex and high-risk environment, human rights defenders, journalists, and activists continue to face both digital and physical threats for the vital work they do. Whether defending land and environmental rights, exposing injustice, or organizing for equality, they are often on the frontline of resistance—yet too often lack the tools and support systems to ensure their safety. This toolkit was created in response to that urgent need: to offer practical, adaptable, and locally rooted strategies for staying safe while continuing the work that matters most.

This toolkit draws not only from best protection practices, but from lived realities, contextual analysis, and the insights of those navigating hostile environments every day. It is both a guide and a companion—a tool designed to help defenders anticipate, respond to, and recover from threats while fostering a culture of collective care and security. It is grounded in a feminist and trauma-informed lens, acknowledging that safety is not just a technical issue, but deeply personal, political, and systemic.

Acknowledgements

This toolkit is the result of a collaborative process, shaped by the commitment and contributions of many individuals and communities who share a vision for a safer, more just world.

Sincere appreciation to the DPI team Helen Namyalo Kimbugwe, Noelyn Nassuuna, Fred Drapari, and Edson Tukashaba for conceiving the idea for this toolkit. Their unwavering commitment to developing defender-centred resources and amplifying the voices of those at risk has been instrumental in bringing this initiative to life.

We extend our sincere appreciation to Julie Butinde, our Research and Content Consultant.

Special thanks go to the over **60 activists, defenders, journalists, lawyers, researchers and community organizers** from across Uganda who participated in the context analysis meetings. Their insights, lived experiences, and strategic recommendations were invaluable in shaping the toolkit's relevance and responsiveness to real-world threats

To all who contributed—openly or quietly—thank you. Your voices and courage continue to inspire us.

The DPI Team

Introduction

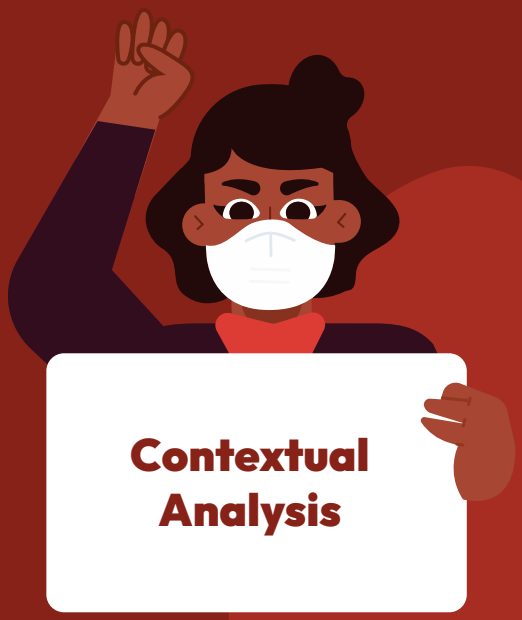
The safety, security and protection of Human Rights Defenders (HRDs) remain critical and necessary, as highlighted by the establishment of the 1998 United Nations Declaration on Human Rights Defenders.[1] This commitment was further reinforced in 2000 with the appointment of the UN Special Rapporteur on the situation of human rights defenders,[2] a recognition of the persistent threats and attacks HRDs face due to the nature of and, as a result of their work.

Even with these initiatives in place, the challenges persist today. Additionally, advancements in technology, the evolving geopolitical landscape, and the dynamic nature of the risks and threats themselves, underscores the urgency for updated safety, security, and protection mechanisms. These measures must not only address contemporary threats but also be tailored to the specific risks faced by different types of HRDs today.

Purpose of the Safety & Security Toolkit

Informed by a series of consultations with activists, journalist and HRDs and leveraging on Defenders Protection Initiative (DPI)'s years of experience in fostering safety and security of HRDs, this toolkit offers practical safety and security guidelines for Activists, Journalists and other HRDs/organizers to safeguard themselves while continuing their vital work. Your efforts to drive social change, development, and justice are invaluable, and this toolkit is intended to equip you with the necessary safety measures to continue your work effectively and securely.

1. United Nations. (1998). Declaration on human rights defenders. Office of the High Commissioner for Human Rights. Retrieved frowithm https://www.ohchr.org/en/civic-space/declaration-human-rights-defenders
2. International Justice Resource Center. (n.d.). Special Rapporteur on the situation of human rights defenders. Retrieved from https://ijrcenter.org/un-special-procedures/special-rapporteur-on-the-situation-of-human-rights-defenders/



Contextual Analysis

Historical patterns indicate a surge in human rights violations, threats, and violence against Human Rights Defenders (HRDs), journalists, and activists in Uganda, particularly in the lead-up to and during election periods.

Between 2014 and 2015, in the lead-up to the 18th February, 2016 Presidential elections, violations included: selective enforcement of the **Public Order Management Act, 2013** [3] to block HRDs from rallying for electoral reforms, [4] dispersal of civilians from campaign rallies of opposition party candidates using teargas, the deployment of teargas on journalists covering the gatherings. [5]

With technological advancement and the advent of digital activism coupled with the COVID-19 pandemic, which drove increased reliance on digital tools, human rights violations took a digital form. This was evident in the 2021 Facebook block and the week-long internet shutdown that occurred in the middle of the 2021 presidential elections.

From 2024, ahead of the 2026 elections, DPI held a series of consultative contextual analysis and scenario-building meetings with over 60 key respondents, comprising HRDs, activists, and journalists. They expressed fears that similar violations would occur, and in some cases had already begun, underscoring the urgent need to understand and address the evolving risks and threats faced by HRDs in order to develop proactive mitigation and prevention strategies. The trends, risks and challenges identified included:

Abuse and Violence

- Physical abuse.
- Destruction of equipment.
- Arbitrary Arrests and Illegal Detentions.
- Surveillance, Kidnapping/ Disappearances.

Online Threats

- Cyber bullying/ harassment.
- Digital, financial Monitoring & Surveillance

Organizational & Structural Challenges

- Increased scrutiny of NGOs and NGO Leaders.
- Restrictive Laws.
- Militarization of Services.

Restrictions on Freedom of Expression

- Misinformation and Disinformation.
- Stigmatization and criminalization of HRDs/activists, their organisations and their work.

3.https://media.ulii.org/media/legislation/18570/source_file/382bdadaf4956329/2013-9.pdf
4.https://www.monitor.co.ug/News/National/Police-block-opposition-rally-on-electoral-reforms-rally/-/688334/2255132/-/fqj30y/-/index.htm
5.https://www.hrw.org/news/2015/10/19/uganda-end-police-obstruction-gatherings

1. Physical Violence, Arbitrary Arrests and Enforced Disappearances

During electoral periods, opposition campaign rallies, activist gatherings, and protests are frequently dispersed with violence by police and other security forces, even in the absence of disorder. Preventive arrests are common, as are forced shutdown of protests and demonstrations, arbitrary arrest and detention of protestors and abductions of opposition members/government critics.

Notable Incidents

2014

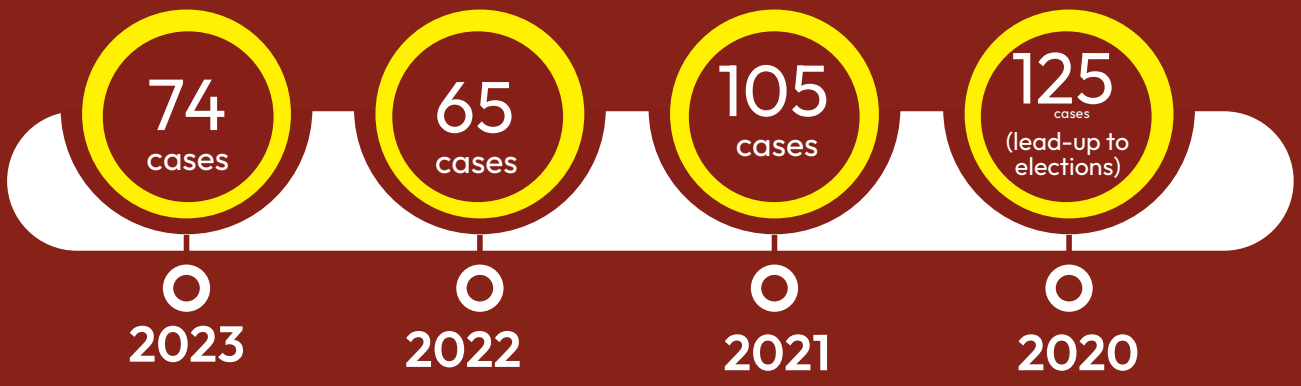
Seasoned HRD Bishop Zach Niringiye, together with opposition party leaders, was blocked from organizing rallies in Eastern Uganda to garner support for electoral reforms ahead of the 2016 elections.

The leader of the Jobless Brotherhood activist group disappeared and was reported to have been tortured following protests against rising corruption. [6]

2016

6 youth activists arrested on inflated charges of inciting violence after bringing chickens to City Square in protest of high youth unemployment. [7]

Similarly, journalists, often covering these events, are subjected to physical assaults, intimidation, confiscation and destruction of equipment and arbitrary arrests as documented by the Human Rights Network for Journalists-Uganda in its 2023 Press Freedom Index Report. [8]



Notable Incidents:

2015

Oct-Nov: Within 2 months **3** journalists shot at with live bullets while covering Political events in Kampala, Mityana and Jinja. [9]

2015

Police attack journalists covering the arrest of Hon. Ssemujju Nganda, Kyadondo East MP. This is a day after a direct threat issued by the then Inspector General of Police against NTV and NBS journalists saying; "...we are going to go against you. [10]

2021

8 journalists were beaten and injured by military officers while covering former Presidential Candidate Robert Kyagulanyi's delivery of a petition to the United Nations High Commissioner for Human Rights (OHCHR) to take action against security agencies for violating the rights of Ugandans. [11]

2025

28 journalists beaten and injured by security forces while covering Kawempe North by-elections. This section outlines practical safety measures for activists and journalists, including precautions before attending or covering campaign rallies and protests, immediate response strategies during attacks, and post-attack measures to ensure their protection and safeguard the continuity of their vital work in promoting transparency and accountability.

---

6. https://reliefweb.int/report/uganda/uganda-events-2015
7. https://www.hrw.org/world-report/2016/country-chapters/uganda
8. Press Freedom Index Report 2023 – Media Freedoms in the Age of Digital Revolution, Human Rights Network for Journalists-Uganda (HRNJ-U), accessed from:https://hrnjuganda.org/?wpdmpro=press-freedom-index-report-2023-media-freedoms-in-the-age-of-digital-revolution
9. Foundation for Human Rights Initiative (FHRI), Human Rights and Elections in Uganda (2016): A Call for Action – Human Rights Violations During Uganda's 2016 General Election, 2016.
10. Foundation for Human Rights Initiative (FHRI), Human Rights and Elections in Uganda (2016): A Call for Action – Human Rights Violations During Uganda's 2016 General Election, 2016.
11.https://acme-ug.org/2021/02/17/eight-journalists-beaten-on-orders-of-military-officer-at-un-human-rights-office/


PROPAGANDA
propaganda

Preventative Safety Measures & Response Strategies.

Before Campaign, Protest/Field Reporting

1. Risk Mapping & Profile Awareness

• Identify who might target you, whether state actors, political or corporate interest groups and how they may act, for example through surveillance, threats, smear campaigns, or physical violence.
• Know your risk profile which may depend on factors such as your gender, location, advocacy focus, media affiliation, or political visibility.
• Understand relevant laws, especially the Constitution of Uganda (Articles 23 & 29), the Public Order Management Act (POMA), and Penal Code provisions commonly misused to arrest for incitement unlawful assembly).
• Maintain pre-arranged legal representation through trusted lawyers or legal aid organizations.

2. Safety Planning

• Develop a safety plan with clear check-in protocols for protests, meetings, or fieldwork.
• Share your plan with trusted contacts.
• Notify someone of your whereabouts and expected return time.

3. Emergency Readiness

• Carry a legal emergency card with:
  a. Lawyer's name and number
  b. Medical contact
  c. Close relative or HRD network contact

4. Field Reporting & Protest Safety

• Use a buddy system, avoid working alone, especially during travel or outreach.
• Move in teams with legal and safety observers where possible.
• Identification: Carry press IDs, HRD tags, or observer badges.
• Carry minimal or neutral physical materials when in high-risk areas.

In-the-Moment Responses to Abuse or Violence

1. Immediate De-escalation
- Stay calm, avoid provocation, and document discreetly if possible.
- If attacked try to retreat to safety and record details of attackers (appearance, uniforms, vehicles, etc)

2. Activate Your Emergency Protocol
- Have a panic signal like a text code, missed call, or app alert to notify allies.
- Contact legal support or emergency protection networks like DPI.
- Contact legal support or emergency protection networks like DPI.

3. Medical & Legal First Response
- Seek medical care immediately and ensure injuries are documented with photos and reports.
- Report to police only if safe and strategic, otherwise go through intermediaries or trusted legal organisations.

Post-Attack Support & Strategy

1. Document the Abuse
- Record what happened: time, location, perpetrators, type of violence.
- Gather witness statements, media footage, and medical records.

2.File Reports Strategically
Submit complaints to:
- Uganda Human Rights Commission.
- Media Council (for journalists)
- Independent lawyers or CSO documentation platforms.

3. Psychosocial Support
- Seek trauma counseling, especially for survivors of sexual violence or public humiliation.
- Create or tap into peer support circles for journalists and activists.

4. Public Pressure & Solidarity
With the survivor's explicit consent,mobilize for public attention and solidarity through;
- Press releases
- social media campaigns to spread awareness.
- Engaging regional and international advocacy bodies (African Commission on Human and Peoples' Rights, UN Special Rapporteurs).

5. Safety Protocols for Media Houses/CSOs
- Create in-house safety manuals and reporting pathways.
- Appoint security focal persons within teams.

6. Protection Networks
- Strengthen alliances among journalists, HRDs, and legal/ medical responders.
- Use Signal groups for rapid alerts and coordination.

See Annex 1 for Emergency and Support organisations and resources.

Tailored Tips for Specific Groups

For Women Activists & Journalists:
- Anticipate gender-based violence and online harassment.
- Use secure reporting channels specifically dedicated to women (see Annex I).
- Avoid isolated interviews or field visits, always go with a colleague.

For Rural or Grassroots Activists:
- Build strong ties with local allies (e.g., cultural, religious leaders) who can intervene or negotiate.
- Secure offline safety measures like shelter houses, coded language, or local alarm systems.

During Arrest or Detention

- Stay calm and compliant but alert.
- Politely assert your right to remain silent and right to legal representation.
- Avoid confrontation or physical resistance, which can escalate the situation.
- Use a panic code or pre-arranged signal to alert your network/lawyer.
- If allowed, send a brief message indicating your location or what's happening.
- Observe and remember the names, ranks, or badge numbers of officers, vehicles, and detention locations.

Post-Arrest Response Strategies

- Immediately activate a rapid legal support network to trace location and file habeas corpus applications.
- Issue a public statement through reputable civil society platforms or coalitions.
- Where appropriate, mobilize media and online campaigns to highlight cases of illegal detention and demand accountability.
- Offer medical and psychosocial support post-detention (especially for trauma, sexual violence, or inhuman treatment).
- Encourage rest and structured debriefing with trusted allies.
- Collect affidavits, photos, or medical records to build evidence for compensation or legal action against unlawful detention.
- Partner with national and international organizations to pursue strategic litigation or UPR submissions.

2. Online Harassment, Digital Monitoring and Surveillance of Activists, Journalists and Human Rights Defenders in Uganda

In Uganda, online harassment and digital surveillance have become increasingly sophisticated tools used to intimidate, [12] silence, and exert control over activists, journalists, and Human Rights Defenders (HRDs). [13] These tactics not only violate fundamental rights to privacy and freedom of expression, but also create a chilling effect that threatens personal safety, mental wellbeing, and civic participation.

The use of technology to monitor, discredit, or target HRDs, often under vague or punitive legal frameworks, has deepened digital vulnerabilities across civil society. As such, there is an urgent need for strengthened digital security practices, legal protections, and coordinated advocacy to defend those who speak truth to power and hold institutions accountable. [14]

Here are practical and contextual safety measures and response strategies tailored for online harassment and digital surveillance faced by activists and human rights defenders (HRDs) in Uganda.

Preventative Safety Measures & Response Strategies

Proactive Measures

1. Strengthen Digital Hygiene

- Use strong, unique passwords and enable multi-factor authentication for all key accounts (email, social media,cloud storage).
- Regularly audit digital footprints: remove personal info from public spaces, limit what you post in real-time.
- Lock down device access with PINs, biometric locks, and encryption.

2. Secure Communication Channels

- Switch to end-to-end encrypted apps like:
  - Signal for messages and calls
  - ProtonMail or Tutanota for email
  - Jitsi Meet or Element for secure video conferencing

3. Minimize Metadata Exposure

- Avoid posting photos or files with location data or EXIF info.
- Use tools like MAT2 (Metadata Anonymisation Toolkit) to scrub documents before sharing.
- Be cautious about the permissions you grant apps. Ask yourself if they really need access to certain information like your contacts and location.

12.https://edition.cnn.com/2023/05/25/africa/uganda-women-politicians-online-abuse-as-equals-intl-cmd/index.html
13.https://observer.ug/news/ssekaana-sentences-uls-president-ssemakadde-to-two-years-for-contempt-of-court/
14.https://pen.org/press-release/stella-nyanzi-ugandan-writer-activist-released/

4. Anonymity & Pseudonymity (When Needed)

- For high-risk HRDs, consider using pseudonymous accounts or aliases online.
- Use separate browsers or devices for sensitive work and personal use.

5. Limit Platform Tracking

- Use privacy-focused browsers like Brave or Firefox (with add-ons like uBlock Origin, HTTPS Everywhere, Privacy Badger).
- Use VPNs or Tor to mask your IP and bypass surveillance or censorship.

Immediate Safety Responses

1. Do Not Engage but Document

- Do not engage publicly with trolls or attackers, engagement often escalates abuse.
- Take screenshots of threats, hate messages, or smear campaigns, including usernames, timestamps, URLs.

2. Activate Support Systems

- Notify trusted allies or digital security responders like DPI.
- Report the harassment to platforms (Twitter/X, Facebook,TikTok) and local support networks.
- Request rapid legal and psychosocial support, especially for gendered or doxxing attacks.

3. Trace & Block

- Use tools like WhoIs lookup to trace domain or IP-based threats with technical support.
- Use social media tools to limit exposure to harassment:
  Twitter/X: mute or block accounts, filter notifications
  Facebook: restrict or block users, adjust privacy settings
  Instagram: hide offensive words, enable comment filters, block accounts

Psychological Support & Self-Care

1. Healing and Building Psychological Resilience

Online harassment can be traumatic. HRDs are encouraged to:

- Take temporary breaks from triggering platforms.
- Speak with trauma-informed counselors or peer groups. (See Annex 1)
- Document harm not just for evidence but as a step toward healing and advocacy.

Strategic Legal and Advocacy Response

1. Know the Law

- Familiarize yourself with Uganda's Computer Misuse Act, 2022 [15] (often weaponized), Anti-Pornography Act (2014)[16] and the Data Protection and Privacy Act (2019) [17], rarely enforced, but still relevant for advocacy.

2. File Legal Complaints

- Work with trusted lawyers or legal CSOs to explore options such as: Cease-and-desist notices, Filing harassment or defamation cases, Seeking protection orders for repeat online stalkers.

3. Strategic Campaigning

- When appropriate, work with networks to publicize abusive incidents, leveraging:
- HRD Coalitions in Uganda (See Annex 1)
- International mechanisms (UN Special Rapporteurs on Freedom of Expression and HRDs)

Tailored Tips for Activists,HRD, Journalist's Organisations and Forums.

Digital Safety Training

Offer regular workshops for HRDs, activists, and journalists on:

- Secure communications
- Threat modeling
- Responding to doxxing and disinformation

Community Moderation Models

Build collective moderation plans for online spaces—e.g., shared admin duties, joint protocols for handling abuse in activist networks.

Safe Reporting Channels

Create or link to platforms where HRDs can anonymously report digital threats and receive support like:

- DPI seek support tab on website

15. https://nita.go.ug/laws-regulations/computer-misuse-amendment-act-2022
16.https://bills.parliament.ug/attachments/The%20Anti-pornography%20act,%202014.pdf
17.https://www.nita.go.ug/sites/default/files/2021-12/Data%20Protection%20and%20Privacy%20Act%20No.%209%20of%202019.pdf

3. Physical and Financial Monitoring & Surveillance

Trends show that digital surveillance of activists and HRDs has, in some cases, escalated into physical monitoring and targeting. Individuals have been shadowed near workplaces, homes, or during activities in the field, sometimes leading to abductions and enforced disappearances by security-linked officials and plainclothes men using unmarked, dark-tinted vehicles locally known as "drones."

Civil society organizations have also reported financial surveillance, including scrutiny of institutional accounts and personal transactions of NGO leaders and staff. For example, in 2024, during the **"March to Parliament"** protests against corruption, the financial statements of Chapter Four Uganda, which was providing legal aid to detained protesters, were leaked on X (formerly Twitter).

Such surveillance not only disrupts legitimate operations but also contributes to a climate of intimidation and self-censorship. This section offers practical safety measures and response strategies to mitigate these risks and enhance organizational and personal resilience.

Preventative Safety Measures & Response Strategies

Against Physical Surveillance

1. Routine Variation

- Avoid predictable travel routes and times.
- Use different transport modes when possible.

2. Safe Meeting Protocols

- Hold sensitive meetings in secure, private, or neutral spaces.
- Use "no phone"rules during sensitive meetings to prevent tracking or eavesdropping

3. Surveillance Awareness Training

Train HRDs to identify:

- Unmarked or tailing vehicles and motorcycles.
- Plainclothes officers or informants.
- Surveillance devices like CCTV, drones, pens, spectacles/ sunglasses and lapels.

4. Strengthen Physical Security

- Install CCTV, motion-sensor lights, or basic alarms at offices and homes.
- Keep a security logbook for suspicious visitors or incidents.

Against Financial Surveillance

1.Separate Personal & Organizational Finances

- Maintain separate accounts for organisational funding and personal income.
- Avoid using personal mobile money lines to receive grants or donor funds.

2. Secure Financial Communications

- Use encrypted platforms (e.g., Signal, ProtonMail) to share financial info or bank details.
- Avoid discussing sensitive transactions over unprotected calls or SMS.

3. Transparency with Oversight, Not Exposure

- Maintain proper financial records for legitimate audits—but do not overshare donor or beneficiary lists in public forums or online.

4. Engage Financially Literate Partners

- Work with accountants or finance officers who are familiar with NGO compliance laws and political risk management in Uganda.

Response Strategies When Under Surveillance

Physical Surveillance

1. Confirm, Don't Assume

- Cross-check incidents with trusted colleagues to confirm you're being followed or watched.

2. Document and Report

- Discreetly record or photograph surveillance evidence when safe.
- Report persistent surveillance to HRD protection organisations or legal support groups.

3. Engage Trusted Security Focal Points

- Inform a designated protection contact or legal advisor.
- Activate a relocation or safe house plan if threats escalate.

Financial Surveillance

1. Secure At-Risk Beneficiaries

- Protect the identities of partners, clients, or grantees that could be targeted due to funding links.

2. Legal Preparedness

- Be ready to respond to questions from the NGO Bureau, URA, or banks with documented, lawful transactions.
- Work with CSO legal coalitions to preempt illegal freezes or seizures of assets.

3. Reputation Defense

- If financial attacks like smears about foreign funding go public, coordinate a calm, fact-based response with donor support and aligned civil society.

Psychosocial & Organizational Resilience

- Create internal wellbeing systems in form of check-ins and or retreats for HRDs under stress due to surveillance.
- Integrate collective risk mapping and scenario planning in team activities.
- Encourage low-profile lifestyles to reduce unnecessary exposure of assets or habits.

4. Increased scrutiny of NGOs, their Leaders and Restrictive Laws

Increased scrutiny and the use of restrictive laws have become recurring threats against activists, human rights defenders, and civil society organizations in Uganda. Authorities have frequently applied Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) legislation selectively to target NGOs, often under the pretext of protecting financial integrity.

Even the overarching legal framework governing NGO operations, the NGO Act (2024) [18] has been criticized for its broad and vague provisions, which enable arbitrary interpretation and enforcement.

This trend has manifested in unauthorized raids, cordon-and-search operations, and the freezing of bank accounts on unsubstantiated claims of illicit financial activity. Other administrative actions include deregistration, denial of operational permits, and the introduction of overreaching regulations that further shrink civic space.

These measures not only disrupt legitimate NGO operations affecting service delivery to beneficiaries and partners but also threaten the broader freedom of association and the vital role civil society plays in holding duty bearers accountable.

18. Non-Governmental Organisations (Amendment) Act, 2024. /https://bills.parliament.ug/attachments/Non-Governmental%20Organisations%20(Amendment)%20Act,%202024.pdf

Notable Incidents:

2016

- Controversial passing of the NGO Act
- Raids on the offices of ActionAid Uganda and the Great Lakes Institute for Strategic Studies (GLISS), followed by t which granted discretionary powers to the NGO Bureau and included vague terminology. [19]

2017

- Raids on the offices of ActionAid Uganda and the Great Lakes Institute for Strategic Studies (GLISS), followed by the freezing of their bank accounts over alleged suspicious transactions. [20]

2021

- Government-ordered closure of multiple NGOs over alleged compliance irregularities. [21]

19. Implications of the NGO Act, 2016 on the Right to Freedom of Association in Uganda: A Case Study of ActionAid Uganda. Makerere University School of Law. https://makir.mak.ac.ug/items/a60750e4-f4aa-4476-ac4a-aa2886daf55f
20. Bank of Uganda Freezes ActionAid Accounts. https://www.monitor.co.ug/uganda/news/national/bank-of-uganda-freezes-actionaid-accounts-1722098
21. Uganda Suspends 54 NGOs. https://www.dw.com/en/uganda-suspends-54-ngos-in-clampdown/a-58924792

Preventative Safety Measures & Response Strategies

Know the Law:
» Familiarize yourself with key laws such as the Anti-Money Laundering Act, the Countering the Financing of Terrorism Act, and the NGO Act (2024).
» (Note: Following recent amendments, NPOs are no longer classified as "accountable persons" under the AML Act.)

Ensure Full Compliance:
» Submit all required returns and reports on time, including PAYE, NSSF, and other applicable taxes. Maintain accurate financial records to reduce vulnerability to compliance-based targeting.

Renew Permits Promptly:
» Apply for renewal of permits with NGO Bureau permits before expiry to avoid administrative penalties or suspension.

Secure Data Storage:
» Use cloud-based storage systems with strong encryption, and keep minimal local copies of sensitive data. Restrict access to essential personnel only.

Build Coalitions and Networks:
» Engage with NPO coalitions, human rights networks, and legal support organizations to share early warnings, advocacy updates, and coordinated responses.

Continuous Advocacy and Policy Engagement
» Develop policy papers and engage in sustained advocacy efforts. Defenders Protection Initiative (DPI), together with the NPO Working Group on FATF, successfully lobbied for the removal of NPOs from the list of accountable persons [22] under the Anti-Money Laundering Act (AMLA).

Response Strategies

Strategic Litigation:
» Challenge unlawful restrictions, arbitrary deregistration, or asset freezes through the courts to set legal precedents protecting NGO operations.

Legal and Financial Support Mechanisms:
» Maintain contact with trusted human rights lawyers and pro bono legal aid networks. Establish a rapid response fund to cover legal fees or operational disruptions.

Public Communication and Solidarity:
When safe and with leadership consensus, issue press releases or coordinate with civil society alliances to expose unlawful targeting and build solidarity.

Documentation and Reporting:
Document all incidents of raids, harassment, or financial freezes. Report to Uganda Human Rights Commission, regional mechanisms, or international partners for accountability and a

22. NGOs Push for Rapid Implementation of Anti-Money Laundering Act Amendments.https://chimpreports.com/ngos-push-for-rapid-implementation-of-anti-money-laundering-act-amendments/

5. Misinformation and Disinformation

Misinformation: False information shared without malicious intent.
Disinformation : Deliberately false information intended to deceive.

In Uganda, misinformation and disinformation campaigns are increasingly weaponized to discredit, isolate, and endanger activists, journalists, and human rights defenders (HRDs). These coordinated efforts often involve fabricated narratives, doctored images, or manipulated videos aimed at undermining the credibility and legitimacy of HRDs, particularly those involved in governance, anti-corruption, and civic space advocacy.

As digital spaces become more central to activism and journalism, misinformation, online abuse, and surveillance must be recognized not only as technical threats but also as strategic tools of repression. This section provides practical guidance for detecting and mitigating disinformation, responding to smear campaigns, and strengthening digital resilience for Uganda's frontline defenders.

Increased Stigmatisation and Polarisation

False or misleading narratives about HRDs/activists—shared widely through social media, radio, Vlogs, and other platforms—contribute to the increasing stigmatisation of defenders as "troublemakers," "foreign agents," or enemies of cultural/national values. These narratives often exploit existing social divides, including political, tribal/ethnic, or religious tensions, to turn public opinion against HRDs.

Increased Scrutiny, Criminalization and Restrive Laws

State and non-state actors have strategically used disinformation campaigns to justify restrictive laws, policies, and crackdowns on NGOs. False narratives about HRDs being foreign agents and thugs (Bayaye) promoting immorality/ or destabilising society have been used; to justify increased surveillance and monitoring, strict administrative demands, misapplication of laws and criminalization of legitimate HRD/ NGO work.

Reputational Damage and Personal Risk

Persistent misinformation and disinformation erode the credibility, legitimacy, and personal reputations of HRDs and their organizations which has forced many into self-censorship and withdrawal from activism and advocacy work – further shrinking civic space.

Preventative Safety Measures & Response Strategies

Preventive Safety Measures

1. Build a Verified Online Identity

- Maintain consistent branding across platforms in terms of name, logo and handles to help audiences distinguish your authentic voice.
- Use verified accounts or clearly link all official channels to your organisation's website or email signature.

2. Pre-bunking & Proactive Messaging

- Publish clear, accessible content about your work, partners, and values so disinformation has less power to distort facts.
- Use FAQs, bios, and press kits to proactively inform the public and media.

3. Team Readiness & Digital Literacy

- Train your team to:
  - Detect manipulated content in form of deepfakes and altered images.
  - Understand troll behavior and bot amplification
  - Identify coordinated smear campaigns
- Designate a rapid response focal person for digital reputation issues.

4. Community Resilience Building

- Cultivate informed and supportive audiences who can help counter false narratives with truth.
- Partner with trusted journalists, media houses, and CSOs to create a united response.

Real-Time Response Strategies

1. Monitor and Document Disinformation

» Use free or low-cost tools like CrowdTangle, TweetDeck, Google Alerts, or WhatsApp monitoring bots to track where misinformation is spreading.
» Screenshot, archive, and timestamp misleading content for reference or legal action.

2. Issue a Swift, Calm Rebuttal

» Prepare a neutral, fact-based response correcting false claims. Avoid emotional or combative language.
» Share your response on multiple channels: website, social media, newsletters, and aligned networks.

3. Amplify the Truth Through Allies

» Ask partner organizations, media allies, or influencers to repost your rebuttal or speak out on your behalf.
» Use visual content including infographics, short videos, and quote cards to increase reach and impact.

4. Platform-Level Reporting

» Report harmful or misleading posts using the social media platform's abuse/reporting features e.g., misinformation, impersonation).
» For verified disinformation, request takedowns through CSO coalitions, lawyers or media monitors.

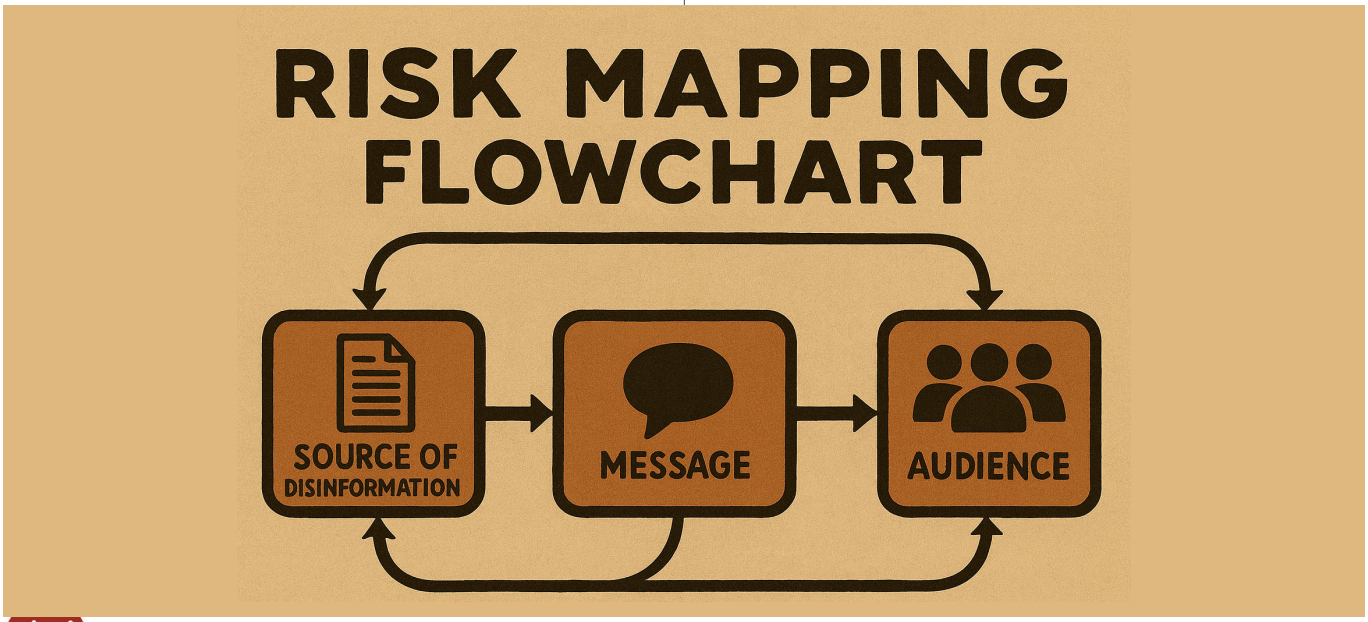
Long-term Response Strategies

1. Narrative Security Planning

» Include narrative risk mapping in your safety audits:
  » Who might spread disinformation about you?
  » What are likely messages and goals?
  » What audiences are most vulnerable to manipulation?

2. Strategic Media Engagement

» Build long-term relationships with independent journalists and editors who can counter misinformation with verified reporting.
» Offer regular briefings or updates to ensure the media understands your work.



Annex 1. Resources

Emergency Response	
Defender Protection Initiative (DPI)	+256 39 2201102 Scan QR code on the last page to connect with a protection officer.
Defend Defenders	+256 707 020086
Front Line Defenders	Secure Contact Form +353-1-210-0489
Uganda Police	**Toll-Free :** 0800 300 102, 0800 122 291 / 0800 996 999, 0800 999 399 **Emergency:** 999/112 **Kidnap Desk:** 0800 199 991, 0800 199 992 **WhatsApp Desk:**+256 779 999 999
Legal Support	
Haki Defenders	jambo@hakidefenders.org
Chapter Four	+256 200 929990
Uganda Human Right Commission	Regional Offices
Human Rights Network For Journalists-Uganda	+256 800 144 155
Digital Security Support	
Haki Defenders	jambo@hakidefenders.org
Chapter Four	+256 200 929990
Uganda Human Right Commission	Regional Offices
Human Rights Network For Journalists-Uganda	+256 800 144 155

Secure Reporting Channels for Women	
Women Human Rights Defenders Network -Uganda	Helpline : +256756457038
Pollicy	+256 708310397, +256 760193143
Uganda Women's Network (UWONET)	info@uwonet.or.ug

Secure Reporting Channels for Journalists	
Witness Radio	www.witnessradio.org
Human Rights Network For Journalists-Uganda	+256 800 144 155

HRD Coalitions	
National Coalition of Human Rights Defenders – Uganda (NCHRD-U	info@hrdcoalition.ug

Annex 2. Self Assessment

1. Do you use a VPN when accessing the internet, especially for activism-related activities?
   Always ☐ Sometimes ☐ Never ☐

---

2. Do you use a pseudonym or alternative account for online activism?
   Yes, consistently ☐ Occasionally ☐ No ☐

---

3. Do you regularly update your passwords and use two-factor authentication (2FA)?
   Yes, for all accounts ☐ Only for some accounts ☐ No ☐

---

4. Do you back up your sensitive data on a secure external drive or cloud service?
   Yes, regularly ☐ Sometimes ☐ No ☐

---

5. Are your web hosting and database services managed by a foreign provider to avoid local surveillance?
   Yes ☐ No ☐ Not applicable ☐

---

6. Do you use alternative financial channels (e.g., trusted partners' accounts) for transactions to minimize surveillance risks?
   Yes ☐ No ☐ Not applicable ☐

---

7. Have you considered opening a foreign bank account as a backup in case of local account restrictions?
   Yes ☐ No ☐

Interpreting Your Results

- Mostly "Yes" Answers - You have strong security measures in place. Continue staying vigilant and updating your strategies.
- Mostly "Sometimes" Answers - You have some security measures, but there are areas for improvement. Strengthen your weak spots.
- Mostly "No" Answers - You are at high risk. Take immediate steps to enhance your security based on the recommended measures.

DEFENDERS PROTECTION INITIATIVE

Plot 5, Kintu Alley,
Kulambiro Ring Rd,
Kampala

communications@defendersprotection.org

+256 392 201102

@defprotection

Defenders Protection Initiative

Defenders Protection Initiative