## CONTENTS

### INTRODUCTION.
- Opening remarks 02
- Welcome address 02
- Key note address 02-03
- Acknowledgements 03

### SESSION 1: TRENDS IN INTERNET USE IN ZIMBABWE.
- 1.1 Free speech v the right to dignity in the digital age: an analysis of the cybercrime and cybersecurity bill 05
- 1.2 Safeguarding the vulnerable online 06
- 1.3 Investigating Cybercrime 07
- 1.4 Plenary 08

### SESSION 2: PRIVACY, DIGNITY AND ACCESS TO INFORMATION IN ZIMBABWE.
- 2.1 Internet governance and the enjoyment of constitutional rights: Privacy, access to Information and freedom of expression 12-13

### SESSION 3: USING LAW AND POLICY TO SAFEGUARD THE INTERNET.
- 3.1 An overview of regional laws and policies that protect online rights: 15
- 3.2 Fighting cybercrime while upholding free expression & privacy 16
- 3.3 Access to information and media freedom in a digital age 17

### SESSION 4: THEMATIC GROUP DISCUSSIONS
- 4.1 Perspectives to principles: Cybercrime and cybersecurity 19
- 4.2 Feedback from Thematic Group Discussions 19
- 4.3 Concluding remarks 21
- 4.4 Acronyms 21
On the 23rd of November 2018, MISA-Zimbabwe convened stakeholders for the annual Multi-stakeholder Internet Governance forum at Cresta Oasis in Harare. The meeting was the third instalment of the conference which was first held on the 21st of August 2015. The Conference came at a time when there is media reportage of intention by the Ministry of information and Communications Technology to advance an omnibus bill that regulates cybercrime and cybersecurity, electronic transactions, and data protection aspects all in one Bill. As this proposed Bill is yet to be presented to Parliament for debate, there still remains ample opportunity for stakeholders to contribute meaningfully in pursuit of various objectives, including in pursuit of this year’s conference theme of “ensuring a safe internet for all.” This is more-so considering that regardless of the technical approach that is employed by the Ministry in legislating around cybercrimes and related aspects, the internet remains a key and central conduit, be it in cybercrime, electronic transactions or in data protection pursuits thus the discourse around a safe internet is also a key factor that needs to be continually interrogated.

Discussions articulated the conference theme from different angles although ultimately speaking to various aspects relating to or affecting the safe use of the internet. Some of the discussions centred on the current challenges in creating a balance between freedom of expression and the other rights of online users; how the digital age is influencing the enjoyment right to privacy, freedom of expression and access to information and on how the law and policy can be used to ensure a safe internet for all, amongst other discussions. The Conference brought together a wide range of stakeholders from the academia from within and outside Zimbabwe, the media, Civil Society Organisations, Policy makers from both the ICT and the Information, media and Publicity Portfolio Committees as well as development partners amongst others. Even more enriching, was the presence of the Zimbabwe republic Police as well as the ICT sector regulator POTRAZ, whose participation is critical in present as well as future engagements around internet governance. A summation of main issues raised and discussed at the Conference ensues below.
OPENING REMARKS:

Kuda Hove:
MISA-Zimbabwe, Legal and ICT Policy Officer

Kuda Hove, the program Director for the day opened the meeting, remarking that in convening this year’s conference, MISA-Zimbabwe was inspired by what has happened in the past on the internet in Zimbabwe and beyond. In Zimbabwe for example, he noted that in the run up to elections, the internet, particularly social media, has been used in a negative way to attack female candidates, amongst other continuing incidences of irresponsible and harmful use of the internet. Against this background then, the question of how there can be a safe internet in Zimbabwe arose, inspiring the year’s conference theme.

WELCOME ADDRESS:

Golden Maunganidze:
MISA- Zimbabwe Chairperson

The MISA-Zimbabwe Chairperson thanked participants for honouring the invitation to gather again and put minds together to discuss pertinent issues affecting internet use in Zimbabwe. He expressed appreciation for the diversity of stakeholders present which in his opinion, stood to enrich the engagement and proposals raised thereon. He noted that the conference remained a relevant platform for stakeholder engagement on use of the online space, more so as technology continues to evolve and resultantly, as States look to introduce more laws to regulate the internet space. Mr Maunganidze noted the importance of stakeholders doing their best to help the government in coming up with sound policies for both online and offline freedom of expression. Mr Maunganidze encouraged the stakeholders to engage freely and assured them that all their contributions would be taken into consideration for future transmission to policy makers.

KEY NOTE ADDRESS:

Honorable Chalton Hwende:
Chairperson of the Parliamentary Portfolio Committee on ICT Postal and Courier Services

The Chairperson’s speech set the tone for the ensuing engagements with a scan of the obtaining environment from an ICT-related point of view as well as pointers on the grey and emerging areas in relation to internet use in Zimbabwe. He noted the appropriateness and timeliness of the conference theme, particularly how it was all encompassing in its call for action from every person in combating cybercrime and in safeguarding the vulnerable online. Hon Hwende also lauded the holding of the conference as a platform for creating evidence-based legislation to protect privacy and develop a sustainable and digital Zimbabwe. He called for particular focus during the conference, on the internet needs of people with disabilities, including how they as well as rural or remote populations stand to also contribute to the public policy discourse. Hon Hwende further challenged the conference to balance the discourse on safe internet use with thoughts on how this pursuit can also be coupled with job creation.

The honourable MP, also stressed on the importance of safe use of the internet considering its increasing importance as a conduit for information dissemination and communication by both the public as well as by investors and other business oriented persons, and increasingly so, through social media. All persons using the internet whether for business or other purposes he noted,
need to feel safe in that space and the conference presented an opportunity for all present, to contribute to the development of knowledge, skills and standards for safe and responsible internet use. He further noted that while the internet offers immense opportunities and is a great window to the world, it was increasingly coupled with online bullying and harassment whose prevalence was already confirmed by the Advocates for Progress’s online survey. Against this background, he expressed his hope that all gathered will play a huge part in creating a safe and responsible digital environment for all Zimbabwean within their own spheres of influence, including through initiatives that are inclusive of women, youth, people with disabilities, marginalised groups and those in the Diaspora as cybersecurity is everyone’s responsibility.

Honorable Hwende also took the opportunity to share some of the concerns his Committee has already received thus far relating to internet access and its use in Zimbabwe which include limited internet access and in particular, the high cost of data.

He ended his speech by expressing his keen interest in engaging with the public as well as in increasing citizen engagement and awareness on related matters, as well as on the Cybersecurity Bill which he anticipated, would be brought to Parliament in the ensuing weeks and following which, the Portfolio Committee would begin engaging the public on through nationwide stakeholder consultations. Hon Hwende invited MISA to be a friend of the Committee and whose technical input into its oversight work is most welcome.

ACKNOWLEDGEMENTS

Tabani Moyo:
MISA-Zimbabwe Director

The MISA-Zimbabwe Director expressed appreciation to Honourable Hwende for delivering the Conference’s key note speech. He also gave his recognition and appreciation to the conference’s funders and partners who included the Konrad Adenuer Stiftung represented by its Director Mr Mbae, representatives of the Portfolio Committee on Information, Media and Publicity, the MISA-Board Chairperson and its other members, representatives of CIPESA and CALR with whom MISA was partnering in the hosting of the conference. Mr Moyo also acknowledged the presence of POTRAZ, the Zimbabwe Internet Governance Forum represented by Mr Zvavanjanja, the delegation from Botswana under CIPESA, members of the academia and civil society and all delegates present.
SESSION 1

TRENDS IN INTERNET USE IN ZIMBABWE
1.1
FREE SPEECH v THE RIGHT TO DIGNITY IN THE DIGITAL AGE
An analysis of the cybercrime and cybersecurity bill.

Advocate Brian Hungwe

Advocate Hungwe described the Cybercrime and Cybersecurity Bill as a legal offshoot of the digital era which principally seeks to address issues in the social media, more against a background where obtaining criminal laws such as the Criminal Law Codification Act, do not adequately address crimes emanating from the cyber space. He noted that while the intention of the State in legislating around cybercrime is noble, its proposed provisions need to be juxtaposed against the right to freedom of expression as espoused in the Constitution and that the key question to be borne in mind should be whether the Bill promotes freedom of expression or not.

He noted that while cyberspace regulations such as the proposed Bill are meant to achieve various public interest purposes, genuine public fear at the moment is that in trying to regulate cyberspace, the Bill will also have the effect of stifling online expression and access to and dissemination of information.

Advocate Hungwe further noted that for the Bill to be seen as progressive, it requires thorough civil society interrogation and input, wider public discourse on the Bill that is also guided by academics who are oriented in cyber security research as a means of encouraging progressive modifications of the Bill to avoid “giving birth to a monster” of a law. He noted that the critical areas of concern in the Bill are around access to information, freedom of expression, privacy and data protection.

He emphasised the need for repressive parts of the Bill to be interrogated and modified before the Bill is passed into law to rather having to resort to other means such as court judgements that proclaim the same can already be determined at this point. This is more so as litigation is often wasteful, time consuming and expensive and according to him it “paints an ugly picture of the state, unreleenting in controlling the minds of its people and suffocating their rights, only to be grudgingly restricted by the third branch of the state.” Thus if this can be avoided, the better. Advocate Hungwe stressed the need for the Bill's conformity to the constitutional guarantees espoused in section 61 and section 62 to be a key guide is assessing the Bill. This far he noted, there are a number of controversial sections for further consideration which include:

i) section 4 which provides for the procedure for the creation of the Cyber security centre whose members he highlighted, is largely linked to the state save for one member from CSOs, giving rise to questions on the committee’s independence as it is likely to be beholden to the state rather than the public.

It was the Advocate’s suggestion that instead, members of such committees should be appointed through a parliamentary process which would ensure that members are beholden and accountable to the public and not to the state.

(ii) The criminalisation of false information in the Bill.

This was also touted as a major concern, more-so danger in a democratic society. Reference was to the judgement in the case of Chimakure and Others v the Attorney General where the court dealt with the issue of criminalisation of falsity and noted that the same reasoning should be applied when considering offences based on falsity in the Bill.
SAFEGUARDING THE VULNERABLE ONLINE

Mr Alfred Ncube- Childline Zimbabwe

Alfred Ncube gave a talk on various aspects relating to challenges faced by vulnerable groups such as women and children online. To illustrate the growing need for protection for these vulnerable groups, Alfred gave two case studies on the use of online platforms in a manner that violates the rights of children. The first illustration was that of a Sudanese girl who was auctioned on Facebook to potential men for marriage while the other was of a picture of a hunger stricken Somali girl who was pictured with a vulture seemingly ready to pounce on the child.

He noted that in general, women and children still remain the most vulnerable group when it comes to survivors of online abuse and the abuse comes in various forms and from people who are known as well as unknown to them. He further noted that while there are many articulated benefits of Internet usage, until very recently there has been little recognition of the dangers that may also result from the use of such technology especially on vulnerable groups such as women and children in particular. The internet he noted, has facilitated the metting out of various forms of abuse of children including various forms of maltreatment as well as sexual and emotional abuse. A major challenge in particular he also noted, is Child pornography, which is "regularly" used as a means of desensitising children and normalising sexual activity between adults and children. Part of it he noted, are acts such as the exposure of children to inappropriate material young persons he extent of which however, is rather difficult to gauge. The extent of this scourge however is difficult to clearly gage.

Apart from visiting pornographic sites, he noted, e-mail also offers an additional means for children to be exposed to sexually offensive or developmentally inappropriate material. For example, a free e-mail service that is commonly used by children can be saturated with commercial e-mails relating to sexual services, “adult” material and e-mails that appear to link to child pornography. Other online ills he noted, include the use of foul language as well as harassment of children over the internet. Alfred suggested a number of strategies that can be utilised to prevent harm of children over the internet and these can include the following;

• Cooperation at the individual and community levels.
• Measures aimed at offenders, including the criminal prosecution of offenders.
• Parents playing a major and central role, including in actively protecting children from media content in the home.
• Children being continually educated on taking charge of their online safety including by not:
  (i) Divulging personal information unless a parent approves;
  (ii) Pretending to be anyone else online;
  (iii) Sending photographs or credit card details without parental consent;
  (iv) Meeting cyber-friends in person without parental approval.
• Ignoring nasty or insulting messages;
• Informing parents if they access undesirable content;
• Protecting their privacy and those of family and friends when using the internet
• Thinking twice before publishing or sharing anything on the internet.

In his concluding remarks, Alfred implored stakeholders on the fact that the protection of children from internet abuse is everyone's role and that it should be complemented by very strict laws that protect children from online abuse.
1.3

INVESTIGATING CYBERCRIME

Superintendent Amos Tavaziva- Zimbabwe Republic Police, Commercial Crimes Unit- Cybercrimes Unit

Superintendent Tavaziva’s presentation focused on outlining the trends and scope of cybercrime in Zimbabwe as well as the challenges that the Police are currently facing in investigating cybercrimes in Zimbabwe. He defined Cybercrime as “a crime in which a computer or cell phone is the object of the crime or where it is used as a tool to commit an offence” or any criminal act in which the perpetrator hacks or breaks into a computer or computer network in order to illegally obtain sensitive information or disseminate destructive computer software. Cybercrimes he noted, can be divided into three categories generally known as the three Ts that is:

(i) **Computer as a tool** – where the computer is used as a tool to commit an offence e.g. fraud, identity theft, phishing, cyber bullying and stalking.
(ii) **Computer as a target** – where the computer is the subject of the attack e.g. denial of service attacks.
(iii) **Computer as a tangential** – where the computer is used as a secondary tool.

In terms of current approach to cybercrime in Zimbabwe, Sup Tavaziva explained that the legal framework is chiefly centred on the Criminal Law (Codification and Reform) Act [Chapter 9:23], in particular, sections 136 and 162-168. Cybercrime related offences he noted, are also found in other laws including the following:

- The Interception of Communications Act [Chapter 11:20]
- The Postal and Telecommunications Act [Chapter 12:05]
- The Censorship and Entertainments Controls Act [Chapter 10:04]
- Children’s Act [Chapter 5:06]

At the operational level, cybercrimes are dealt with by the CID Commercial Crimes Division- Cyber Crime Unit whose capacity continue to be enhanced through a number of initiatives that include trained personnel with varying qualifications as well as a Cyber Laboratory which was formed in 2015, to aid in Forensic investigations. In the past three years, cybercrimes he noted, have been on a rapid increase as depicted in the table below:

<table>
<thead>
<tr>
<th>Years</th>
<th>Number of cases received</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>35</td>
</tr>
<tr>
<td>2017</td>
<td>38</td>
</tr>
<tr>
<td>2018</td>
<td>618</td>
</tr>
</tbody>
</table>

Table 1- Cybercrime statistics Northern Region- 2016-2018

Sup Tavaziva attributed the sharp rise in cybercrime to a number of reasons which include:

(i) The increased use of mobile banking;
(ii) The adoption of the multi-currency system in the country which has attracted sophisticated international criminals who seek the United States Dollar from the vulnerable locals.
(iii) The added cyber element in the commission of other forms of traditional crimes.
He identified commonly reported cybercrimes as including; cyber stalking; phishing, identity theft, card cloning; fraud, and online banking fraud through platforms such as Ecocash.

Sup Tavaziva also shared some key tips to avoid being a victim of card cloning or skimming which include the following:

(i) Never giving one’s card to someone or asking for assistance at an ATM
(ii) Hiding one’s PIN when keying it into an ATM and being constantly aware of people standing close by during the transaction,
(iii) If possible using an ATM that is monitored by a CCTV camera.
(iv) Monitor your bank statement for unusual balance enquiries.

A number of challenges are currently hindering cybercrime investigation and according to Sup Tavaziva, these include the following:

- Lack of soft and hardware for retrieval of digital evidence and tracking of suspects. Currently the Police have to rely on service providers such as Zimbabwe on Line (ZOL), Powertel, Africom, Tel One, ECONET, Telecel and Net One who can only provide such information through court orders.
- The trans-national nature of cybercrime which is constraining on resources.
- The lack of effective cybercrimes legislation in other jurisdictions making it difficult to get cooperation from other countries, even if Mutual Legal Assistance is sought.
- Apparent bias of the Judicial system in Zimbabwe towards traditional crimes at the expense of cybercrime.
- Since the Cyber Crime Bill as not yet law, the extraction and presentation of digital evidence is challengeable at the courts.
- Use of foreign internet services such as g-mail and yahoo as well as dynamic internet protocol addresses which continue to pose difficulties in tracing cybercrimes.

1.4
PLENARY

A plenary session ensued the presentations and discussions from the first session raising a number of issues, comments and questions alike. Some of the comments shared included the following:

(i) That the stated need to balance competing rights within the scope cybercrime legislation, is very confusing even for policy makers at times and the hope was that by the end of the conference, how this balance can be created would be made clear. In response, Advocate Hungwe noted that there are always conflicting interests with for example, journalists having their own interests to gather and disseminate information while for organisations such as CHILDLINE, it is the protection of children’s rights such as to privacy and dignity as in the two Sudanese and Somali cases studies given. He noted that the fundamental issue that should be interrogated is what effect or interest does an action save, whether its public interest of public benefit. For as long as the information disseminated is in the public interest or benefit, it would be justified to override the rights of the child to privacy. In the case of the Somali Child the Advocate advanced, it was in the world’s interest to know of the magnitude of the famine that children in Somalia were facing for purposes of mobilising much needed support.

Alfred from CHILDLINE also shared his thoughts regarding the publication of pictures of pictures, noting that the developed world is very particular about that and that it is a serious offence to
share pictures such as under discussion but that in Africa perhaps, it is the level our vulnerability that perhaps compels persons to accept having such pictures taken of them. He further noted that in the United States of America for example, there are so many shootings including in schools but there is hardly ever any publication of dead bodies by the media. Alfred also shared that it is critical that every child’s privacy, dignity and psychological impact be considered and protected as much as is possible even in instances where publication may be legally sound.

(ii) That the Cybercrime Bill appears authoritarian and that the state seeks to cushion itself against information that it does not want to share judging by some of the aspects it seeks to criminalise and that the effect of the Bill could be to induce self-censorship across society.

Aside for the above comments, participants also posed a number of questions for the presenters as follows:

**Advocate Hungwe**

- How can the growing scourge of fake news, including through online platforms be addressed legally against a background on stated judicial positions that frown on laws that criminalise falsity.

In his response, Advocate Hungwe advanced that there is always a problem in putting a condition to falsity from a constitutional point of view and proposed the removal of falsity from the provisions relating to the publication of information so that it becomes broad i.e. remove falsity attached to publication of information.

**Zimbabwe Republic Police**

- What is the conviction rate of cybercrimes and success with transnational cases?

The Superintendent responded by sharing that the only statistics at hand are for the period 2016-2018 because before then, there was no centralised desk dealing with cybercrime cases as each Police officer could handle such. For the Northern region however, the statistics were as follows:

<table>
<thead>
<tr>
<th>Year</th>
<th>Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>(i)</td>
<td>25</td>
</tr>
<tr>
<td>(ii)</td>
<td>38</td>
</tr>
<tr>
<td>(iii)</td>
<td>618</td>
</tr>
</tbody>
</table>

With the increase in the cybercrime cases, attributed to increased use of plastic money.

Regarding the conviction rate, Sup Tavaziva noted that the challenge is that cybercrimes are new to everyone in the criminal justice system, Police and Judiciary included, posing problems at various levels, such as the gathering and preservation of evidence. As a result, convictions are rather law at present. He also noted that he had no statistics at hand regarding the conviction rate.

- What is the extent of the Zimbabwe Republic Police’s corporation with other countries?

The Police responded by noting that obtaining mutual assistance in the investigation of cybercrimes from other countries remains a challenge and implored members of Parliament to play their role in pushing for alignment of laws with the Constitution.
• **Does the ZRP have the appropriate technology for effective evidence gathering for purposes of cybercrime, more so in light of technology that secures anonymity?**

In response the ZRP stressed that the Force does have some limitations in this regard but these should soon become a thing of the past as it looks to open its Cybercrime laboratory soon and which is expected to have necessary gadgets for those purposes.

Regarding evidence gathering and in particular presentation of evidence in court, the Police called for the urgent alignment of laws with the Constitution so that they can fully facilitate some of these necessary procedures, including in providing an effective framework for mutual assistance by other jurisdictions.

Kuda Hove also added to this discussion noting that one of the challenges is that the country still has no laws that deal with electronic evidence and how it is produced or reproduced for purposes of presenting it in court and that this is a major issue affecting the courts when they look to make decisions in cyber related cases. He added that the government may need to consider investing in measures to ensure effective collection and safekeeping of electronic data.

• **Whether or not the ceasing of gadgets infringes freedom of expression privacy**

In Response, Sup Tavaziva explained that cybercrime is just like any other crime for which when laws are made to fight crime, they take cognisance of the Constitution to avoid infringing rights of individuals.

More specifically he noted that the Criminal Procedure and Evidence Act allows the Police to confiscate exhibits during investigations and that if one's gadgets infringes on someone's rights, then the law can be applied to allow access to those gadgets as part of the investigations.

It was further noted that the commission of a crime allows the limitation of rights to the extent permissible in terms of section 86 of the Constitution including the ceasing of gadgets, although in this regard, the Police should only proceed on the strength of a warrant of search and seizure.
SESSION 2

PRIVACY, DIGNITY AND ACCESS TO INFORMATION IN ZIMBABWE
The discussion by Dr Tsabora looked at the Constitution’s human rights agenda, interrogating the connection between human rights and Internet Governance, with special focus on the rights to privacy, freedom of expression and of the media and the right of access to information. He based the discussion on the United Nations (UN) Working Group on Internet Governance definition of internet governance where it defined as:

“… the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.”

From this definition he noted, a number of key aspects emerge which further show the nexus between internet governance and human rights as well as the general the demands of a governance framework, which include the following:

- Governance as Regulation e.g. through Laws and Social Norms.
- Governance as a shared responsibility amongst different stakeholders such as governments, private sector and civil society.
- Governance as a multi-stakeholder inclusive process, i.e. where inclusivity and participation are key.

Further to these, a number of principles and norms on internet governance were also identified and which are critical considerations when legislating around internet related aspects and in ensuring that the framework fully accommodates and balances all competing interests. These include that:

- The internet must enhance access to, and sharing of information, ideas and knowledge
- The Internet must enhance and promote freedom of expression
- Privacy must be strengthened through data protection and other measures
- Ethical standards must accompany the evolution and use of the internet
- Access to the Internet should be available for all regardless of gender
- Internet must promote sustainable development (social, economic and political development)

Worth noting however, is the fact that some of the shared principles and norms are also human rights and freedoms by their nature, while some are directly linked to the realisation of particular human rights. For example, the principle on access to and sharing of information is in itself a constitutional right provided for in section 62 of Constitution, the one on enhancing expression is related to the right to freedom of expression as provided for in section 61, while to strengthen privacy including through data protection laws, is already guaranteed within the scope of the right to privacy provided for in section 57.

Against this background, a number of threats that need to be borne in mind when considering the required regulatory responses. These include the following:

(i) The fact that the internet now makes it much harder for governments to limit the spread
of knowledge and information.
(ii) That while freedom of expression promotes the enjoyment of many other human rights, the flipside is that individuals’ free speech may also be socially, physically, financially or psychologically harmful to others.
(iii) That the right to freedom of expression in online contexts can damage other individuals’ rights, such as to privacy, reputation and dignity as well as other public interests,
(iv) That there is less online personal security as evidenced by an increase in online related offences such as hacking, identity theft, fraud, phishing, bullying and stalking

Dr Tsabora stressed that a closer look at the legal framework is required towards assessing the extent to which it is in line with the demands of an effective internet governance framework on the one hand, and whether it also adequately promotes affected human rights. Some of the laws and aspects to consider from a Zimbabwean point of view, include:

- the extent of media and social media regulation;
- Adequacy of data protection laws
- Adequacy of AIPPA in protecting privacy
- Whether or not criminal sanctions are the solution for breach of free expression and other related rights.
- The nature of the relationship as well as responsibilities between the Government and multinational companies.
- Whether ethical standards can promote freedom of expression as well as privacy at the same time.

2.2 PLENARY

Dr Tsabora’s presentation elicited a few questions and comments as follows:

(i) With respect to Zimbabwe, artist are losing on royalties due to easy access to musical content on the internet. Is the Copyrights Act adequate to curtail and protect Intellectual property and what best can be done to protect Intellectual property.

In response Dr Tsabora pointed out that the Zimbabwe Music Rights Association [ZIMURA] is there and supposed to promote the rights of musicians in the country including safeguarding their intellectual property but its effectiveness seems in question as musicians still continue to complain about piracy. It appears that even this initiative has also failed in getting solutions to protecting their Intellectual property. Aside from then he further noted, there are no adequate home grown mechanisms to safeguard these rights for musicians who have been forced to rely on live shows, and on mechanisms from other countries. The situation is compounded by the fact that the Copyright Act is aged and out of sync with the digital age and needs an urgent and comprehensive review.

(ii) How ethical or legal are acts such as the blocking or shutting down of wifi [without authority] for some users who will be abusing public wifi, with the intention of assisting other persons to access the same resource.

The ZRP responded by stating that if there is a complainant that is filed with the Police then a criminal case will be instituted. A representative of POTRAZ also added that hacking can only be ethical when done in agreement with the one being hacked and that consent is always required at all times and without such consent it becomes a crime. The network owner and those whose privacy rights are infringed in such instances, can take legal action against a hacker who acts without consent.
SESSION 3:

USING LAW AND POLICY TO SAFEGUARD THE INTERNET
3.1.
AN OVERVIEW OF REGIONAL LAWS AND POLICIES THAT PROTECT ONLINE RIGHTS

Nhlanhla Ngwenya- OSISA

Nhlanhla began his discussion by noting that there is a convolution between regulation and control by most governments and that this is affecting people’s online rights. He pointed out that while regulation denotes equity and the balancing of rights without taking away the freedoms of other users, control on the other hand speaks to a situation where there is dictation of what people should access on the internet and it is important that laws to not have the latter effect. A number of states he noted, are pushing for control rather than regulation which is concerning.

Clarity of CSO policy propositions is also key, Nhlanhla noted, including on the kind of laws that society wants and whether this includes laws that promote action that goes unchallenged. On the characteristics of requisite laws, he noted that whole sum laws that cover both online and offline crimes are preferable, and not laws that only focus on cybercrime. This is more-so because in the regulation of cyberspace, society is confronted with several laws that still take away rights whether or not there is a cyber law or not, thus comprehensive laws regulating both the online and offline space are critical in order to fully protect all rights.

Regarding Regional Trends, Nhlanhla Ngwenya noted that a number of initiatives are underway that impact on online rights which include the SADC internet Governance Forum, as well as various state initiatives and progress on related legislation. Countries like Malawi and Tanzania for example, have enacted cybercrime laws while Namibia, Zimbabwe, Zambia are at the Bill and policy dialogue stages. At the same time other countries are in the process of amending already existing laws to conform to the standards set in the cybercrime laws for example South Africa which is amending its Film and Production Amendment Act.

In other countries however, there is noticeably an erosion of cybersecurity gains such as in Tanzania where the subsequent Cybercrimes Bill Nhlanhla noted, “is more brutal than the initial one.” He also emphasised that as discourse on online rights continues, consensus on the scope of the law amongst stakeholders is key in order to strike a balance amongst all competing interests.

For required benchmarks, Nhlanhla outlined a number of regional and international standards, noting however that despite this wide berth of guiding standards, a number of factors still hinder the full and effective protection of rights online which include the following:

• Lack of public service and interest leadership
• Politicisation of the Internet
• Conflation of cybercrime discourse with politics
• Culture of unaccountability and leaders’ entitlement
• Tokenism in policy formulation
• Weak parliaments and ignorance, characterised by lack of informed and efficient push for required reforms by Parliamentarians
• CSOs incapacity in effectively lobbying and advocating for required standards.

In closing, Nhlanhla made a few recommendations including on the need to build advocates around the sector as well as:

• The holding of wide consultations before bills are taken to Parliament
• Consideration of the responsibilities of each stakeholder including of users in the development of laws impacting on online use,
FIGHTING CYBERCRIME WHILE UPHOLDING FREE EXPRESSION & PRIVACY

Lillian Nalwoga - CIPESA

In her presentation, Lilian looked into the definition of "cybercrime" which she based on the one provided for in the Budapest Convention where cybercrime acts largely fall under four broad pillars that is;

• Offences against the confidentiality, integrity and availability of computer data and systems
• Computer-related offences
• Content related offences
• Copyright related offences

She noted that most national legislation on cybercrime follows the same approach, although one major issue across a number of countries, is that some of the definitions are too broad and that generally, the interpretation of cyber rights and digital rights is problematic.

The centrality of the right to freedom of expression as it is enshrined in all major international and regional human rights law instruments was flagged out as was the fact that despite being strongly guaranteed at various levels, the right continues to be violated particularly in the quest to legislate against cybercrimes as cyber laws are being used as a weapon against expression. The arbitrary arrest of dissenting voices as well as the onward use and abuse of courts of laws to stifle internet freedom was also noted as another attendant challenge to freedom of expression in countries such as Tanzania, Uganda, Burundi and Zambia.

Lilian also noted other existing challenges which include, internet disruptions and blockages in countries such as Cameroon, Uganda, the Democratic Republic of Congo, and Zimbabwe, while other countries face excessive content regulations. A limited understanding of the scope of digital rights and the lack of balance between the competing rights to privacy, freedom of expression, was also noted as perpetuating online rights violations.

Unlawful and disproportionate surveillance was also highlighted as a growing concern in countries such as Ethiopia, Zimbabwe, Kenya, Uganda, Malawi and Zambia. As with other presenters, Lilian also bemoaned the absence of data protection laws with only 22 countries in Africa out of 54 having such laws despite the increased collection of personal information by various sectors such telecommunications and banking.

3.2. The accompaniment of data protection laws with cyber-laws to ensure that there is adequate protection
• domestication of regional and international instruments by states,
• pursuit of genuine multi-stakeholderism in related dialogues;
• People-centred policy formulation and where necessary, the overhaul of legislative frameworks as a means of effectively promoting freedom of expression and access to information.
• Capacity building of MPs and CSOs
• Establishing vibrant national internet governance forum.
In conclusion, Lilian stressed the call by the United Nations Human Rights Council that “the same human rights that people have offline must be protected online” and that fighting cybercrime is a shared responsibility that is key in ensuring online security.

3.3.
ACCESS TO INFORMATION AND MEDIA FREEDOM IN A DIGITAL AGE

By Patience Zirima- Media Monitors

Patience initiated her presentation with a discussion on the centrality of media freedom and access to information to freedom of expression and emphasised how interconnected the three rights are. She noted that for example, the media needs to have freedom of expression as well as access to information in order to adequately fulfil its fourth estate role for the benefit of citizens.

Participents were also drawn to the fact that despite being amply provided for at regional and international levels, the three rights are not absolute and are subject to limitations as provided for in the Constitution for example in section 61(5). The limitations however, she must also meet set standards for example, limitation of the right of access to information must pass a three-part test that ensures that restrictions are prescribed by law; necessary in a democratic society and serve legitimate interests. The media on the other hand while it has freedom to pursue its trade, it is also expected to be responsible through fair, accurate and ethical reporting. Reportage that for example promote hate, incites war among other vices, is not protected within the scope of freedom of expression or media freedom.

Emphasis was also placed on the need for access to information and press freedom to be equally enjoyed on digital platforms as they are in legacy media. However, technological changes have also brought with them challenges of hate speech, disinformation, fake news and bullying, amongst other vices, creating headaches on what mechanisms exist or should be introduced to keep social media in check and to promote responsible use of such platforms.

Patience also focussed on the role of intermediaries as gate keepers “regulating” as and when needed, the kind of content they host or pass and noted that there are increasing calls on the need for these intermediaries to play a stronger gatekeeping role through filtering or taking down offensive content.

Because any person can now produce content online, the issue of verification of information, its accuracy and reliability, as well as accountability of social media for content shared, is also another growing concern.

Further with all the intricate aspects affecting freedom of expression and media freedom in this digital age, Patience noted that it is still critical that rights online be balanced with perceived threats to democracy and national or public interest.

Some of the important measures proffered in this pursuit, include increasing online accountability mechanisms, strengthening journalism as a counter to disinformation, as well as legislative provisions on data security and cyber security.
SESSION 4:

THEMATIC GROUP DISCUSSIONS
4.1

PERSPECTIVES TO PRINCIPLES

CYBERCRIME AND CYBERSECURITY

By Cade Zvavanjanja- Zimbabwe Internet Governance Forum [ZIGF]

The Conference participants were broken into three groups to come up with principles for consideration in coming up with legislation on cybercrime and cybersecurity, electronic transactions and on data protection. Before breaking away into the three groups, Cade gave a brief talk on principles on cybercrime and cybersecurity and related issues.

Cade defined cybercrime as “any criminal activity in which computers or networks are a tool, target or a place of criminal activity” and noted that it basically falls into two types that is, insider attacks as well as external attacks.

Cyber security on the other hand he noted, relies on various measures of security and at different levels including, information security, application security, network and internet security

He also noted that the increased dependency on computers has given way to new crimes which in turn are continually posing challenges for investigators due to their speed, anonymity and the fleeting nature of evidence. Some of the challenges he noted include:

- Preservation of digital evidence due to its chaotic form
- High possibility of malicious or unintentional alteration of the evidence without any traces left.
- The circumstantial nature of digital evidence which makes it difficult for forensic investigators to trace the systems’ activity.

As the country moves to coming up with comprehensive cybercrimes legislation, some of the key characteristics of digital evidence to bear in mind include that it must be; believable, reliable, admissible, authentic and complete. Another important aspect is the fragility of digital evidence which should also be borne in mind especially for purposes of collection and use of digital evidence.

The different types of electronic data are also distinguishable as including volatile, transient, fragile and non-volatile data. It also includes temporarily accessible, active, archival, back up, residual as well as metadata and it is critical that all these classes of data are borne in mind in the discourse on enhancing cyber security.

Cade Zvavanjanja concluded by reiterating the key issues for consideration on principles of cybercrime and cyber security which include; jurisdiction, admissibility of evidence, legislative compliance amongst others.

4.2

FEEDBACK FROM THEMATIC GROUP DISCUSSION

Below are the proposals made for consideration s principles for each of the three Bills. as follows:

1. Proposed Principles on the Electronic Commerce and electronic transactions Bill Major threats in relation to the Bill
• Unlawful sharing or over sharing of electronic information for example by banks or telecommunications companies. Sharing of information should be limited.
• Lack of personal liberty on how, when and how much of electronic money one can spend.
• Phishing
• Snooping
• Profiling, based on information provided
• Over surveillance by the state
• Use of information beyond what it was collected for, for example by the state for example through the ‘know your customer” program that banks have.

Benefits/ opportunities

• An e-commerce and e-transaction law would assist the government by facilitating information that can be used in fiscal planning.
• Such information can help the government to understand how people spend their money.
• Information collected would also help the government to put in place measures to curb illicit money flaws.

Principles for the Bill

• The Bill should facilitate good faith and ease of doing business.
• It must provide for financial oversight mechanism.
• Regulation of electronic transactions must be governed by international standards and benchmarks such as the Basel 3 standards for the banking system.
• The Bill must also enhance confidence in Zimbabwe as a market, including facilitating Zimbabwe’s linkage to the international financial and banking systems.
• The Bill must also speak to other laws such as the Reserve Bank of Zimbabwe Act and the Banking Act.
• It must also facilitate the use of modern systems such as SAMSUNG pay.

2. Proposed Principles on the Cybercrime and Cybersecurity Bill Broad assessment

• Law officers, the Judiciary as well as Parliamentarians need capacity building in relation to this Bill’s scope and implications before it is debated in Parliament.
• A multi stakeholder consultation and endorsement is required before the Bill is finally adopted.
• A multi-stakeholder input is also needed in coming with benchmarks on online content, as well as drawing from approaches employed by other jurisdictions.
• Efforts to obtain buy in from all affected stakeholders must be taken and intensified.

Principles

• The Bill needs a clear definition of Cybercrimes which is broad enough and which is benchmarked on international standards.
• The Bill must have measures to deal with fake news and misinformation, more-so as the cyberspace provides real-time sharing of information.
• The Bill must list and fully define all cybercrimes.
• The name of the Bill is too long and threatening and instead, it should be renamed the Cyber security Bill.
• The Cybercrimes Bill must be guided by and be in sync with the Constitution of Zimbabwe
• The bill must also have provision for retraction of defamatory statements as a remedy.
• The proposed penalties must be proportionate with potential harm that can be suffered and not be too lenient
• For system errors or data breaches, there should be set timeframes within which information holders inform the data subjects that their data has been breached or lost.

3. Proposed principles on the Data Protection Bill

• The Bill must provide adequate protection against possible abuse of data by state entities.
• The Bill must clearly outline the consequences that accrue to anyone in the event of abuse of personal data
• The Bill must also include measures that protect against abuse or unwarranted use of data which falls outside the scope of any investigation that may be under way.
• Once passed, the Bill must be regularly reviewed in line with prevailing trends and standards
• Laws that compel the submission of personal data such as for SIM card registration and for opening bank accounts must be tightened to provide adequate protection against abuse of collected data

4.3 CONCLUDING REMARKS

Kuda hove concluded the meeting by stressing that all the input made during the Conference would be collated together for future use particularly as part of CSO submissions in relation to each Bill. He also promised participants that once ready, the Conference report would be available for collection as hard copies or for downloading online.
<table>
<thead>
<tr>
<th>ACRONYMS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALR</td>
<td>Centre for Applied Legal Research</td>
</tr>
<tr>
<td>CIPESA</td>
<td>Collaboration on International ICT Policy in East and Southern Africa</td>
</tr>
<tr>
<td>CSOs</td>
<td>Civil Society Organisations</td>
</tr>
<tr>
<td>POTRAZ</td>
<td>Postal and Telecommunications Regulatory Authority</td>
</tr>
<tr>
<td>ZIGF</td>
<td>Zimbabwe Internet Governance Forum</td>
</tr>
<tr>
<td>ZIMURA</td>
<td>Zimbabwe Music Rights Association</td>
</tr>
<tr>
<td>ZRP</td>
<td>Zimbabwe Republic Police</td>
</tr>
</tbody>
</table>