



BUILDING CAPACITY FOR MONITORING AND DOCUMENTING HUMAN RIGHTS VIOLATIONS DURING INTERNET SHUTDOWNS

A ZIMBABWE NEEDS ASSESSMENT REPORT



About Report

Internet shutdowns are on the rise. In the past few years, an escalation of this blunt censoring practice has affected different regions of the world including Africa. Shutdowns have become one of the most excruciating repressive tactics that governments use to restrain civic participation and free flow of information. This report intends to provide a launch pad which can guide Human Rights Practitioners (HRPs) or Human Rights Monitoring Organizations (HRMOs) with circumventions tactics that can be utilized during blackouts. The purpose of this assessment seeks to evaluate the efficacy of strategies used by HRPs/HRMOs for communicating during blackouts. The goal of this project envisages to see a Zimbabwean Civil Society that is prepared to document and monitor human rights violations without hiccups during internet shutdowns. To achieve that, the researcher conducted a needs assessment which was responded to by 83 HRPs in Zimbabwe, with a wealth of experience in human rights monitoring.

The scope of the assessment focused on Zimbabwe, but the author considers some of the findings and recommendations useful to other African countries. It is important to note that the results described in this report are not representative of wider population of HRPs in Zimbabwe. As such, we implore you to understand that percentages used throughout this report represent a relative purposive small non-generalizable sample size.

Building from these efforts, we would welcome reproduction of such work which is prudent for HRPs in Zimbabwe to technically appraise their efforts and consider conducting needs assessments tied to mitigating online censorship, strategic litigation on shutdowns, mitigating internet shutdowns, detecting internet shutdowns and development of internet shutdown action plans.

Authored and designed by;
Bright Thulani Chimedza

Special thanks to all of the experts and civil society representatives who participated in the survey and contributed to this assessment.

PUBLISHED DATE: 10 January 2024

CONTENTS

01.

INTRODUCTION

02.

BACKGROUND

03.

METHODOLOGY

04.

KEY FINDINGS

05.

COMPREHENSIVE FINDINGS

State of Preparedness

Likelihood Probabilities

Examining communication strategies

Capacity Pedigree and Internal Appraisal

Communication strategies/Contingency pathways

Familiarity with circumvention tools

Reliance on tradition communication tactics

Collaboration with Digital Rights Practitioners

Challenges experienced

Role of the Donor Community

06.

CONCLUSION

07.

RECOMMENDATIONS

08.

APPENDIX

INTRODUCTION

Internet shutdown is a growing menace curtailing freedom of expression on the internet and other human rights. For this report, the researcher will rely on technical definition of internet shutdown that was developed at the [RightsCon Summit in Brussels in 2016](#) which conceptualised an Internet Shutdown as;

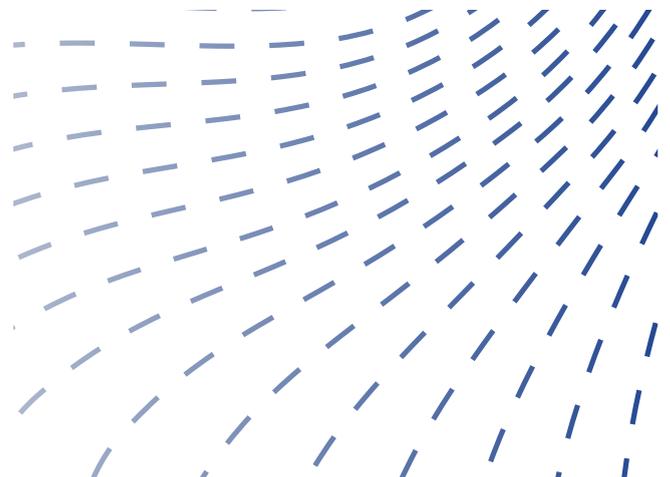
“

a deliberate disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information

”

In most cases such blackouts may involve blocking or restricting access to certain websites, social media platforms, throttling internet speeds or completely shutting down internet access. Zimbabwe is not spared from some of these tactics, and this has predominantly been experienced when opposition political parties or civil society organisation intend to advance or practice their right to freedom assembly enshrined in the constitution. By limiting the flow of information, it is perceived that responsible authorities aim to curb the organisations and coordination of protests, as well as prevent the dissemination of information that may undermine their authority. Often times, the Zimbabwe government misconstrues the meaning of section 6 of the [Interception of Communications Act](#) when they authorise blanket bans which are ultra vires because they are inconsistent with the Constitution, particularly [section 61](#) on freedom of expression.

Nevertheless, these actions do not only violate the law but also infringe international statutes such as the [UN Joint declaration on freedom of expression and conflict situations](#) and [Declaration of Principles on Freedom of Expression and Access to Information in Africa](#). The focus of this report, however, is not to assert the illegality of shutdowns to policymakers or regional bodies, but rather to understand how HRPs in Zimbabwe respond to internet shutdowns and the strategies they employ to circumvent, document and monitor human rights violations during shutdowns. This research provides an understanding for a coalition of digital rights CSOs to understand what resources and needs are required in order to better fight back against shutdowns.



BACKGROUND



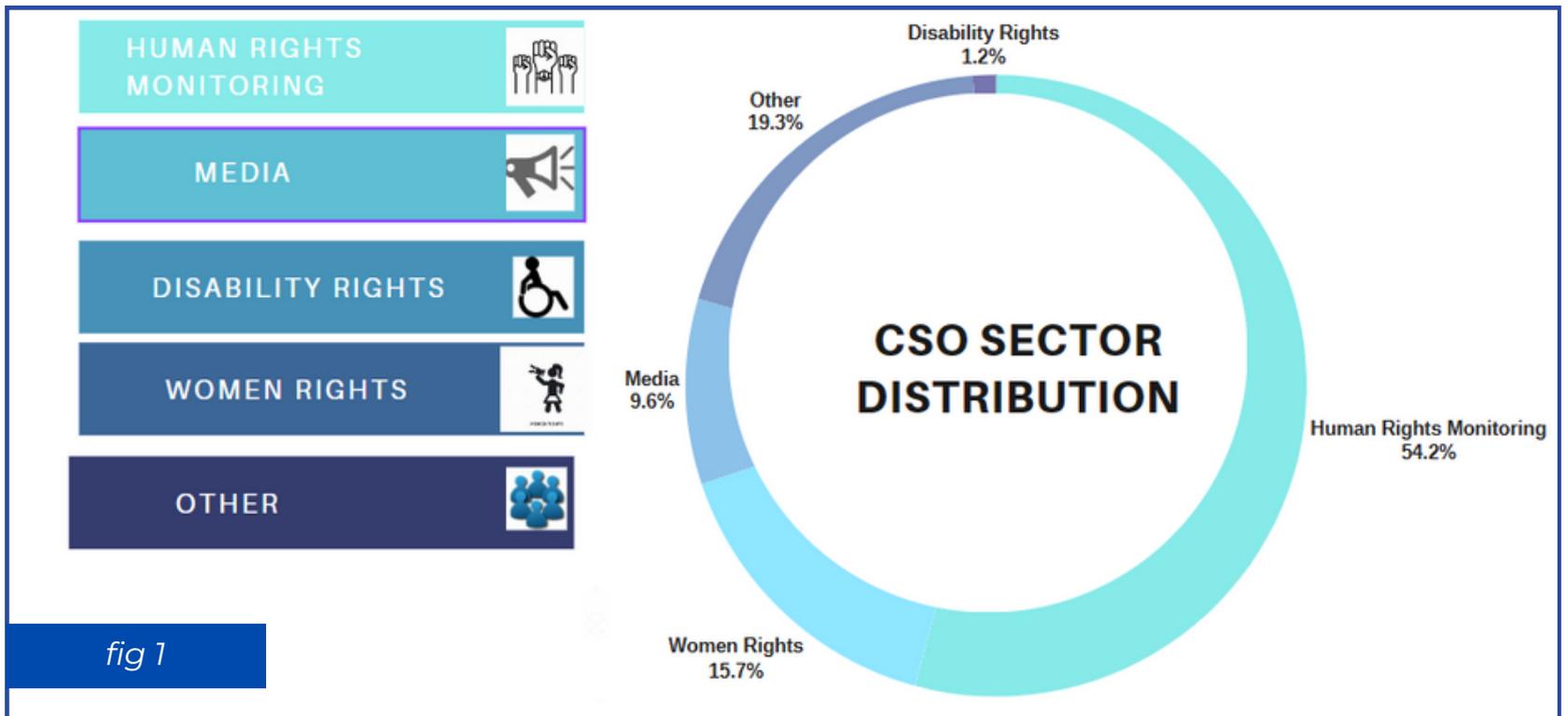
In Zimbabwe, internet shutdowns arguably gained prominence in July 2015 amidst National Stay Away protests against government corruption and economic mismanagement. During this time, the Zimbabwean government was alleged of implementing internet disruptions and partially blocking of social media platforms, including WhatsApp. Similarly, In July 2016 ahead of a planned nationwide protest against the government's economic policies, Zimbabwe experienced targeted internet disruptions and slowdowns. Access to social media platforms and communication apps was significantly hampered, limiting the ability of citizens to organize and share information. In the aftermath of the 2018 harmonised elections, protests and violence erupted, leading to intermittent disruptions of internet connectivity. Access to social media platforms such as Facebook, Twitter, and WhatsApp were temporarily blocked. Another shutdown was experienced in January 2019 and this black out lasted for several days. The government ordered a nationwide blackout following widespread protests against fuel price increases and economic hardships. During this shutdown, access to social media platforms and the internet as a whole was completely blocked. In 2022, Network data from NetBlocks confirmed a significant slowing of internet service for many users in Zimbabwe on Sunday 20 February 2022, as a major political opposition rally was held in Harare. The incident impacted multiple operators and prevented live streaming from the Yellow Sunday demonstration by the Citizens Coalition for Change party, which sought to unseat the ruling ZANU–PF.

The following month, on the 13th of March 2022, a series of disruptions were experienced amid further opposition demonstrations but this time around metrics confirmed that the disruptions occurred at the backbone which serves each provider, and not at the cell towers due to congestion as claimed by some sources. Ahead of the 2023 harmonised elections, various organisations reported that internet connectivity had been affected in Zimbabwe. NetBlocks for example, reported that the quality of internet access was degraded on 22 August 2023, affecting millions of individuals who rely on the internet for accessing information.

The aforementioned narrative reveals that Zimbabweans have experienced 8 notable internet shutdowns to date and it somewhat suffices to claim that a year or two cannot pass by without Zimbabweans experiencing either throttling or an internet shutdown. Strategic litigation has been one of the circumvention advocacy interventions which Human Rights Practitioners (HRPs) in Zimbabwe have resorted to and it relatively worked in selected cases. In addition to these concerted legal actions, to better document and prepare for shutdowns, it becomes pertinent for HRPs in Zimbabwe to come up with other innovative ways of documenting human rights violations during blackouts and develop robust communication/contingency strategies that can be utilised in anticipation of future shutdowns.

METHODOLOGY

The author employed a largely qualitative study. The researcher utilised an evidence-based approach to ensure that the information presented is accurate and reliable. The inclusion criteria targeted HRPs working in the Civil Society organisations in Zimbabwe, who are heavily involved in monitoring human, women, media, and disability rights. The data presented in this survey was collected via a web-based survey distributed to HRPs between 21 November and 10 December 2023. The survey was open to any of these groups, but 4 semi structured interviews were extended only to HRMOs that have a niche in documenting and monitoring human rights violations in near-real time.



The interviews served as a triangulation pathway to gain a deep understanding of responses shared via the survey. In total, the survey received 83 responses who responded to similar questions and their reflections should be seen to be anecdotal. These respondents were drawn from practitioners working in the human rights monitoring sector, disability sector, media, women rights sector and others. As for the survey questions, they were coined in a way that ensured the assessor acquaints himself with a narrowed inquiry on:

- 1)How internet shutdowns impede the operations of HRPs,
- 2)HRPs state of preparedness
- 3)Training acquired
- 4)Tools and apps used during shutdowns
- 5)Shutdown predictions
- 6)Challenges associated with the strategies
- 7)Communication strategies
- 8)Collaboration with technocrats
- 9)Role of the donor community and the likelihood of a shutdown in 2024.

All questions were optional, and HRPs could choose to answer anonymously.

KEY FINDINGS

92.6%

of the respondents considered the development a toolkit as a major step towards enabling HRP to circumvent internet shutdowns during their monitoring and documentation efforts.

91.6%

of the respondents believe that human rights monitoring organisations (HRMOs) need to strengthen their circumvention strategies

65.1%

Of the HRPs surveyed for this report believe that Zimbabwe is likely to experience a shutdown in 2024.

65.1%

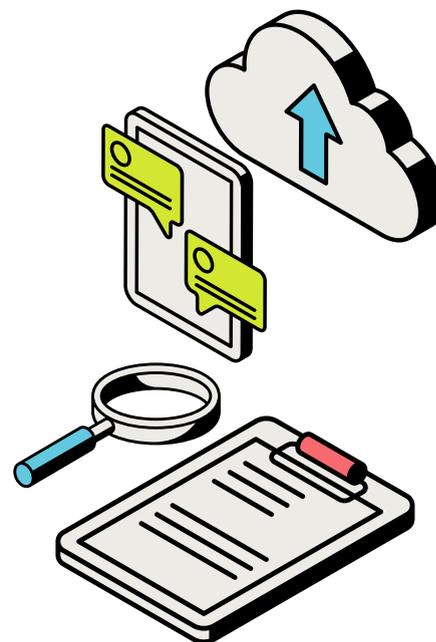
of the respondents claimed that they are working for organisations without communication strategies designed to overcome internet shutdown challenges.

64%

of the HRPs indicated that they do not know organisations that provide technical support on circumventing internet shutdowns.

50.6%

of the HRPs do not invest in predicting internet shutdowns and do not have experience in this field.



COMPREHENSIVE FINDINGS

STATE OF PREPAREDNESS AND ASSOCIATED CONSEQUENCES ON INTERNET SHUTDOWNS

All the respondents unanimously averred that internet shutdowns impede the operations of their organizations. They all have experienced restrictions several times in the past and this hindered the free flow of information from monitors to the HRMOs and vice versa.

Findings also revealed that most organisations are relying on WhatsApp and other mobile applications as a mode of communicating and data gathering channel. As such any form of shutdown, either full internet blackouts, platform-specific blocking, and bandwidth throttling will deter HRPs from collating human rights violations in near-real time. Seized with these predicaments, 92.6% of the respondents indicated that development of a toolkit that guide HRPs on how to monitor and document human rights violations during internet shutdowns is of paramount importance. The essence of this toolkit stems from findings which revealed that 8.4% of the HRPs are working for organisations without robust circumvention strategies, 43.4% believe they the strategies should be strengthened and 48.2% perceive the strategies as weak.

Moreso, findings reflected that HRMOs and HRPs are not prepared for shutdown. This view is validated by statistics from the survey which reveal that 50.6% of the HRMOs do not invest in predicting shutdowns when they are working on their contingency plans, scenario mapping and risks matrixes. Participants also indicated that they do not use digital tools during these processes and rely mostly on internet speed as a determinant factor. This suggests that there is a greater number of HRMOs in Zimbabwe that do not know how to use network measurement tools and technical datasets such as OONI probe, OONI run, IODA Dashboard, NDT speedtest, RIPE atlas, Censored planet data, google transparency reports to mention a few.

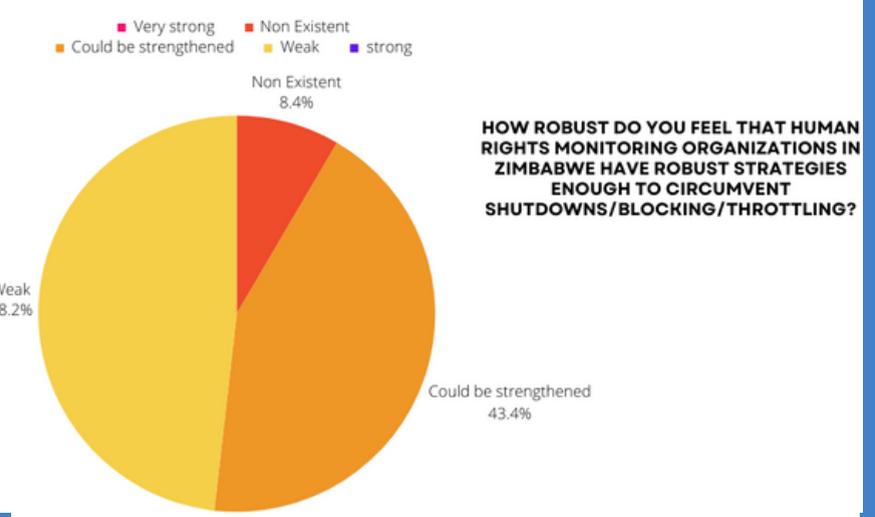
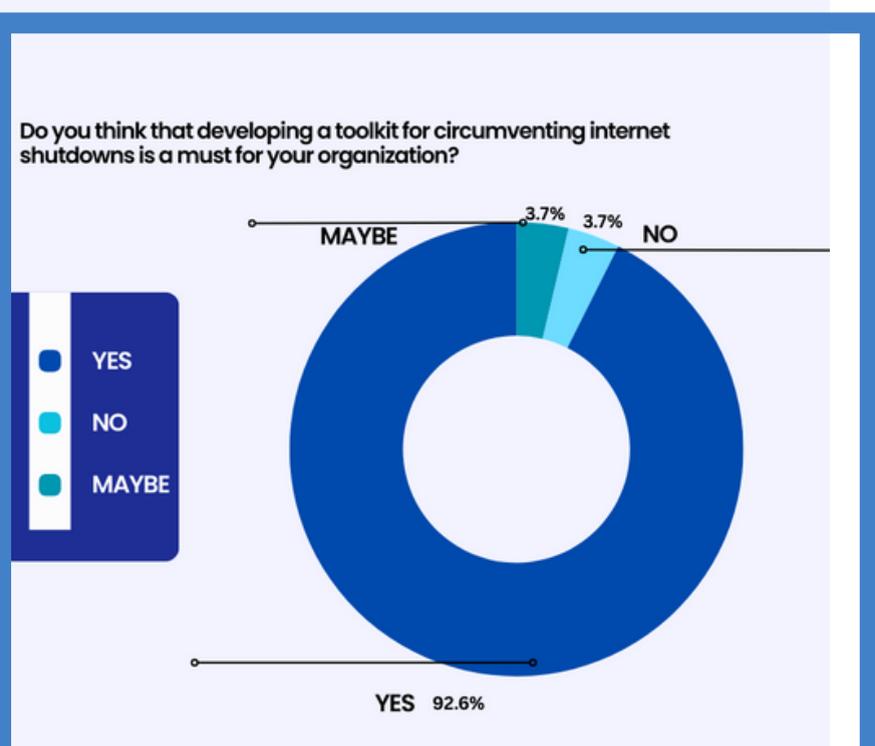
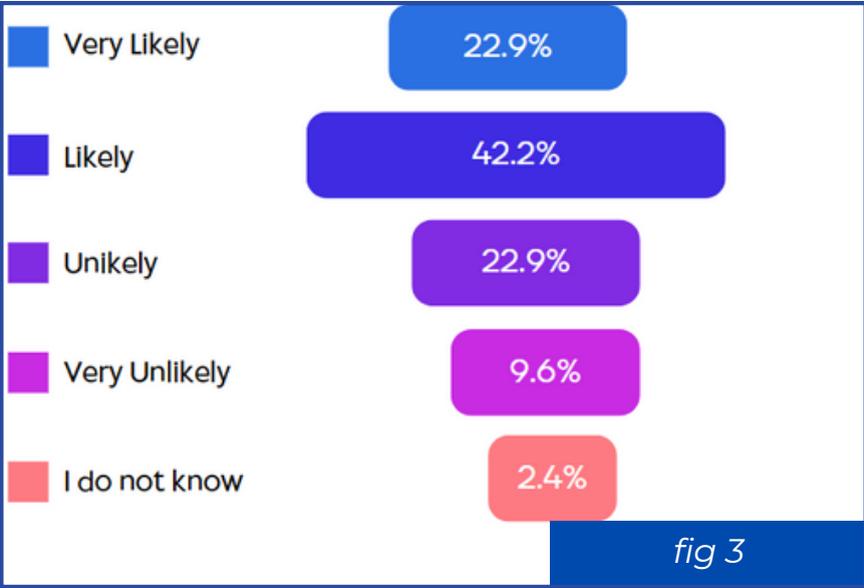


fig 2

LIKELIHOOD OF A SHUTDOWN IN THE YEAR 2024 IN ZIMBABWE

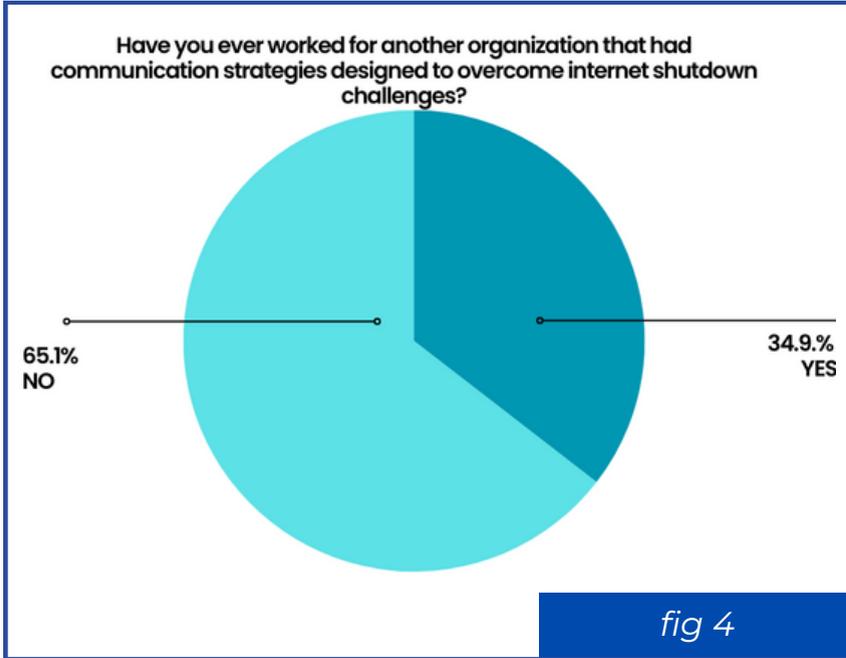
Organisations that monitor and document human rights violations were convinced that the possibility of a shutdown in 2024 is very likely. 22.9% of these organisations claimed that they will not be surprised if Zimbabwe experiences a shutdown in 2024 and the possibility is very likely. 42.2% contended that the possibility is likely, 22.9% indicated that it is unlikely, 9.6% maintained that it is very unlikely and 2.4% of the respondents stated that they do not know. Broken down into two dimensions, 65.1% of the respondents believed that the possibility of an internet shutdown in 2024 cannot be ruled out and 32.5% stated the contrary. The former consider the fragile civic and political space as one of the salient indicators which will exert pressure on the government when faced with civic resistance and the latter believed that the government would use other reprisals detached from blackouts.

How likely do you think that Zimbabwe will experience an internet shutdown in 2024



ASSESSING THE STRENGTH OF COMMUNICATION STRATEGIES AND CONTINGENCY PATHWAYS

Findings suggested that most HRPs are working for HRMOs that do not have communication contingency manuals or handbooks that guide how they can document human rights violations during internet shutdowns. A majority of 65.1% of the respondents pointed out that they don't have communication manuals best suit to guide them on how they can communicate during blackouts. 34.9% indicated that, they have communication policies or manuals but despite the existence of these manuals they struggle to receive reports from their community monitors particularly those in marginalised areas. In the survey, those that claim to have communication strategies have an over reliance on SMS, physical verifications, and phone calls. These implies that HRMOs in Zimbabwe rely heavily on traditional ways of communicating and are somewhat found wanting when it comes to utilising modern shutdown mitigation data gathering tools and applications.



CAPACITY PEDIGREE AND INTERNAL PROCESS APPRAISAL

Reflections from the survey pointed out that HRMOs do not entirely have internal processes that look into internet shutdowns or offline communication. However significant efforts have been put in place by other HRMOs. This was revealed by 50.6% of HRP who have worked on internal processes tied to circumventing internet shutdowns, whilst 41% indicated the contrary and 8.4% and claimed that they are unaware of any internal processes that have facilitated in their respective organisations tied to internet shutdowns. Some of these internal processes include training of their monitors pre, during and post internet shutdowns. 50.6% of the respondents indicated that they do train their monitors and 49.4% of the respondents claimed that they do not provide training to their monitors. Most of the respondents from 50.6 percentage reside in Harare Province and the remaining 49.4% reside in other metropolitan provinces and they cited lack of support hence why they are lagging behind.

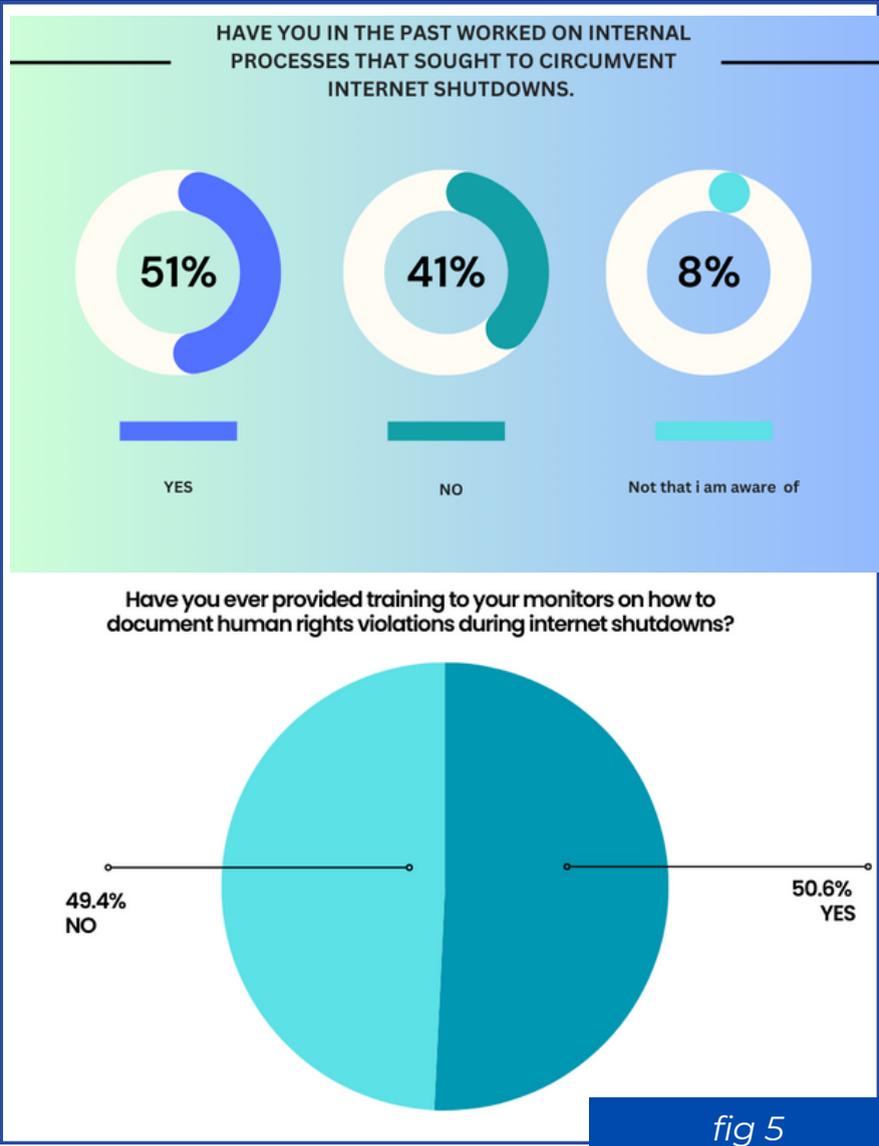


fig 5

HRPS IN ZIMBABWE ARE LAGGING BEHIND WHEN IT COMES TO USING MODERN CIRCUMVENTION TOOLS FOR DOCUMENTING HUMAN RIGHTS VIOLATIONS DURING BLACKOUTS.

HRPs were asked to list their familiarity with specific tools commonly used by HRMOs seeking to circumvent some degree of internet shutdown. Except for the strategy of using SMS services during a shutdown, respondents report being mostly unfamiliar with the other strategies and tools such as eyewitness atrocities, OTG, TELLA, F-DROID, Bridgefy, OONI-Probe. The researcher realised that eyewitness atrocities was mostly used by 21% of the respondents and when he randomly made follow up enquiries, requesting people to tell him more about their experience with eyewitness atrocities, he realised that the bulk of them did not know this application. Some later indicated by eyewitness atrocities 'I thought you meant physical verifications using the eye and I did not know that you were referring to a mobile application'. As such, this means that the number of people who have not used circumventions tools for sharing information might actually be higher than 64.2% as represented in this report. This reveals a salient discovery and a potential route of reform and future work, and it speaks volumes about capacity strengthening required for enabling HRMOs or HRP to document human rights violations during internet shutdowns independently.

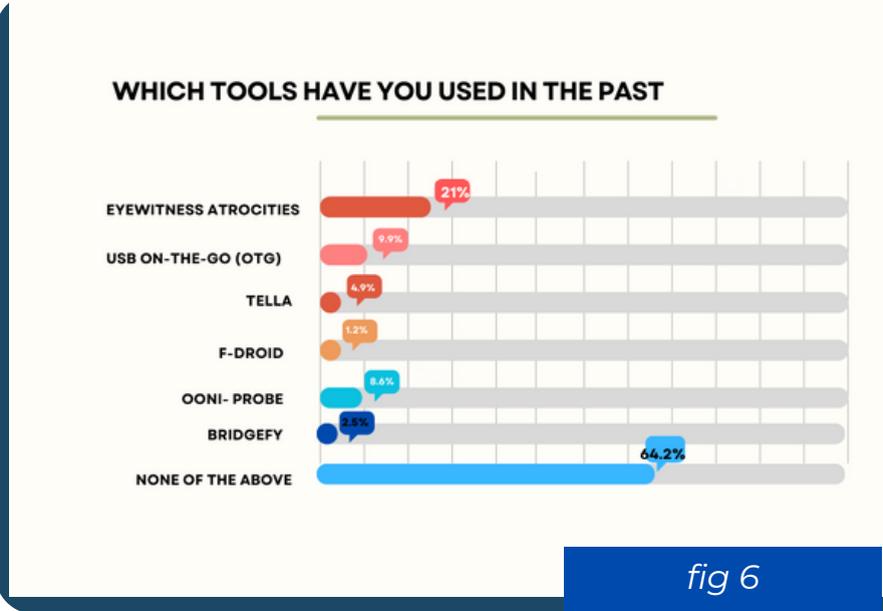


fig 6

HRPS IN ZIMBABWE ARE RELYING HEAVILY ON TRADITIONAL WAYS OF COMMUNICATING

An optional open-ended question was developed to allow participants to list the applications and tools they used during past blackouts. This exercise was responded to by 75 participants, and it presented different results contrary to what was gathered from the closed ended questions cited in fig6. Results from this activity hypothetically indicate that participants hardly use modern digital tools or modern communication channels. Out of the myriad of digital tools, applications and methods for communicating, only 5 ways of communicating were listed by the respondents. From the 5 methods, 39% indicated that they do not know any circumvention tools 21% used VPNs, 21% used SMS, 12% used calls, 5% used telegram, 1.13% used Bridgefy. The probable and logical explanation to this indicates that, HRP's in Zimbabwe admire using tools and applications that are user friendly and some even indicated that training on how to use other modern applications and tools should be upscaled.

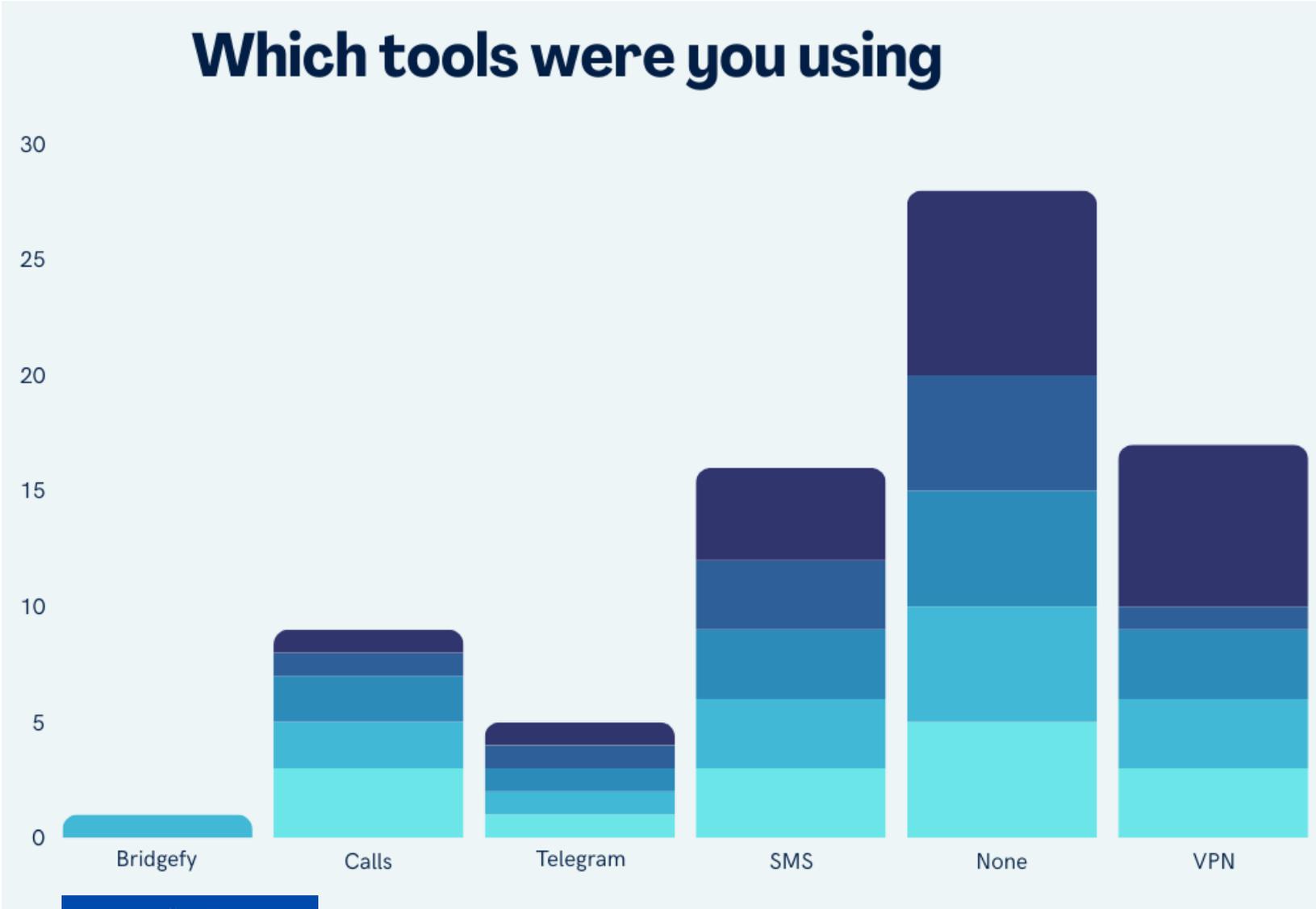


fig 7

HRPS DONT HAVE ACCESS TO INTERNET SHUTDOWN SUPPORT AND EXPERTISE

HRPs were given the room to list the number of organisations that provide technical expertise to them on circumventing internet shutdowns. Their reflections revealed that, HRMOs are not fully aware of organisations that provide training on circumventing internet shutdowns. 36% of the HRPs indicated that they do know organisations that provided technical support and 64% of the respondents stated that they do not know organisations that provide support, nor have they received technical support on circumventing internet shutdowns. The organisations that were enlisted for providing support are depicted below. Upon triangulation, the author later established that some of the organisations were wrongly cited. For example, Amnesty International Zimbabwe does not provide circumvention technical support, and this was later confirmed by one their staff members. This implies that there are few organisations which provide support on circumventing internet shutdowns in Zimbabwe. Nevertheless, MISA, SAHRDN and Digital Society Africa were commended for their efforts.

Are you aware of other organizations in Zimbabwe or SADC who could assist with technical support to monitor human rights violations during an internet shutdown.

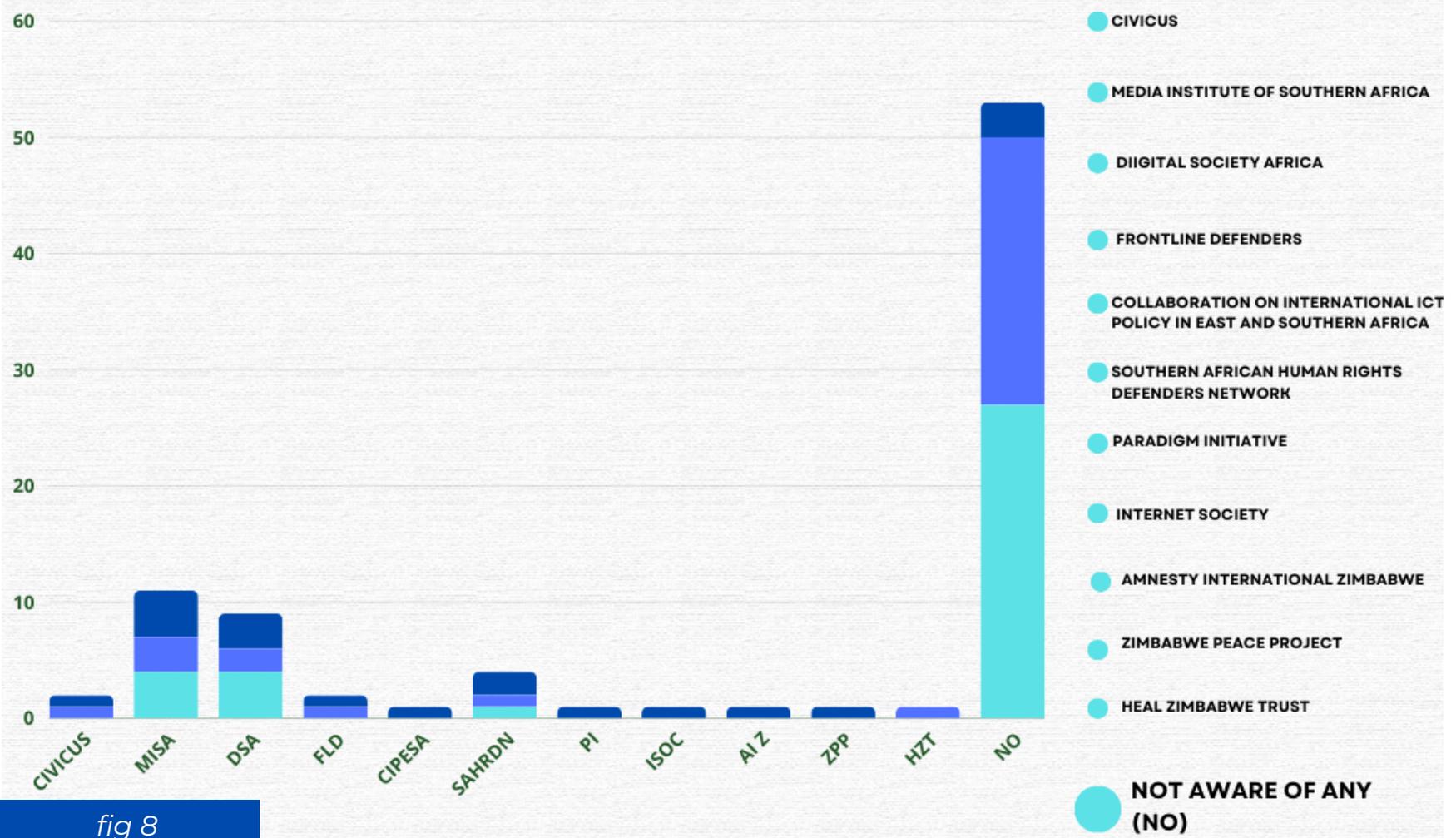


fig 8

Therefore, lack of technical rigor was captured as one of the reasons why HRMOs and HRPs were susceptible to shutdowns because they don't have strong circumventions strategies. From the survey 8.4% of the HRMOs indicated they don't have circumvention strategies, 48.2 % of the strategies are weak and 43.4% of the respondents cited that the strategies are there but have to be strengthened. None of the respondents believed that HRMOs have strong or very strong circumvention strategies.

CHALLENGES EXPERIENCED

The survey received 153 challenges which were experienced by respondents during internet shutdowns. The assessor used thematic analysis to understand these predicaments and succinctly provide 7 recurring themes drawn from the list. These challenges present a vivid picture of the struggles endured by HPRs during internet shutdowns and their reflections pinpoint areas where interventions should be deployed.

There was no Backup strategy.

MISA Zimbabwe sponsored Psiphon VPN) but communities did not know how to use the VPN and they ended up downloading cracked VPNs.

HRPS were of unaware of the alternative messaging applications to use that were not blocked.

PWDs especially the deaf were affected.

HRPS in marginalised areas felt isolated and vulnerable.

Covert human rights abuse increased and disinformation was rife due to intermittent flow on communication.

Curtailed freedom of assembly people could not mobilise and stand in solidarity.

Most of the findings also indicated that people failed to use VPNs during internet shutdowns, and some claimed that awareness and usage of VPNs among Zimbabweans is very low. Very few had VPNs on their phones during shutdowns and only 21% of the respondents indicated that they used VPNs during internet shutdowns in Zimbabwe. Despite downloading the app, most participants struggled to use the VPNs on their devices.

THE ROLE OF THE DONOR COMMUNITY

"In addition to the findings on HRP's shutdown advocacy, most of the respondents cited financial constraints as a key contributing factor to HRP's inability to circumvent internet shutdowns. The researcher then probed further to understand if HRP's believe that funding partners would be keen to support internet shutdown circumvention interventions. 40% of the respondents were pessimistic that the funding community will be interested in these projects, and they cited donor fatigue as one of the reasons. However, a significant 60% were optimistic that funding partners will be interested in these projects and some of the extracts are provided below.



The international human rights framework, emphasizes the importance of internet access and the protection of human rights online. Donors who align with these principles are more inclined to provide fundraising support to organizations addressing internet shutdowns. While there may be variations in the level of support from different donors, overall, there is a growing awareness and commitment within the donor community to provide fundraising support for advocacy strategies pertaining to internet shutdowns. This support stems from their recognition of the importance of upholding human rights, protecting civil liberties, and fostering global connectivity.



Yes, technology is an effective means of activism and the donor community is likely to have a keen interest in making sure people stay connected



Yes i think there are funders that are keen to support internet shutdowns advocacy and this is because internet shutdowns affect everyone across various sectors including education and health. There is therefore an opportunity to always ensure that various funders appreciate the importance of supporting the fight against internet shutdowns.



We worked in the past with Counter Part International supported by USAID.



The aforementioned extracts indicate that HRP's are optimistic that support from donor community will be essential for empowering HRP's to counteract and circumvent shutdowns. The general understanding from the survey advances the view that, without donor support most of the strategies and interventions will not attain the desired outcomes and goals.



CONCLUSION

Reflections from this assessment indicate that internet shutdowns in Zimbabwe are frequent, come in different variations and the magnitude is determined by tensions on the ground. The contextual assessment revealed that shutdowns occur during times of political unrests or protest, leading to restricted access to information and communication platforms. During such times, the lack of internet access inhibits HRPs ability to document human rights violations in near-real time. Participants unanimously agreed that, if Zimbabwe is to experience a shutdown soon, the country will be plunged in an information blackout which will be exacerbated by lack of awareness, technical expertise and support to circumvent shutdowns when they occur.

Building from previous advocacy efforts, this needs assessment identified a clear need for circumvention resilience and prioritisation of digital advocacy especially in marginalised areas of Zimbabwe. Findings revealed that, in these areas, there is little support and investment that has been extended to prepare community members on how to circumvent government-imposed internet disruptions. As such, without well-choreographed and systematic pushbacks, government-imposed shutdowns will continue to cripple HRMOs and HRPs monitoring efforts.

Through the collection and analysis of a diverse range of perspectives collected, this needs assessment should be considered as a steppingstone for HRPs and HRMOs to strengthen and curate nuanced models, that will enable them to document human rights violations during internet shutdowns. As a researcher, the author of this report will continue to examine the prevailing context with the intention of providing exclusive findings as and when required.



RECOMMENDATIONS

1

HRMOs should consider what steps they can take in advance to prepare for internet shutdowns before they occur and a lot of trainings for trainers for the following recommendations should be considered. By the time a government implements a shutdown, it is often too late to adapt and download circumvention tools and applications. Therefore, HRMOs should closely work with digital rights organisations that have expertise in predicting shutdowns. Once indications reveal a looming shutdown, HRPs should lobby the government desist from shutting down the internet. These actions be complemented by advocacy work targeting the government using tools such as OONI's Cost of Shutdown Tool (COST) which shows the economic impact of an internet shutdown.

2

HRMOs should run campaigns imploring HRPs and citizens to download circumvention tools way ahead of time. Prior doing so, HRMOs should store their circumvention apps in Android Package Kits (APK) files which can be shared from device to device by text, Bluetooth, or email. Alternatively, HRMOs can come up with offline simulations which provide step by step instructions and one example is the [Internet Shutdown game](#). As such, having a number of applications would give HRPs options, in the event that some of the tools will not work. Over and above for this to work, digital advocacy trainings should be facilitated over time to ensure that communities are familiar with these circumvention strategies. Mostly importantly, HRPs should use tools and applications that are permissible by law in their respective areas.

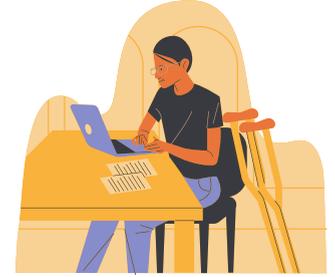
3

HRMOs should facilitate Virtual Private Networks (VPNs) community trainings. VPNs allow users to bypass local Internet restrictions by connecting to servers in other countries. If the Internet shutdown isn't total (service blocking) or if some networks remain accessible, VPNs can be a way to access the broader Internet. Always ensure that monitors have VPN on their gadgets especially when anticipating a shut down. At the same time monitors should be trained on how to hide some of these applications on their devices in anticipation of being targeted by state apparatus. It is also equally important for HRMOs to pay licensing fees for these VPNs and provide a step-by-step guide on how to use these VPNs way ahead of time or collaborate with providers of such services which can offer some of these licenses for free for example Tunnel Bear and Psiphon which normally give free license when they anticipate that a shutdown will occur in a specific country. However, this would work if the government does not outlaw the use of VPNs.

4

Digital rights activists should offer support to HRMOs prior shutdowns on how to use Proxy servers or Hypergiants (HGs). The former serve as intermediaries between the users and websites, masking the real location of the user and enabled access to blocked content. The latter install servers inside other networks to serve users in those networks or their customers. This strategy localizes their content within the hosting network, reducing traffic crossing network boundaries.

RECOMMENDATIONS



- 5 HRMOs should disseminate and train HRP on how to use Tor network. The tor network anonymises internet traffic by bouncing it through multiple servers worldwide, making it difficult for authorities to track users. This browser allows users to access blocked websites. Since it can bypass Internet censorship, it is beneficial when the regular Internet is restricted.
- 6 Funding partners should consider supporting HRMOs or Media organisations with financial support to establish Community Local Networks (CLNs) in marginalised parts of Zimbabwe. CLNs are low-cost community networks that will improve internet access in rural areas. CLNs is one of the best ways of connecting the unconnected and will be a breakthrough for bridging the digital divide. CLNs provide knowledge management platforms, and these will be crucial for acquainting HRPs in secluded remote areas with skills, knowledge, methods of what to do prior, during and post an internet shutdown. This intel should be compiled and put in a guide that is available in local languages, as language is one barrier that is widening the digital divide. This can be achieved by collaborating with partners like Localisation Lab to assist with translation.
- 7 HRMOs should train their monitors on how to use Mesh networks. Mesh networks are made up of computers and mobile phones linked directly to each other instead of via a centralized Internet service provider (ISP). These networks are decentralised networks where individuals connect directly to each other, creating a network without the need of an internet service provider. This will be possible in urban areas across Zimbabwe where people live close to each other. Apps such as Signal offline messenger, Near Peer Offline Chat, Vojer, Manyverse, Bridgefy, Briar or FireChat allow people to create local mesh networks using Bluetooth to send messages without the Internet. This form of networking has become common.
- 8 During shutdowns HRMOs should invest in Low Connection Publishing platform such as Text services (Txi). This is a web service used to produce web pages with slow internet. The service can also be used to collate information in one place for easy access in areas with weak data connections. It is useful in times of crisis reporting and allows users to share information easily from central source. This service can be used as an email service and each Txi can contain links, images, lists, headings and more.
- 9 HRPs should gain interest towards using offline calling apps such as Walkie talkie and Serval Mesh. Serval Mesh for example, allows users to make private phone calls easily. Users can keep their existing phone number on mesh mode which is important during an emergency.
- 10 HRMOs should train their monitors on how to use of text messages applications that are secure. The Silence application for example is one app that is end-to-end encrypted that that can be utilised by HRPs when sending SMS messages. For this to work, both sender and receiver must have it installed on their devices and exchange keys with each other. Alternatively, HRPs can use SMSWithout borders, an app that was created during Camerouns 240 hours long shutdown. This application allows citizens to register their twitter and Gmail credentials with the services then use mobile phone SMS functions during an internet shutdown to post twitter, send and receive emails.

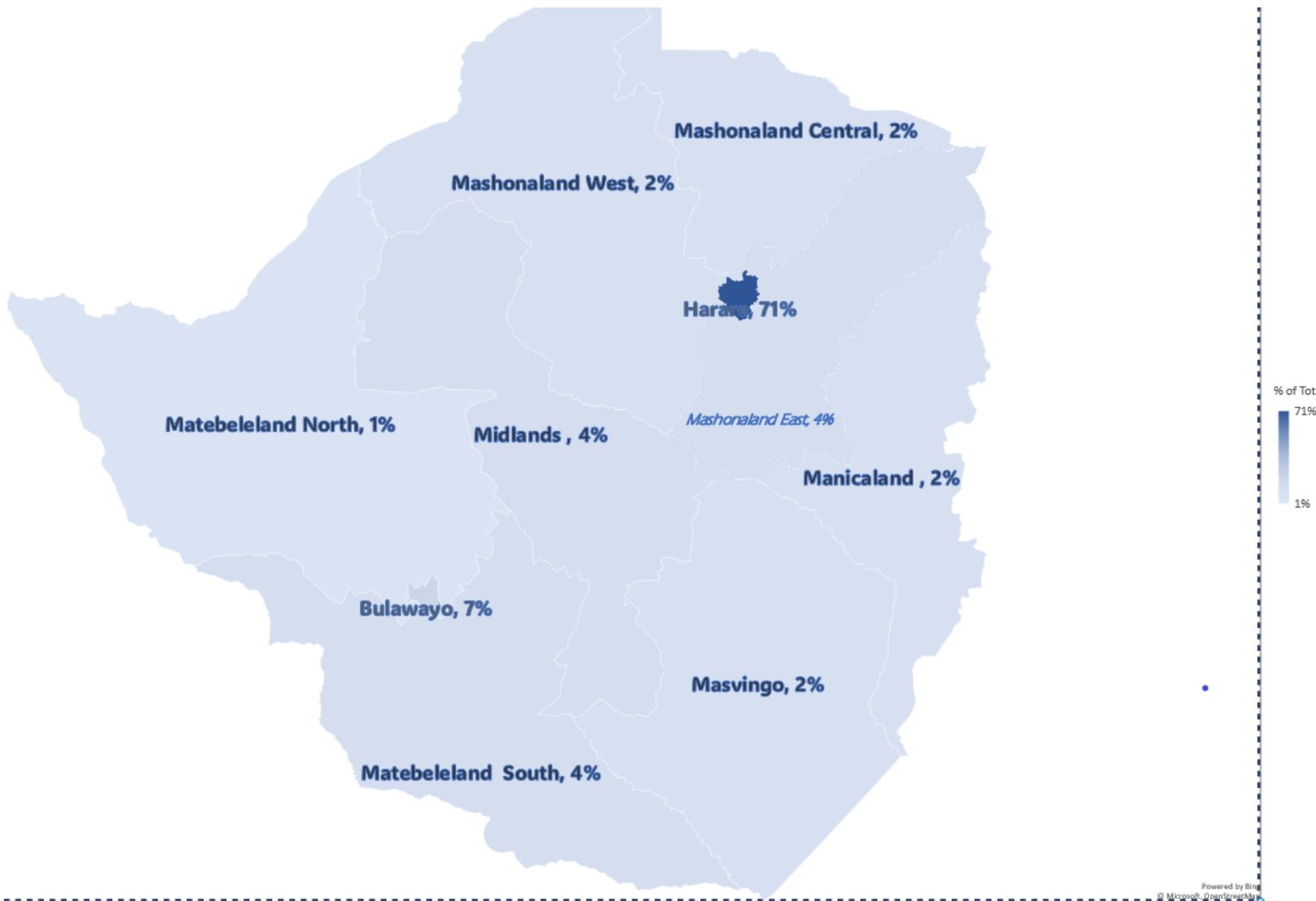
ACKNOWLEDGEMENTS

The author would like to thank Advocacy Assembly and Small Media Foundation for the opportunity and support throughout the research process. Would also wish to relay hearty thanks to WITNESS for providing training on how to safely and effectively document human violations during internet shutdowns, tips on how to guarantee safety of monitors, methods on how to ensure their documentation is preserved, verifiable, and can reach others even without internet access.

***We thank you for your continued support
in our efforts and we look forward to your
continued support.***

APPENDIX

Geographical Scope and Population Distribution



Survey had a national scope and was responded to by 83 human rights practitioners including 48 females and 35 males. The survey was fairly dispatched to executives and middle management practitioners within the Zimbabwe Civil society. The response rate was high in Harare possibly because most CSOs are based in Harare. Follow ups were made to organisations in other provinces but the response rate was relatively low. However, the assessor appreciates the feedback relayed to him and considers their reflections as binding views which are fairly shared in their respective provinces.