Joint Civil Society Statement: Cyber Security, Cyber Crime, and Anti-Terrorism Bills at MISA HOUSE on December 5th 2024

The undersigned civil society organisations (CSOs) would like to set out why they are opposed to the enacting of the Cyber Security, Cyber Crimes and Anti-Terrorism Bills currently before Parliament, in their current form.

In opposing the enactment of these Bills and calling for their withdrawal from Parliament, we the undersigned CSOs would like to emphasise that we understand and support the need for regulation of cyber space for the protection of citizens and the nation.

The concern of the CSOs, therefore, is not that the use of cyber space will be overseen by justiciable laws but that the three Bills, as they have been drafted, are in fundamental ways an affront to democracy and citizen rights.

It is our view that the Bills represent a proposal to:

1. Give the Republican President inordinate and undemocratic power over citizens utilisation of the internet.
2. Give the President and therefore powerholders unjustified and barely fettered access to the private communication of citizens, political parties and all entities that use the internet in the country.
3. Grant extensive surveillance powers of citizens, citizen groups and enterprises to the state without clear accountability or justification.
4. Create vaguely defined crimes that carry highly punitive consequences.
5. Supress freedom of expression and dissent.

This statement will proceed to provide non-exhaustive examples of the above:

- The Cyber Security Bill in Section 3 (1) seeks to establish "the Zambia Cyber Security Agency in the Office of the President which is to be responsible for the administration of the Act under the general direction of the President. The Zambia Cyber Security Agency therefore operates under the direct control of the President, granting sweeping powers with minimal checks and balances.
- In instituting the Cyber Security in the Presidency, the Act accords the president unfettered powers to appoint the Director General of the Agency and all its staff.

Our concern *is that an already too powerful Presidency, be granted the authority to oversee how citizens and the country in general utilises the internet which is now the primary vehicle for all commerce, education and information?* The unchecked oversight *risks political interference and undermines independent governance.*

The President is envisaged by the Bill to have unchecked powers to appoint the watchdogs of the internet who as will be shown later can intercept any communication between any parties in the country on very vague justifications.

International Benchmark: Best practices, such as the UK's National Cyber Security Centre, ensure independence from political control.

Implication: Risks political interference and undermines independent governance.

Recommendation: Restructure the Agency to function independently, with oversight by a parliamentary committee and judicial review of decision

- The Cyber Security and Cyber Crimes Acts if passed as proposed would be primarily overseen by law enforcement officers. Most troubling to the CSOs is that the Bill proposes that the proposed law enforcement officer can among other members of recognised agencies such as the Anti-Corruption and Drug Enforcement Commissions can astoundingly be **any other person appointed as such by the President.**

- The law enforcement officers, if they believe, on undefined reasonable grounds, that a crime has been, is about to, or is likely to be committed are given the excessive power to request a judge ex-parte (without the accused being heard) to be given permission to:

a) intercept communication.
b) require an electronic communications service provider to intercept and retain specified communication or communications of a specified description received or transmitted, or about to be received or transmitted by that electronic communications service provider
c) to enter premises and retrieve computers and data. (Computers include phones)
d) force individuals not accused of any crime (such as IT staff) to assist the law enforcement officer to access computers and retrieve data.

Concern *- These powers that can be utilised on vague reasonable grounds are excessive for recognised law enforcement officer. They can then be accorded to* ***anyone*** *the President might appoint up as a law enforcement officer. Nothing in this law prevents that person from being a functionary of the ruling party serving only the President's interests.*

- The Cyber Security Bill, Section 21: establishes a Central Monitoring Centre to manage interception but lacks provisions for data security or retention limits and protection of intercepted data. In other words, how intercepted data kept used or further transmitted is out of the hands of the owner even if they are found not guilty of an offence.

Concern*: This provision enables mass surveillance, disproportionately affecting activists, journalists, and political opponents.*

Treaty Reference: This Violates Article 17 of the ICCPR on privacy and Article 19 on freedom of expression.

Recommendation: Require explicit judicial authorization for all interceptions and limit conditions to cases of verified threats.

The Cyber Crimes Bill, Section 21(1) (b): criminalises the initiation of the transmission of multiple electronic messages from or through a computer or computer system. Penalizes sending multiple electronic messages without clear thresholds or intent requirements. This is over criminalization of Messaging

Concern: *This means an individual or business could be charged for sending messaged to a number of recipients. Important to note is that the offence envisaged is not that the content of the message may be criminal, but the simple fact that the message targets multiple people. This*

provision alone would would suppress CSO, campaigns, political activities, and legitimate business communications and therefore handicap CSO work It would also make normal use of smart phones by citizens criminal.

Recommendation: Define criteria for offenses and require intent to harm.

- Overbroad Definitions and Criminalization (Clause 3 of the Cyber Crimes Bill: Unauthorized Access)

The provision criminalizes any 'unauthorized' access to computer systems without specifying intent or harm.

***Concern**: Legitimate activities such as ethical hacking, cybersecurity testing, or whistleblowing may inadvertently fall under this provision.*

Recommendation: Include exemptions for good-faith security research and whistleblowing in the public interest.

- Section 26 of the Cyber Crimes Bill prohibits cyber terrorism. Cyber Terrorism is defined in the Bill and the provision may be used to penalise legitimate expression of discontent on government or social practices. Further the clause references offences under the Anti Terrorism Act of which an Amendment is currently before Parliament definition does ensure adequate protection for legitimate protest under a computer system.

***Concern** The threat to freedom of expression is that the provisions are open to interpretation by law enforcement agencies who have been shown to act in the interest of the ruling party.*

Recommendation must provide adequate protections for legitimate protests and actions using a computer system. The provisions must set out clear parameters for what constitutes the offence when exemptions apply.

As stated above, this list of concerns is not exhaustive. These are selected exemplifications of the undemocratic, stifling power the Cyber Security, Cyber Crimes and Anti-Terrorism Bills seek to grant to the state. Powers that can and very probably would be used against citizens, CSOs, critical voices and political rivals.

The undersigned CSOs, again, call for the withdrawal of these Bills that would abrogate both the constitution and citizen rights. This would allow for broad consultation and the drafting of cyber legislation that respects democratic principles, citizen rights and protects the nation.

Issued and signed by: Laura Miti – Executive Director, Alliance for Community Action for and on behalf of:

Laura Miti

Alliance for Accountability Advocates Zambia (AAAZ)

Advocates for Democratic Governance Foundation (ADEG)

Chapter One Foundation (COF)

Alliance for Community Action (ACA)

Caritas Zambia (CZ)

Council of Christian Churches in Zambia (CCZ)

Peoples' Action for Accountability and Good Governance in Zambia (PAAGZ)

Transparency International Zambia (TIZ)

Zambia Council for Social Development (SCSD)

Free Press Media

MISA Zambia

PANOS Institute Southern Africa

Common Cause Zambia

Contact:

Email: info@acazambia.org

Phone: +260 977 319119

End of Statement