Analysis of the Zambia Cyber Crimes Bill, 2024 and Cyber Security Bill, 2024

Zambia has published the Cyber Security Bill, 2024 and the Cyber Crimes Bill, 2024, which would repeal the Cyber Security and Cyber Crimes Act of 2021. These proposed laws' objective of combating cyber crimes and promoting a safe and healthy digital society is welcome, as is the need for the country to strengthen its cyber security posture, including through legislation.

However, the current drafts of the laws not only miss the opportunity to cure some of the deficiencies in the 2021 cyber crimes law but introduce several, more regressive provisions.

In this Analysis of the two Bills, the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) and Bloggers of Zambia, on behalf of the Zambia CSO Coalition on Digital Rights point to the retrogressive and vague provisions in the two Bills, and offer recommendations that can make render the proposed laws more robustly rights-respecting and effective in combating cyber crimes.

Progressive Provisions

1. **Separation of cybersecurity and cybercrime functions:** The two bills depart from the current law, by separating the cybersecurity aspects from the criminal aspects.

2. **Structured cybersecurity governance:** The Cyber Security Bill establishes dedicated bodies such as the Cyber Security Agency and the Cyber Incident Response Teams (CIRTs). It also emphasises the importance of protecting critical information infrastructure (CII), and introduces regulatory oversight over cybersecurity service providers, all of which strengthen the country's cybersecurity posture.

3. **International cooperation:** The bills provide a framework for mutual legal assistance and cooperation with foreign entities. Definitions of some of the offences are aligned with international standards which are useful in combatting transnational/cross-border cybercrimes.

4. **Procedural framework for investigations:** The bills provide a procedural framework for investigating cybercrimes, including data preservation, access to stored information, and digital evidence handling.

5. **Addressing emerging cyber threats:** The bills introduce new offences in response to emerging cyberthreats, for example identity-related crimes, attacks on critical information infrastructure, cyber harassment, cyber terrorism, and "revenge pornography".

Main Issues and Concerns

1. **Weak Human Rights and procedural safeguards:** The bills do not affirm adherence to regional and international human rights standards and obligations, such as privacy, freedom of expression, access to information, or due process. Also, enforcement measures lack comprehensive human rights and due process safeguards to ensure provisions and practices are proportionate, necessary, and pursue legitimate aims.

2. **Potential for abuse of power:** The bills provide law enforcement agencies significant discretion in applying their provisions, thereby increasing risks for political interference, unchecked surveillance and the widespread targeting of dissenters. These are aided by broad surveillance powers and ambiguous definitions of terms and offences, which create room for subjective interpretation and arbitrary application. These could be used to suppress freedom of expression and legitimate public discourse.

3. **Weak oversight and governance:** There are limited independent or judicial review processes mandated for surveillance, data collection, or search and seizure activities. Further, the centralised control of the Cyber Security Agency and Central Monitoring and Co-ordination Centre (CMCC) and the absence of independent oversight mechanisms raise accountability concerns. Also, there is no clear separation of cybersecurity functions from the cybercrime-related functions between the two bills, which could lead to duplication and implementation challenges. There is no clear recognition of the role of the Zambia Data Protection Commission (ZPC).

4. **Overly broad surveillance powers:** Law enforcement is granted broad interception powers including real-time data collection and communication interception and extensive search-and-seizure powers. The provisions do not include clear limits or provide sufficient safeguards such as judicial oversight, proportionality, or transparency and accountability.

5. **Insufficient safeguards for privacy:** The bills enable widespread surveillance and interception without clear provisions on data retention limits, purpose limitation, secure handling of intercepted data and oversight. This could allow for indefinite storage of data, increasing the risk of misuse or unauthorised access. Also, the absence of anonymity protections for whistleblowers, journalists, and researchers could criminalise legitimate anonymous or pseudonymous activities. The provisions limit privacy rights, and are in total disregard of the country's Data Protection Act, 2021.

General Recommendations

1. Provide adequate human rights and procedural safeguards: The bills lack robust protections for privacy, freedom of expression, access to information and procedural fairness. Incorporate a dedicated section affirming the bills' compliance with Zambia's constitutional and international human rights obligations. Further, align the bills with the *Declaration of Principles on Freedom of Expression and Access to Information in Africa* and the African Union Convention on Cybercrime and Personal Data Protection. Conduct a Regulatory and Human Rights Impact Assessment and require periodic review of the bill's implementation for potential human rights impacts.

2. Strengthen oversight and governance mechanisms: Introduce mandatory independent judicial oversight, notification and documentation and annual reporting requirements on the use of powers under the bill, ensuring accountability and public trust. Additionally, establish independent oversight mechanisms for the Cybersecurity Agency, CMCC and surveillance practices. Furthermore, review the structure and functioning of the newly established agencies vis-a-vis the roles of other agencies e.g. Office of the President, Ministry of ICT, Zambia Information Technology Authority (ZICTA), security agencies, among others, to enhance coordination and avoid duplication of roles and fragmentation. It is also important to have clear delineation of cybersecurity functions and cybercrime functions to avoid confusion or duplication of roles.

3. Ensure proportionality: Many offences in the Cyber Crimes Bill criminalise minor or vague conduct without proportionality thresholds. Introduce proportionality clauses limiting criminalisation to significant harm, or graduated scales that enhance penalties based on severity, complexity and impact of offences on victims, critical infrastructure or organisations.

4. Invest in capacity building: Provide a framework for training of law enforcement, prosecution and judiciary officials on applying the law proportionately, balancing enforcement with human rights protection.

5. Ensure compliance with data protection laws: Ensure that the bills align with the provisions of Zambia's Data Protection Act, 2021, to protect individuals' privacy rights.

The Cyber Crimes Bill, 2024

Clause No.	Issue/Concern	Proposal/Recommendation	Justification
Section 2: Definitions	A number of terms are accorded the meaning in the Cyber Security Bill, 2024. However, most of these provisions are problematic with overly bearing negative impact on human rights and freedoms in the online spaces. They are largely vague and ambiguous. Some of them present opportunities for discretionary interpretation, which increases the chances of abuse of these provisions to suit the interests of favoured individuals such as politicians and those appointed into leadership positions of various government agencies. Among the terms of concern are: "law enforcement officer," "critical information," "critical information infrastructure," "internet connection record".	Retain the definition in Cyber Security and Cyber Crimes Act 2021 which defined a law enforcement officer in section 2 to include a "police officer above the rank of sub-inspector". The parameters and safeguards of critical information application should be clearly defined and precisely limited to personal data or national security data. In the alternative, it should be limited to "critical information infrastructure". Delete the entire definition of the internet connection record. In the alternative, the definition should be limited to the known parameters including internet protocol addresses and the name of the internet service provider.	While the wide definitive scope could be literally interpreted to expand the effectiveness, it creates ambiguities in the chain of enforcement and may create room for abuse of office by unscrupulous officials seeking to take advantage of the law.
Section 3: Prohibition of Unauthorised Access to Computer Systems	This section broadly criminalises unauthorised access to computer systems, risking the prosecution of ethical hackers and cybersecurity researchers who act in good faith to identify vulnerabilities.	Incorporate explicit exemptions for ethical hacking, penetration testing, and other good-faith cybersecurity activities authorised by system owners or researchers, e.g. penetration testing, to encourage responsible vulnerability reporting.	Ethical hackers play a crucial role in identifying and mitigating security vulnerabilities, and preventing exploitation by malicious actors. The *EU's NIS2 Directive* includes safe harbour provisions that protect researchers acting in good faith. It is important to balance cybersecurity enforcement with innovation and protection.

Section 4: Unauthorised Interference with Data or Computer Systems	The provision does not differentiate between minor infractions and significant disruptions, potentially criminalising actions without substantial harm. The provision could criminalise actions such as modifying or altering software for legitimate purposes, including repairing or improving systems.	Introduce a proportionality clause to limit criminal liability to cases causing significant harm or committed with malicious intent. Add exceptions for authorised maintenance, upgrades, or actions aimed at improving system functionality, provided there is owner consent.	Global best practices, such as **Article 5 of the** *Budapest Convention,* emphasise proportionality to prevent penalising minor or accidental infractions. This would ensure enforcement targets only serious cyber threats. This also ensures that IT professionals and system administrators are not inadvertently penalised while performing legitimate work. There is a need to differentiate between harmful and legitimate uses of technology.
Section 5: Unauthorised Disclosure of Data Relating to Critical Information or Infrastructure	The section may conflict with whistleblower protections, penalising disclosures intended to expose wrongdoing or protect public interest.	Introduce a whistleblower protection clause to exempt disclosures made in good faith, where such disclosures reveal corruption, negligence, or threats to public safety.	Encouraging ethical disclosures promotes transparency and accountability without compromising the protection of critical infrastructure.
Section 7: Illegal Acquisition of Data	This section could criminalise journalistic investigations or academic research involving proprietary or sensitive data.	Create exceptions for academic, journalistic, and public-interest research conducted ethically and responsibly.	Journalistic and research activities often involve accessing sensitive data but are critical for public awareness and academic progress.

Section 10: Prohibition of Recording Private Conversations	This section contains overly broad language that could be used to suppress or restrict legitimate journalistic investigations or public-interest whistleblowing activities aimed at exposing corruption or other public-interest concerns.	Add a public interest exemption allowing recordings for exposing reporting on corruption, crime, or other matters of significant public interest.	Balancing privacy rights with the public's right to know is crucial. Exemptions for public interest would ensure that critical journalistic and whistleblower activities are not unduly penalised. The *Johannesburg Principles on National Security and Freedom of Expression* stress the importance of protecting public interest disclosures. Without exemptions, this provision risks stifling freedom of expression and investigative journalism.
Section 11: Misuse of Devices	The prohibition of tools capable of hacking fails to distinguish between malicious intent and legitimate cybersecurity research.	Include explicit exemptions for authorised users, researchers, and developers conducting cybersecurity assessments.	The *UN Draft Cybercrime Convention* **(Article 11(2))** provides a clear precedent by exempting tools used for lawful purposes, ensuring legitimate cybersecurity activities are not criminalised.
Section 14: Identity-Related Crimes	Broad language could criminalise pseudonymous online activities, including advocacy or activism by individuals seeking safety. It also lacks clarity on criminal intent or specific safeguards against the misuse of identity-related provisions.	Clarify definitions of identity misuse. Add protections for legitimate anonymous or pseudonymous activities. Clarify that anonymity or pseudonymity for legitimate purposes, such as whistleblowing or personal safety, is not a crime. Define criminal intent explicitly and ensure safeguards against misuse.	Protecting anonymity is essential for free expression, especially for vulnerable individuals or those exposing wrongdoing. The **UN Special Rapporteur on Freedom of Expression** has emphasised the importance of protecting anonymity to enable free expression, particularly for vulnerable groups.

Sections 17, 18 and 19: Prohibition of child pornography, Solicitation and Grooming	Clause 17 on prohibition of child pornography, Clause 18 on prohibition of child solicitation and Clause 19 on prohibition of child grooming are progressive provisions in as far as they protect children against pornography, sexual activity and training of children in performance of sexual activity.	While the provisions are exhaustive and may be interpreted as such due to a highly interconnected world, it would be important to add the aspect of; "importation or exportation of an image or representation of child pornography through a computer system." This will add cross-border protection to children against child pornography and will fall in line with regional commitments such as article 29 of the African Union Convention on Cyber Security and Personal Data Protection.	This provision, if implemented effectively, will help to deal with common online threats including sex predation and solicitation of children for sexual purposes. Align with the UN draft Cybercrime Convention and AU Convention on Cybersecurity.
Section 20: Prohibition of On-line Human Trafficking	Prohibition of online human trafficking using a computer or computer system by clause 20 and the highly prohibitive penalty is a progressive step in efforts that aim to deal with the vagaries of dealing with online crime including serious crimes such as trafficking in persons.	Enhance the punishment for conviction of trafficking in persons through computers or computer systems to life imprisonment since computers and the internet are currently the majorly used tools for organising crime of trafficking in persons and other trafficking crimes.	The sum effect is that once it is passed and the provisions are applied in a fair and just manner, it will lead to a check on the potential online harms that individuals suffer from cyber criminals.

Section 21: Transmission of unsolicited deceptive electronic communication	This clause makes attempts to speak to the dissemination of false information, multi-media messaging and disinformation. On the other hand, the head note refers to, among others, unsolicited deceptive communication. It is important to note that the provision is not clear and may be misleading. Additionally, the provision essentially limits the generation of content, transmission of information and freedom of expression. In its ambiguity, it has a chilling effect on freedom of expression and access to information. Similarly, Clause 21(1)(c), in as far as it prohibits establishment of a software application system, potentially limits innovation and may discourage innovators from developing applications in fear of potential arrest and prosecution.	Delete Section 21 (1) (a), (c), and (d). Reduce the fine to not exceeding one hundred thousand penalty units, or imprisonment for a term of not exceeding six months or to both.	This limitation curtails human rights and freedoms under articles 19 of the Universal Declaration of Human Rights (UDHR) and the International Convention on Civil and Political Rights (ICCPR), and article 9 of the African Charter on Human and Peoples' Rights. The 2017 Joint Declaration on Freedom of Expression and 'Fake News,' Disinformation and Propaganda noted that: *General prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression, as set out in paragraph 1(a), and should be abolished.* The High Court of **Zambia** in *Chipenzi v. The People* struck out a provision of the Penal Code that prohibited the publication of false information likely to cause public fear on the basis that it did not amount to a reasonable justification for limiting freedom of expression.
Section 22: Prohibition of use of computer or computer system for offences	This provision is ambiguous and may create instances of double jeopardy (trial of accused persons more than once over the same offence or similar charges).	Delete the entire Clause 22.	The provision may create opportunities for abuse of the justice processes by unscrupulous individuals including politicians to punish or frustrate political opponents, dissidents, government critics, human rights defenders and civil society organisations.

Section 24: Harassment, Humiliation, and Dissemination of False Information	This section could potentially criminalise freedom of expression by penalising content deemed obscene, lewd, vulgar, or defamatory without clear definitions or protections for legitimate expression or criticism. Such overly broad and subjective language could be used to criminalise dissent, satire, or criticism, infringing on freedom of expression. It creates absurdity in interpretation. The words are not clearly defined and may be interpreted to suit the needs of political figures who wish to punish those who criticise them.	Delete clause 24 (a) and (b) Clearly define what constitutes "obscene," "vulgar," or "false information" Include exemptions for satire, parody, legitimate criticism, and public-interest speech.	Overly vague language could be abused to silence dissent or criminalise legitimate expression. Clear definitions would reduce the risk of misapplication. They would also ensure that the law targets harmful conduct without suppressing legitimate expression. Criminal defamation is widely known to interfere with articles 19 of both the UDHR and the ICCPR. In 2010, the African Commission called on state parties to repeal criminal defamation laws on the grounds of interfering with freedom of expression and work of the media. *Zambia repealed its Defamation Law in 2022*, the current clause 24(2) silently but steadily re-introduces criminal defamation. A similar provision was invalidated by the **Kenyan High Court ruling in Geoffrey Andare v. Attorney General (2016)** for being vague and infringing on free speech. If the Bill is enacted with this provision, it will be a major blow to Zambia's human rights record in regard to defamation. And worse still, the clause is proposing a heavy penalty in case of a breach.

Section 25: Prohibition of Cyber Attacks	The definition of a "cyber attack" is vague and could unintentionally criminalise acts like stress testing or simulations conducted by cybersecurity professionals.	Define "cyber attack" narrowly and exempt authorised simulations or stress tests carried out for legitimate cybersecurity purposes.	Clear definitions and exceptions reduce the risk of penalising legitimate security activities.
Section 26: Prohibition of Cyber Terrorism	The section lacks safeguards against abuse, such as labelling activists or dissenters as cyber terrorists.	Require clear and substantial evidence of intent to harm national security, not just dissenting views or activism.	Safeguards ensure that the law targets genuine threats without infringing on civil liberties. Align with the Johannesburg Principles, emphasising the need for proportionality and necessity in national security measures.
Section 29: Search and Seizure	Broad powers for law enforcement to search and seize digital evidence. The provision lacks mechanisms for independent judicial oversight or proportionality principles, which could lead to abuse.	Require mandatory judicial oversight for all search and seizure actions. Specify clear thresholds for issuing warrants, and mandate data minimisation. Add proportionality requirements for all search-and-seizure operations.	Judicial oversight ensures accountability and protects against arbitrary or excessive intrusions into personal privacy. The **Budapest Convention (Article 19)** emphasises the necessity of judicial oversight to prevent overreach and protect privacy rights.
Section 32: Data Preservation	The lack of time limits for data preservation orders risks indefinite retention of personal data, violating privacy rights.	Specify and limit preservation to for example 90 days, renewable only by court order, and require notification to affected parties unless it compromises an investigation.	The **UN Draft Cybercrime Convention (Article 25)** sets clear time limits and safeguards to ensure proportionality and data minimisation.

Section 34: Real-Time Data Collection	The provision allows real-time data collection without adequate safeguards such as judicial authorisation or independent oversight. The ex parte application process for collecting traffic data risks misuse and lacks transparency, potentially infringing on privacy and due process rights.	Mandate judicial authorisation or oversight and limit real-time data collection to investigations of serious crimes. Require post-facto notification to the affected individual, unless doing so would jeopardise an ongoing investigation, and introduce regular audits of traffic data collection practices.	The inclusion of transparency and accountability mechanisms protects against misuse of surveillance powers while ensuring legitimate investigations are not hindered. The *Budapest Convention* **(Article 20)** includes safeguards against the misuse of real-time surveillance, protecting privacy and freedom.
Sections 33–35: International Cooperation	Provisions for mutual legal assistance and extradition are underdeveloped, lacking clarity on data protection and procedural safeguards.	Strengthen the framework for international cooperation by aligning with **Articles 35–46 of the** *UN Draft Cybercrime Convention* and ensuring compliance with international data protection standards. Add explicit safeguards against politically motivated extraditions and ensure fair treatment standards.	Effective international cooperation is essential for combating transnational cybercrime while upholding human rights and ensuring procedural fairness.

The Zambia Cyber Security Bill, 2024

Clause No.	Issue/Concern	Proposal/Recommendation	Justification
Section 1: Objectives	The objectives lack explicit commitment to protect human rights or fostering international cooperation on cybersecurity. Their disproportionate focus on state security may lead to curtailment of individual freedoms.	Amend the objectives to explicitly state the commitment to human rights protection (a rights-based approach) and promotion of international cooperation on cybersecurity.	Aligning with international instruments strengthens international collaboration and ensures compliance with global human rights standards. The **Draft UN Declaration on Freedom of Expression** emphasises the primacy of human rights in digital governance. The **Budapest Convention (Article 2)** and **Draft UN Cybercrime Convention (Article 6)** require cybersecurity measures to respect human rights.
Section 2: Definitions	Key terms such as traffic data, content data, subscriber information and cybersecurity risk are missing. Others, such as law enforcement officers, call-related information, critical information, internet connection record, are broad, vague and imprecise. For example, a law enforcement officer includes "any other person appointed by the president". These hinder legal clarity, create legal ambiguity, potentially leading to overbroad application, surveillance or data misuse.	Incorporate precise definitions from the **Budapest Convention (Article 1)** and **Draft UN Cybercrime Convention (Article 2)** of: Traffic Data, Content Data and Subscriber Information. Consider restricting powers to a police officer instead of a law enforcement officer, and move to the Cyber Crimes Bill. Delete internet connection record, or limit definition to known parameters.	Consistency in terminology facilitates international cooperation and legal clarity. Clear definitions protect against arbitrary or intrusive data processing and align with international norms. It is important to have clear delineation of cybersecurity and cybercrime functions. Officers of anti-corruption or drug enforcement have no role in promoting cybersecurity. Yet they may have a role in investigating crimes.

Part II: Zambia Cybersecurity Agency	Centralised Control given the Agency's placement under the President's Office risks executive overreach and political interference. The unilateral appointment of the Director risks compromising the integrity and professionalism of the office-holder. Furthermore, there is insufficient judicial oversight or public accountability mechanisms for decisions made by the Agency (Clause 4). Decisions of the Agency should be subject to judicial review to prevent abuse of power or excesses.	Make the Agency an independent body answerable to Parliament, with obligations to report on a regular basis. Decisions of the Agency should be subject to judicial review to prevent abuse of power or excesses. Clarify the role of the Agency vis-a-vis ZICTA's role in Cybersecurity matters. The appointment of the Director-General should be a competitive process to ensure professionalism. This should be subject to ratification by parliament.	This ensures checks and balances and builds public trust. Also, where there are multiple institutions with a role in cybersecurity, fragmentation could occur. Several examples of similar setups show that those agencies are not independent, and could be subject to political, financial, commercial and other interests.
Part III: Cyber Incident Response Teams	The Agency has no diverse membership or the same has not been explicit on who constitutes the "Team". Overly broad powers are granted to the CIRT in handling cyber incidents, including the power to access, monitor, and seize computer systems (Clause 56). There is no clear limitation on the scope of these powers, which could lead to abuse, especially in political cases or in matters involving dissent or critical and oppositional voices. This can lead to disproportionate invasions of privacy.	Provide for multistakeholder composition and roles of the CIRT, and the sector CIRTs. Proportionality and necessity principles must be explicitly stated in the Bill to ensure the Agency's actions are limited to cases where there is a legitimate threat. All search and seizure actions by the Agency must be subject to judicial authorisation, as required under Article 17 of the ICCPR and Article 17 of the Republican Constitution of Zambia (Right to Privacy). In accordance with accepted best practices, for accountability, there should be a limit on the duration and scope of monitoring powers and the Agency should be required to publish regular reports on how these powers are used.	It is important for CIRTs to have multistakeholder membership and to be supported in the role.

Part IV: Protection of Critical Information Infrastructure	The Agency has unilateral power to designate infrastructure as "critical," risking overreach. The Bill does not mandate stakeholder consultation or provide for regional cooperation on protecting critical infrastructure. Lack of stakeholder consultation and transparency in designating critical infrastructure may result in arbitrary restrictions on digital services. The offences under the section are punitive.	Require transparent criteria for designating critical infrastructure. Require judicial or legislative review for such designations. Include provisions for mandatory stakeholder engagement before designation of infrastructure. Require a study/assessment to be conducted of critical information infrastructure and their impact on the country, utilising the evidence as a basis for engagement and designation.	Transparency mitigates risks to service providers and users. The **AU Convention (Article 29)** encourages regional cooperation in securing critical infrastructure. The **Budapest Convention (Article 2)** promotes transparency and accountability in safeguarding such systems.

Part V: Interception of Communications	The Bill continues the activities of the Central Monitoring and Co-ordination Centre. However, the Centre's supervision and oversight is weak. The lack of independent oversight mechanisms for monitoring the use of interception powers undermines accountability. The Bill grants broad interception powers with minimal safeguards, no judicial oversight, risking abuse and violation of privacy rights. Also, the lack of transparency mechanisms can result in unchecked surveillance. Service providers are required to install systems capable of being intercepted (s.39).	Require judicial authorisation for all interception activities and establish oversight mechanisms. Limit interception to cases where it is necessary and proportionate, with safeguards for data retention and deletion. Introduce clear time limits and reporting obligations. Require a high threshold for lawful interception, including evidence of a legitimate and compelling need or a crime being committed under a specific law. Introduce mandatory reporting and independent oversight mechanisms to monitor the use of interception powers. Abolish s.29(9) which bars rights to remedy. Abolish s.30 which allows oral interception requests. Require retrospective judicial review within 24 hours of any emergency interception order/request. Provide a clear threshold for emergency interception powers to clearly defined and time-bound emergencies. Establish an independent oversight body to monitor interception activities, with powers to audit interception requests and approvals, investigate complaints from affected individuals, and to publish periodic transparency reports. Consider moving the provisions to the Cyber Crimes Bill.	Interception of communication is an investigatory /criminal justice function, which should be under the cybercrime bill and not the cybersecurity bill International best practices require independent oversight in safeguarding privacy and human rights in lawful interception operations. The **Malabo Convention (Article 25)** mandates judicial review for surveillance activities. The **Budapest Convention (Article 15)** and **Draft UN Cybercrime Convention (Article 24)** emphasise proportionality and judicial oversight to prevent abuse.

Part VI: Licensing of Cybersecurity Providers	Overregulation risks stifling innovation and excluding smaller or non-profit entities from participating in cybersecurity solutions. Licensing requirements could marginalise small and medium enterprises (SMEs).	Simplify licensing requirements and provide exemptions for SMEs and non-profit organisations. Establish a tiered licensing framework proportional to provider size and scope. Introduce provisions for licensing cross-border service providers.	This encourages innovation while maintaining oversight.
Part VII: International Cooperation	The Bill lacks detailed provisions for mutual legal assistance, expedited data preservation, and cross-border investigations. Lack of detailed frameworks for cross-border cooperation could undermine efforts to combat transnational cybercrime and protect privacy.	Include specific protocols for Mutual legal assistance (Articles 27-32, **Draft UN Cybercrime Convention)**; Expedited data preservation (Article 25, **Budapest Convention)**; and data sharing with privacy safeguards (Article 36, **Draft UN Cybercrime Convention**).	International cooperation is critical to enhance Zambia's ability to combat transnational cybercrime effectively, and fulfil its obligations under the Malabo Convention (Article 30) for regional cooperation.
Part VIII: Inspectorate	The bill adopts a securitised approach to cybersecurity through the office of the inspectorate. The section does not incorporate explicit conditions and safeguards for procedural measures. Also, the broad search and seizure powers means that Inspectors can access private systems arbitrarily and without judicial oversight. No explicit requirement for the interception warrant to be specific and limited in scope. Risk of broad or blanket warrants that infringe on privacy rights.	Make judicial warrants mandatory for all investigations. Ensure warrants are specific, including details such as targeted individuals or entities, type of data to be intercepted and time limitations. Prohibit bulk interception or untargeted surveillance. Require owners of critical infrastructure to put in place measures to safeguard their cybersecurity, including appointing Infosec officers, conduct independent external audits from credible/licensed cybersecurity companies, among others.	This is important to prevent arbitrary actions and safeguards individual rights. The approach to establish an Inspectorate is retrogressive as cybersecurity is an ICT function. Most organisations need support, capacity building and awareness not the stick approach. See the Draft UN Cybercrime Convention (Article 24).

Part IX: General Provisions	The Bill provides law enforcement with broad procedural powers (search, seizure, data retention) without adequate safeguards which threaten privacy and due process rights. There are no provisions for proportionality, judicial oversight, or clear time limits. There is limited protection for misuse, and no penalties for misuse of powers by officials.	Incorporate safeguards, including judicial oversight or independent review; proportionality and necessity as guiding principles; and clear limitations on scope and duration of procedural measures, including for data retention and access. Include penalties for officials who abuse their powers under the Act. Require judicial/court warrants to be specific, limited and detail the scope, person, time frame, substance/content of search and seizure activities. Search and seizure powers for law enforcement should be restricted to the cyber crimes law. Use the term police officer, instead of a law enforcement officer.	Law enforcement must respect human rights and due process. These safeguards align with the Budapest Convention (Article 15) and the Draft UN Cybercrime Convention (Article 24). The term law enforcement officer is so broad, and does not specify for precision, who such a person is or is not.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 10B Katalima Crescent, Naguru.| P.O.Box 122311,Kampala (U)
+256 414 289 502| programmes@cipesa.org| @cipesaug
www.cipesa.org