FREEDOM OF EXPRESSION IN CYBERSPACE

An Analytical Survey for Southern Africa

MEDIA INSTITUTE OF SOUTHERN AFRICA
MISA
PROMOTING MEDIA DIVERSITY • PLURALISM • SELF-SUFFICIENCY • INDEPENDENCE

CONTENTS

Published by Media Institute of Southern Africa, 2014.

Author: Michael N. Phoya

Editor: Levi Kabwato

Designer: Alexandra Peard

SUMMARY

This report presents the findings of a survey, conducted in June 2013 via a partnership between the Media Institute of Southern Africa (MISA) and Privacy International (PI).

Ninety journalists and bloggers across southern Africa participated in the survey, which revealed that while there is general awareness of privacy laws and regulations in the region, there still is considerable doubt and lack of awareness about frameworks governing communications surveillance and privacy protection.

Fifty seven per cent of the survey respondents are aware of privacy laws in their country while the rest are not. Although the majority answered in the affirmative, it would appear that their understanding of these laws – as indicated by their answers – was far from comprehensive. While a handful were able to articulate the meaning and contextual application of these laws in their individual countries, many gave definitions that suggest that either privacy laws are not clearly observed/understood in their countries or they have just not read about them at all.

One respondent:

"South Africa is in the process of adopting new privacy laws, which govern, among other things, the collection and processing of personal data... More broadly, the constitution guarantees rights to privacy and dignity. The extent to which these limit free speech rights is very much up for debate ... Current intelligence legislation, however, appears to leave unregulated highly intrusive forms of electronic surveillance provided aspects of the communication in question pass out of the country, which leaves many citizens and organisations vulnerable to eavesdropping by the state without credible oversight.

Another respondent:

"There are laws which regulate the dissemination of private information and also which regulate the collection of personal information."

While the survey reveals that as much as 85% of the respondents have never been threatened or personally attacked because of the work they do online, 60% of them, however, suspect that their communication devices have come under threat from either spyware or malware. In almost all cases, such threats are suspected to have originated from their government.

Ten per cent of the respondents have been attacked for their online work, mainly in form of insulting emails and comments on social networking sites such as Facebook and Twitter. Some respondents reported being threatened by government ministers in their country. At least half of the respondents who have not been physically abused stated that they know someone (usually a friend or colleague) who has been physically abused as a result of their online work. The common modes of assault are physical abuse and confiscation of equipment.

As much as 52% of respondents said they are familiar with human rights frameworks in their respective countries while 36% said they are slightly familiar with these. Nine per cent are not at all familiar with the frameworks.

The majority of the respondents combine several tools to conduct their work and general communication. Over 80% of the respondents use laptops and mobile phones, while over 60% use traditional personal computers (PC) and digital cameras.

INTRODUCTION

The rapid growth of information communication technologies (ICTs) in Africa has led to a massive digitalisation of information, which has, in turn, opened up various social and economic opportunities. The democratising nature of information – especially Internet-powered information – has resulted in most governments feeling uncomfortable (some would say insecure) about their own positions.

In light of 9/11 (the New York terror attack) and the so-called Arab Spring, which saw the dismantling of dictatorships in Egypt, Tunisia and Libya, governments south of the Sahara have been paying particular attention to how communication platforms in their countries are being used by citizens. This has led to systematic introduction or amendment of laws that enable mass surveillance and – with little or no judicial oversight – the interception and monitoring of communications.

Content filtering, while not a very common tactic by governments, is an ever-present option. Pending legislation in Malawi, for example, alludes to content filtering and puts this burden on Internet Service Providers (ISPs), whose failure to comply may result in revocation of operating licences and/or other legal action.

The implications of these actions on freedom of expression and media freedom are enormous.

Advances in computer and mobile technology, the expansion of the Internet and the development of social networks and digital tools have removed many geographic, social and political barriers to the exchange of news and information. At the same time, these developments have created new areas of vulnerability for media professionals and bloggers who often are not fully aware of how these new technologies can threaten their privacy and security.

This is particularly true in countries where citizens face major security challenges such as government surveillance and intimidation especially of the political kind. Hence, as the Internet gets entrenched as a human right, how can human rights defenders in southern Africa be empowered to harness its power in order to promote democracy and good governance? Also, against the backdrop of increasing restrictions on freedom of expression and increasing State paranoia in relation to new communication technologies, how can the privacy of human rights defenders be safeguarded and their surveillance be circumvented?

These are the questions that prompted MISA to devise the Freedom of Expression in Cyberspace project to address the relationship between human rights and privacy laws and regulations, while raising awareness on issues of data protection. The project is designed to challenge existing and future communications surveillance programmes targeted at citizen and mainstream journalists in southern Africa.

Over the past 20 years, MISA has positioned itself as the primary advocate for media freedom and freedom of expression in southern Africa. With programmes that have a global outreach, especially through the media violations monitoring programme, the organisation's agenda has been taken up by many civic organisations in the region, creating consciousness of the linkages between media freedom, freedom of expression and broader human rights and democratic campaigns.

PROJECT RATIONALE

Given the level of insecurity surrounding the use of digital and mobile technology by journalists and bloggers, protection of users' privacy is now crucial, particularly when citizens and journalists use online platforms, social networks and mobile devices to express themselves on a wide range of issues.

With this in mind, respondents who comprised of journalists, bloggers, human rights activists, academics, technology experts and students were surveyed to gauge their understanding of the risks and threats they face when using digital media in their line of work. The ultimate goal is to develop simple protocols and identify the best tools to help media workers and the general public better protect themselves online, so they can do their work with minimum exposure to the risk associated with communication surveillance. The survey, therefore, asked questions such as:

- Are you aware of any privacy laws and regulations in your country? And if yes, what is your understanding of these laws?
- Have you ever been threatened or personally attacked because of your online/mobile work? If yes, what was the nature of the violation and what action was taken to address it? If no, do you know anyone who was threatened or personally attacked because of his or her online/mobile work?
- Have you ever suspected that any of your communications devices were under threat from spyware or malware? If yes, how did you identify the threat and what did you do to deal with it?
- Are you familiar with terms like HTTPS, Encryption, Safe email providers, Virtual private networks (VPNs), and secure storage spaces?
- At your place of work, are there resources devoted to helping you maintain individual privacy and digital security?
- How do you rate your ability to use risk reduction tools and strategies when working on computers, using mobile phones or navigating the Internet?
- How much do you mix personal information with professional activity when using social networks like Facebook or Twitter?
- Do you belong to any network or group dedicated to online and mobile security?
- How vulnerable do you think you are to physical and digital risks and threats?
- How familiar are you with international human rights law?
- What do you understand by communications surveillance?

MISA is already using the information generated by this survey to design research and training programs for journalists, media activists, bloggers, and human rights defenders so as to empower them on how they can harness the power of ICTs to promote democracy and good governance in a safe and secure way.

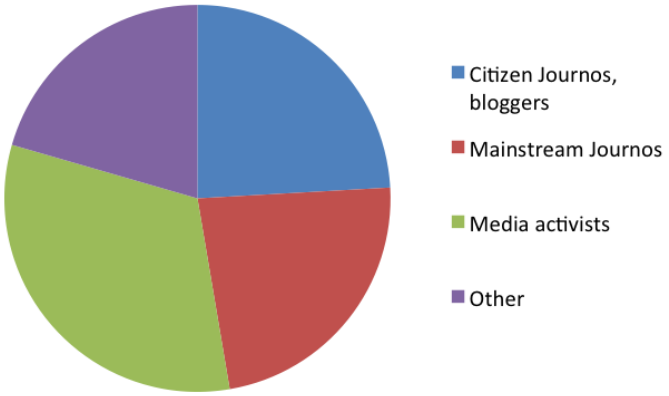
METHODOLOGY

Michael Noel Phoya, a trained journalist and media manager from Malawi was commissioned to design a survey tool to help MISA properly framing the issue of Freedom of Expression in Cyberspace. According to the brief, key themes to consider were privacy, communications surveillance, mobile technology and digital security. In the end, a 23-question electronic survey was designed.

MISA distributed the link to the online survey via the MISA global mailing list, Twitter, Facebook and direct emails to prospective respondents.

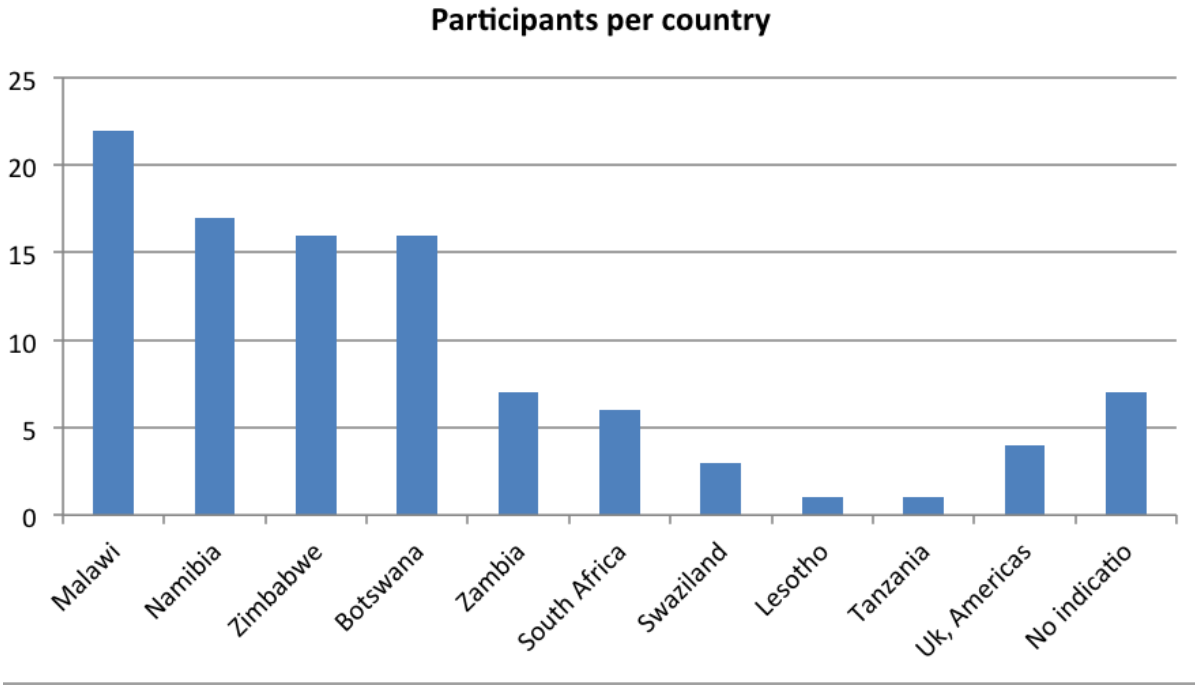
Of the 90 respondents who started the study, 72 % finished. These findings are based on those who finished.

Thirty-five per cent of the respondents classified themselves in the category of media activists, 26% as mainstream journalists, 27% as citizen journalists/bloggers, and 23% as 'Other'.



Categories of respondents

The study primarily focused on southern Africa residents. Twenty-two per cent of respondents were from Malawi, followed by Namibia at 17%, Zimbabwe and Botswana at 16% each, Zambia at 7%, South Africa at 6%, Swaziland at 3%, Lesotho and Tanzania at 1% each, the UK and Americas at 4%, while 7% of respondents chose not to indicate their country of origin.



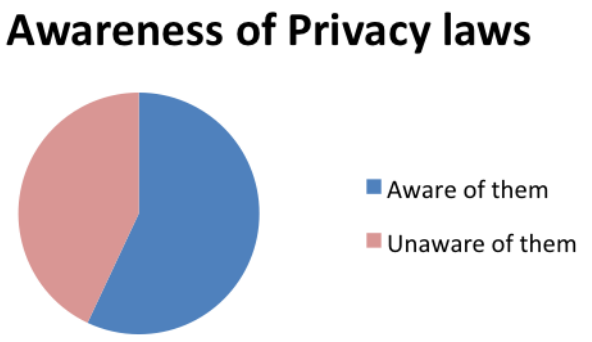
RESULTS

PRIVACY AND HUMAN RIGHTS LAWS

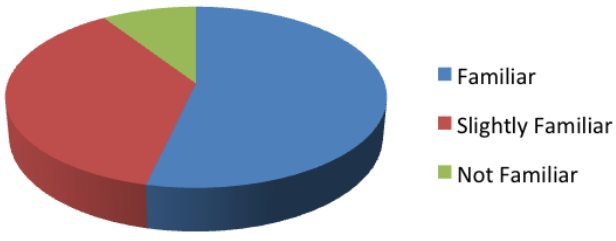
Fifty-seven per cent of the respondents are aware of privacy laws in their country while 43% are not. Although the majority answered in the affirmative, their understanding – as suggested by their responses – is not very comprehensive.

While few were able to articulate the meaning and the contextual use of these laws in their individual countries, many gave definitions that indicate that either privacy laws are not clearly observed/understood in most countries. Some simply saw them as laws designed as tools for governments to oppress the people and not to actually enhance privacy.

For example, while the Access to Information and Protection of Privacy Act (AIPPA) in Zimbabwe speaks to the issue of privacy, the government has consistently used the law to stop journalists from doing their work freely, so much so that the entire law, rather than only some specific section, is viewed as being inconsistent with democratic practice and the right to freedom of expression and media freedom.



On understanding their respective human rights frameworks (human rights law, institutions etc.) 52% said they were familiar with these while 36% said they are slightly familiar. Nine per cent were not at all familiar with the frameworks.

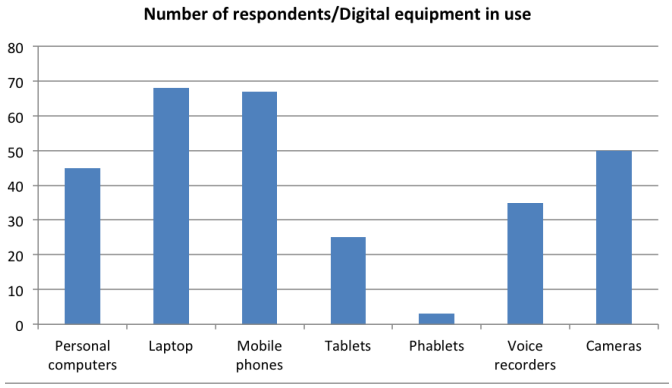


Familiarity with Human Rights Law

ACCESS TO DIGITAL HARDWARE/ ICT'S

The accessibility of digital equipment to media practitioners in Africa has greatly improved over the years. All of the respondents use computers, the Internet and a range of digital tools/mobile devices in executing their duties. Forty-three per cent rated their ability to use these devices as 'excellent' and 44% as very good. Only 13% considered their skills 'fair' while 1% rated them as poor.

There is a range of different digital equipment in use, with laptops and mobile phones proving to be popular, undoubtedly due to their portability.



Overall, the impact of digital media equipment use has been very high, with almost all the respondents citing improved efficiency in their work. The use of such equipment has also inevitably improved how that work reaches its targeted audience. In addition, networking opportunities have been enhanced across borders.

One respondent:

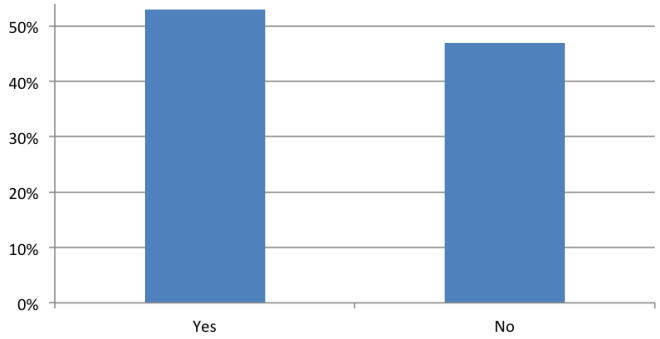
"Digital and mobile tools have transformed my own journalism and editing practice, as well as my activism around media issues, by enabling rapid reporting, collaborative reporting, and networked discovery and dissemination of information and ideas."

THREATS/ATTACKS DUE TO ONLINE/ MOBILE WORK

Respondents said email account hacking was the most serious digital risk they face. Nearly all respondents heavily rely on the Internet and actively use digital tools to communicate and gather information.

Only 15% of respondents said they have been previously threatened or personally attacked because of their online/mobile work. The common abuses/violations cited were insulting emails and comments on social networking sites like Facebook and Twitter. A few cited examples where certain individuals, hiding behind fake names, perpetrated the violations. Others reported cases where they were personally threatened by government officials.

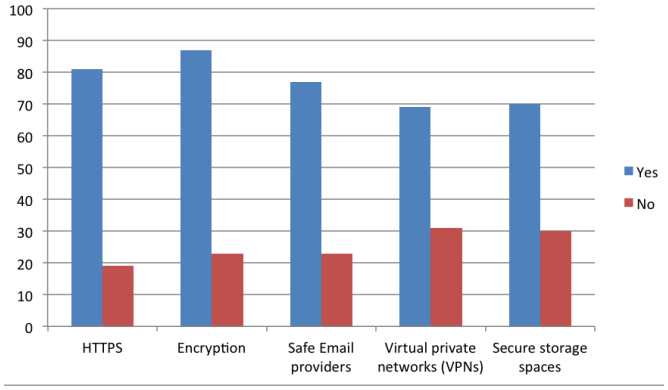
At least 50% of the respondents who have never been physically abused did report know someone who has, but only a few respondents elaborated on this. In some instances, the victim is a friend, colleague or a family member. A few of these instances involved physical abuse and forced commandeering of personal equipment.



Are there resources devoted to helping you maintain individual privacy and digital security?

Most of the respondents equated security in cyberspace to simply having an Antivirus in their devices. In some instances, the software is either a free version or one that is out-of-date.

When it came to grasp of security tools, data encryption, and anonymous internet usage, most of the respondents were aware of the terms used to achieve this:



Familiarity with security tools, data encryption, and anonymous internet usage

However, there is a need to view the results above with caution as most of the respondents operate in environments that are not very sophisticated. As shown above, most of the respondents equate security in cyberspace to merely having anti-virus software.

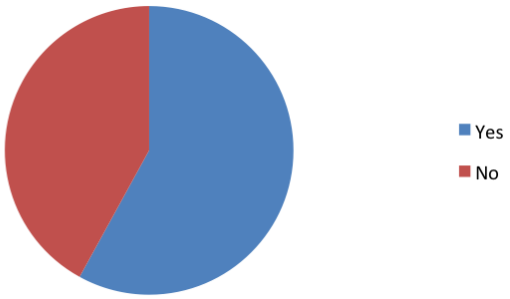
Asked about their skills in implementing secure and, if the need be, anonymous internet usage, 9% considered their skills 'excellent', 35% 'very good', 46% 'fair', and 12% 'poor'. Again, these assertions should be taken with caution.

When it comes to mixing personal information with professional activity when using social net¬works like Facebook or Twitter, 10% say they do so frequently, 13% very often, 19% fairly often, 20% sometimes, 26% almost never, and 13% never.

Over half of the respondents are aware of resources devoted to helping them maintain individual privacy and digital security. However, almost all respondents admitted or implied that these measures are inadequate. Most of them cited computer firewalls, encrypted networks, and anti-virus software as examples. Some cited dedicated IT support staff who, among other measures of security, encourage them to change their passwords repeatedly.

COMMUNICATIONS SURVEILLANCE/ VULNERABILITY TO ATTACKS

Most of the respondents understand communications surveillance as the monitoring of communications, whether digital, mobile, etc., to gain information on a person's activities and/or interactions, without their knowledge or consent. And in almost all cases, the culprit is government.



Have you suspected that your devices have come under attack?

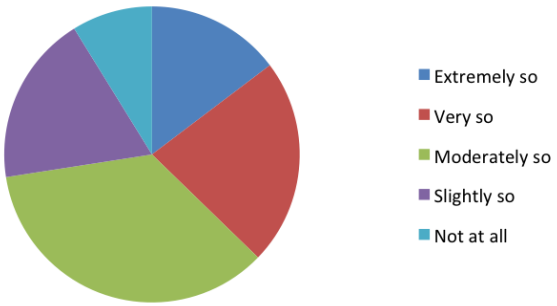
"I do not suspect, I know. The government keeps tags on all mobile phone users/subscribers through telecoms regulations that require everyone to register personal details with their network service provider."

Forty-two per cent of respondents claimed they have never suspected that any of their communications devices had come under threat from spyware or malware. Of the 58% who have, the threat mainly came via emails and phone calls, with a good number of them suspecting that someone is listening to their phone calls.

For some, symptoms came through the slowing down of computer. Most of them used free Anti-virus software to clear the problem while others used IT technicians to look into the matter.

A respondent from Malawi implied that they have no control since government has installed the much feared 'spy machine', formally the Consolidated ICT Regulatory Management System (Cirms) which, according the Malawi Communication Regulatory Authority (Macra), is designed to prevent telecoms customers from being overcharged. It became known as the 'spy-machine' because some thought it would allow for systematic monitoring of phone calls and illegal intrusion into their private conversations.

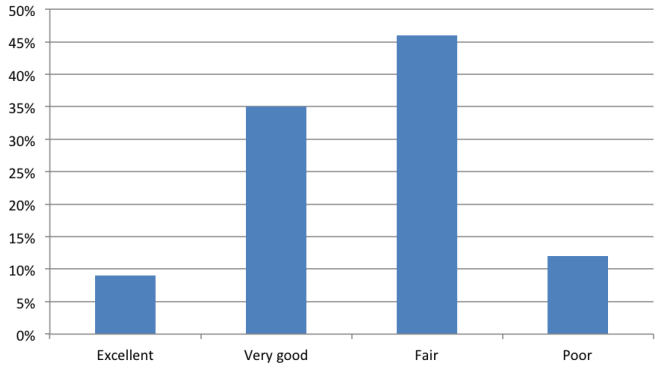
In one instance, a certain media house took action by reporting the threat to the Intelligence Bureau of their country but no action was followed.



How vulnerable do you think you are to physical and digital risks and threats?

When it came to perceptions on vulnerability to physical and digital risks and threats in their workplaces or concerning their online work, only 15% of the respondents felt so while 36% felt moderately so. However, this may show that most of the respondents are not made aware of the threats or do not really comprehend the nature or seriousness of the threat they face, if any.

Those who felt at risk pointed out that freedom of expression in cyberspace is under threat because governments are trying to find ways of regulating it. Some of the reasons given for this vulnerability were a lack of security at work premises, the nature of their work, particularly that of activists attracting governments' attention, and a lack of adequate knowledge in the area of secure online usage.



How do you rate your ability to use risk reduction tools and strategies when working on computers, using mobile phones or navigating the Internet?

Of those who attempted the question of belonging to a dedicated group or network on online security, only 17% responded in the affirmative.

Some respondents from South Africa acknowledged that their country has more institutions of accountability than other countries in the region, but also massively more surveillance capacity, public and private, official and unofficial, hence the risks there are substantial.

Others pointed out, especially in light with the issue concerning the United States' National Security Authority (NSA) informant Edward Snowden, that as users of such cloud services as Gmail, they feel extremely vulnerable to snooping from offshore agencies.

Others argued that since the law and policy can never keep up-to-date with technology, there is a need for non-government organisations (NGOs) and civil society organisations (CSOs) to step in and safeguard people's privacy and lobby lawmakers to update the law, without infringing on people's freedom and pri-

vacy. Some respondents claim media practitioners need to be better informed about the many threats in the cyberspace, saying there is a false sense of security among journalists who think the only danger out there is physical.

A good number of the respondents, especially those from Malawi, want MISA to conduct training on security in cyberspace.

LIMITATIONS

An important limitation of the study to note is that it was conducted online, and thus reflects the views of respondents who have at least a basic level of computer and online literacy and knowledge. For future studies, MISA may choose to employ a more diverse methodology to better understand the views and understanding of a broader range of media workers and citizens in relations to the use of ICTs in the media landscape and online security, safety and freedom of expression more generally.

RECOMMENDATIONS

ICTs can help increase quantity and even the quality of journalism and access to information in Africa. While the future of journalism in Africa is bright there are some notable stumbling blocks.

Apart from access to technology, training and infrastructure, there is also the issue of repressive governments. But for that to be achieved, bodies like MISA need to be at the forefront of formulating policy that can critically capacitate journalists and other practitioners about ICTs and the dissemination of critical content and analysis. Also, practitioners need to be taught on procedures to be taken when faced with such challenges. Below are some of the recommendations based on the analysis of the results of the survey.

MISA needs to educate stakeholders in areas concerning privacy as a right situated within a broader human rights framework. Also, MISA needs to create a platform, preferably on the Regional Secretariat and Chapter websites, where privacy laws for individual countries are clearly outlined and critiqued. These platforms will familiarise southern Africa citizens and mainstream journalists with existing legal frameworks (criminal defamation and insult laws) and how such can be used to restrict freedom of expression in cyberspace and what strategies and tactics can be adopted to defend the online space.

There is a need to sensitise users on how to avoid or deal with spyware and other malicious software. MISA should formulate policy or train journalists, bloggers and human rights activists on key tools and tactics.

There is also a need for media houses/organisations to invest more in advanced data encryption equipment. One actionable outcome from this can be an output document with meaningful/actionable technical and policy information on best practices and steps to address in-house security concerns. These can be adopted, via MISA chapters, by different media houses or individuals.

There is a need for MISA and its Chapters to initiate groups, which can offer support and sharing of information, encryption of data, procedures for reporting suspected surveillance, and other support as needed.

MISA needs to empower journalists, bloggers, human rights defenders and other activists in southern Africa to harness the power of ICT to promote democracy and good governance and to defend their privacy and evade possible surveillance.

MISA needs to raise awareness on issues surrounding digital security (privacy, censorship and surveillance) for citizen and mainstream journalists in southern Africa and fully capacitate southern Africa citizen and mainstream journalists in effective usage of digital media tools for research and presentation of evidence of human rights violations

MISA should facilitate regional participation of technical experts, policymakers, and other stakeholders for an actionable discussion on the importance of understanding regional concerns on cyber security and global Internet Governance matters.