REPUBLIC OF ZAMBIA

REPORT

OF THE

JOINT COMMITTEE OF THE

COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES

AND

THE COMMITTEE ON NATIONAL SECURITY AND FOREIGN AFFAIRS

ON THE

CYBER SECURITY AND CYBER CRIMES BILL, N.A.B. NO. 2 OF 2021

FOR THE

FIFTH SESSION OF THE TWELFTH NATIONAL ASSEMBLY

Published by the National Assembly of Zambia

REPORT

OF THE

JOINT COMMITTEE OF THE

COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES

AND

THE COMMITTEE ON NATIONAL SECURITY AND FOREIGN AFFAIRS

ON THE

CYBER SECURITY AND CYBER CRIMES BILL, N.A.B. NO. 2 OF 2021

FOR THE

FIFTH SESSION OF THE TWELFTH NATIONAL ASSEMBLY

TABLE OF CONTENT

REPORT OF THE JOINT COMMITTEE OF THE COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES AND THE COMMITTEE ON NATIONAL SECURITY AND FOREIGN AFFAIRS ON THE CONSIDERATION OF THE CYBER SECURITY AND CYBER CRIMES BILL, N.A.B. NO. 2 OF 2021.

1. MEMBERSHIP OF THE COMMITTEE

The Committee consisted of Dr M Malama. MP (Chairperson); Mr G M Imbuwa, MP; Ms P Kucheka, MP; Mr D M Kundoti, MP; Mr M Mukumbuta, MP; Dr E I Chibanda, MP; Mr M K Tembo, MP; Dr F Ng'ambi, MP; Mr D Mumba, MP; Mr C D Miyanda, MP; Mr G K Chisanga, MP; Ms A M Chisangano, MP; Mr E J Muchima, MP; Brig Gen S M Sitwala, MP (Rtd); Mr K Mbangweta, MP; Mr L Nyirenda, MP; Ms M Miti, MP; Mr A Malama, MP; and Ms M Lubezhi, MP.

The Honourable Mr Speaker
National Assembly
Parliament Buildings
LUSAKA

Sir,

The Joint Committee has the honour to present the Report on the on the Cyber Security and Cyber Crimes Bill, N.A.B. No. 2 of 2021, for the Fifth Session of the Twelfth National Assembly referred to it by the House on Tuesday, 9th February, 2021.

3. MEETINGS OF THE COMMITTEE

The Committee held ten meetings to consider the Cyber Security and Cyber Crimes Bill, N.A.B. No. 2 of 2021.

4. PROCEDURE ADOPTED BY THE COMMITTEE

In order to fully appreciate the ramifications of the Bill, the Committee requested written submissions from various stakeholders. The stakeholders were further requested to virtually appear before the Committee to orally brief it on the contents of their written memoranda and clarify issues that arose from the presentations. The list of witnesses who appeared before the Committee is at Appendix II of this Report.

5. BACKGROUND TO THE BILL

The African Union Convention on Cyber Security and Protection of Personal Data was adopted by the Assembly of Heads of State and Government of the African Union in

June, 2014. On 29th January, 2016, the President of the Republic of Zambia signed the African Union (AU) Convention on Cyber Security and Protection of Personal Data during the 26th Ordinary Session of the Assembly of Heads of State and Government of the AU. The AU Convention addressed four main areas, namely:

i) electronic transactions;
ii) personal data protection;
iii) electronic commerce; and
iv) cyber security and cyber crime

The Convention provided a guideline for Member States to formulate appropriate legal frameworks that would empower their citizens and ensure their respective online environment was trusted, safe, beneficial and empowering to all individuals.

In 2017, the Government, through the Ministry of Transport and Communications commenced the process of reviewing the *Electronic Communications and Transactions (ECT) Act, No 21 of 2009,* in line with the AU Convention on Cyber Security and Data Protection and in harmonisation with the proposed SADC model laws.

In 2018, the Government approved the repeal of the *Electronic Communications and Transactions Act, No 21 of 2009,* and the replacement of the Act with three standalone laws that would be in line with regional and international best practice and would be responsive to the needs of the Zambian people. Therefore, the ECT Act of 2009, was to be repealed and replaced with the following laws:

(a) Electronic Communications and Transactions Act
(b) Data Protection Act; and
(c) Cyber security and Cyber Crimes Act.

In the fourth quarter of 2019, Cabinet approved the Ratification of the Convention on Cyber Security and Data Protection (Malabo Convention) and approved the presentation before Parliament of two Bills, namely: Data Protection Bill and Electronic Communications and Transactions Bill. Further, Parliament in November 2020 also approved the ratification of the Convention.

In view of this, the Government introduced the Electronic Communications and Transactions Act, No 2 of 2021**.**

6. OBJECTS OF THE BILL

The objects of this Bill were to:

(a) ensure the provision of cyber security in the Republic;

(b) provide for the protection of persons against cyber crime;

(c) provide for child online protection;

(d) facilitate identification, declaration and protection of critical information infrastructure;

(e) provide for the collection of and preservation of evidence of computer and network related crime;

(f) revise the admission, in criminal matters, of electronic evidence;

(g) provide for registration of cyber security services providers; and

(h) provide for matters connected with, or incidental to, the foregoing.

7. SALIENT PROVISIONS OF THE BILL

PART I

7.1 Preliminary provisions

Clause 1 – Short title and commencement

This clause sought to provide for the short title and date of commencement of the Bill.

Clause 2 – Interpretation

This clause provided for the definition section which sought to define various words and phrases used in the Bill to make the law easier to understand.

Clause 3 – Supremacy of Act

This clause sought to provide for the supremacy of the Bill to issues relating to the regulation of cyber security, cyber crimes and forensic.

PART II

7.2 Regulation of cyber security services

Clause 4 – Cyber security regulator

This clause sought to place the mandate of regulation and implementation of the provisions of the Bill on the Zambia Information and Communication Technology Authority (ZICTA).

Clause 5 – Functions of the Authority

This clause defined the functions of the Authority, some of which included the coordinating and overseeing of activities relating to cyber security and the combating of cyber crimes. It further mandated the Authority to disseminate information on emerging cyber threats and vulnerabilities as presented.

Clause 6 – Constitution of Zambia Computer Incidence Response Team

This clause empowered the Authority to constitute the Zambia Computer Incidence Response Team. The clause further provided for the role and functions of the Computer Incidence Response Team which, among other things, was to be the first point of contact with reference to handling of cyber incidents and communication between cyber security emergency response teams or cyber security incident response teams.

Clause 7 – Constitution of National Cyber Security Advisory and Coordinating Council

This clause mandated the Minister to constitute the National Cyber Security Advisory and Coordinating Council which shall, among other things, oversee the implementation of cyber security related functions of the Authority

PART III

7.3 Inspectorate

Clause 8 – Appointment of cyber inspectors

This clause provided for the appointment of cyber inspectors for the purposes of ensuring compliance with the Act.

Clause 9 – Power to inspect and monitor

This clause gave a cyber inspector the power to monitor and inspect a computer system for any unlawful activity.

Clause 10 –Data retention notice

This clause provided for the specification in the retention notice of the data by the electronic communication service provider.

Clause 11 – Power to access, search and seize

This clause gave a cyber inspector the power, with a warrant, to access and search premises and seize material in performance of the functions under the Act.

Clause 12 – Obstruction of cyber inspector

This clause made it an offence for a person to obstruct a cyber inspector from conducting a lawful search or seizure under the Act.

Clause 13 – Appointment of cyber security technical expert

This clause empowered the Director - General to appoint a cyber security technical expert to assist a cyber inspector in exercise of the cyber inspector's powers under the Act.

Clause 14 – Emergency cyber security measures and requirements

This clause gave the Minister the power to issues regulations for emergency cyber security measures.

PART IV

7.4 Investigation of cyber security incidents

Clause 15 – Power to investigate

This clause gave the cyber inspector the power to investigate where the Authority received information regarding an alleged cyber security threat or an alleged cyber security incident.

PART V

7.5 Protection of critical information and critical information infrastructure

Clause 16 – Scope of protecting critical information infrastructure

This clause provided for the scope of application of protecting critical information infrastructure.

Clause 17 – Declaration of critical information

This clause empowered the Minister to declare by statutory instrument, information which was of importance to the protection of national security, economic or social well being of the Republic as critical.

Clause 18 – Localisation of critical information

This clause provided for the localisation of critical information.

Clause 19 – Registration of critical information infrastructure

This clause provided for the registration of critical information infrastructure.

Clause 20 – Change in ownership of critical information infrastructure

Clause 20 mandated a person who intended to change ownership of the critical information infrastructure to apply for authorisation from to the Authority.

Clause 21 – Register of critical information infrastructure

This clause mandated the Authority to maintain a register of critical information infrastructure.

Clause 22 – Auditing of critical information to ensure compliance

This clause provided for the auditing of critical information to ensure compliance.

Clause 23 – Duty to report cyber security incidents in respect of critical information infrastructure

This clause mandated a controller of critical information infrastructure to report cyber security incidents in respect of critical information infrastructure.

Clause 24 – National Cyber Security exercise

This clause empowered the Authority to conduct cyber security exercises in order to test the state of readiness of owners of different critical information infrastructure in responding to cyber security incidents at the national level.

Clause 25 – Non Compliance with Part V

This clause provided for the consequence of non compliance of this Part.

PART VI

7.6 Interception of communications

Clause 26 – Prohibition of interception of communication

This clause prohibited and made it an offence to intercept any communication.

Clause 27 – Central Monitoring and Coordination Centre

This clause established the Central Monitoring Centre through which authorised interceptions in terms of the Act shall be effected.

Cause 28 – Lawful interception

This clause empowered a law enforcement officer to apply to a Judge, for an interception of communication order where that law enforcement officer had reasonable grounds to believe that an offence had been committed and also provided for the procedure for such lawful interception.

Clause 29 – Interception of communication

This clause empowered a law enforcement officer to intercept communication for purposes of preventing bodily harm, loss of life or damage to property.

Clause 30 – Interception of communication for purposes of determining location

This clause provided for the interception of communication for purposes of determining location and the procedure for the interception.

Clause 31 – Prohibition of disclosure of intercepted communication

This clause prohibited and made it an offence to disclose intercepted communications.

Clause 32 – Disclosure of intercepted communication by law enforcement officer

This clause sought to provide for instances when a law enforcement officer may disclose intercepted communication.

Clause 33 – Privileged communication to retain privileged character

This clause provided that a privileged communication intercepted did not lose its privileged character.

Clause 34 – Prohibition of random monitoring

This clause prohibited and made it an offence for an electronic communication service provider to utilise the service for observing or random monitoring.

Clause 35 – Protection of user from fraudulent or other unlawful use of service

This clause provided for the protection of **ser** from fraudulent or other unlawful use of service.

Clause 36 – Interception of satellite transmission

This clause sought to allow for the interception of satellite transmission unless the interception was for the purpose of a direct or indirect commercial advantage or private financial gain.

Clause 37 – Prohibition of use of interception device

This clause prohibited and made it an offence to use an interception device or apparatus.

Clause 38 – Assistance by service providers

This clause provided for the obligations of service providers.

Clause 39 – Duties of service provider in relation to customers

This clause outlined the duties of an electronic communication service provider in relation to customers.

Clause 40 – Interception capability of service provider

This clause sought to mandate an electronic communication service provider to provide a service which had the capability to be intercepted and to store related information in accordance with the provisions of the Act.

PART VII

7.7 Licensing of cyber security service providers

Clause 41 – Prohibition from providing cyber security services without licence

This clause prohibited and made it an offence to provide cyber security services without a licence.

Clause 42 – Application for licence

This clause mandated any person who intended to engage in a cyber security service to apply to the Authority for a licence.

Clause 43 – Renewal of licence

This clause provided for the application of renewal of a licence.

Clause 44 – Refusal to grant or renew licence

This clause provided for the procedure of grant or refusal to grant a licence.

Clause 45 – Validity of licence

This clause sought to empower the Minister to provide for the validity of a licence.

Clause 46 – Revocation or suspension of licence

The clause provided for the procedure and mandated the Authority to furnish the applicant with reasons for the revocation or suspension of a licence.

PART VIII

7.8 International cooperation in maintaining cyber security

Clause 47 – Identifying areas of cooperation

This clause provided for the identification of areas of cooperation in cyber security.

Clause 48 – Entering into agreement

This clause provided for the Republic to enter into any agreement with any foreign state and international body regarding the provision of mutual assistance and cooperation relating to the investigation and prosecution of an offence committed under this Act.

PART IX

7.9 Cyber Crimes

Clause 49 – Unauthorised access to interception of or interference with computer system and data

This clause prohibited and made it an offence to intentionally access or interfere with any data without authority or permission to do so.

Clause 50 – Illegal devices and software

This clause made it an offence for a person to produce, sell, procure for import and export illegal devices and software.

Clause 51 – Computer related misrepresentation

This clause made it an offence for a person to knowingly, without lawful excuse, input, alter, delete or suppress computer data with intent that it be considered as authentic.

Clause 52 – Cyber extortion

This clause sought to criminalise cyber extortion.

Clause 53 –Identity related crimes

This clause made it an offence for a person to knowingly, without lawful excuse use a computer system to transfer, possess or use it as a means of identification of another person.

Clause 54 – Publication of information

This clause made it an offence for a person with intent to compromise the safety and security of another person to publish information or data presented in a picture, image, text, symbol, voice or any other form in a computer system.

Clause 55 – Aiding, abetting, counselling etc

This clause made it an offence for a person to aid, abet, conceal, procure, incite or solicit another person to commit any offence under this Act.

Clause 56 – Prohibition of pornography

This clause prohibited and made it an offence for a person to produce or participate in the production of pornography using a computer system.

Clause 57 – Child pornography

This clause criminalised child pornography. Some of the offences provided for under this clause included the production of child pornography for the purposes of distribution through a computer system, selling any pornography to a child through a computer system and possessing child pornography in a computer system.

Clause 58 – Child solicitation

This clause criminalised child solicitation done through a computer system.

Clause 59 –Obscene maters or things

This clause made it an offence for a person through a computer system to make, produce or have in that persons possession, obscene drawings, painting, pictures, images, posters, emblems, photographs or videos.

Clause 60 – Introduction of malicious software into computer system

This clause made it an offence for a person to intentionally introduce or spread malicious software into a computer system.

Clause 61 – Denial of service attacks

This clause made it an offence for a person to intentionally render a computer system incapable of providing normal services to its legitimate users.

Clause 62 – Unsolicited electronic messages

This clause made it an offence for a person, knowingly and without lawful excuse or justification, to initiate the transmission of multiple electronic communications from or through a computer system.

Clause 63 – Prohibition of use of computer system for offences

This clause prohibited and made it an offence for a person to use the computer system for any activity that constituted an offence under this Act.

Clause 64 – Application of offences under Act

This clause provided for the application of offences under this Act.

Clause 65 – Hate speech

This clause made it an offence for a person to use a computer system for hate speech.

Clause 66 – Minimisation etc, of genocide and crimes against humanity

This clause made it an offence for a person to knowingly, without lawful excuse, distribute or otherwise make available through a computer system to the public material which denied, grossly minimised, approved or justified acts constituting genocide or crimes against humanity.

Clause 67 – Unlawful disclosure of details of investigation

This clause made it an offence to unlawfully disclose details of a criminal investigation.

Clause 68 – Obstruction of law enforcement officer o cyber inspection officer

This clause made it an offence for a person to obstruct or hinder a law enforcement officer, cyber inspector or any person in exercise of the powers under this Act.

Clause 69 – Harassment utilising means of electronic communication

This clause made it an offence for a person using a computer system to intentionally initiate any electronic communication, with the intent to coerce, intimidate, harass or cause emotional distress to person.

Clause 70 – Cyber terrorism

This clause made it an offence for a person to use or cause to be used a computer system for the purposes of cyber terrorism.

Clause 71 – Cyber attack

This clause made it an offence for a person to carry out a cyber attack.

Clause 72 – Cognisable offences

This clause made it an offence under this Act as a cognisable offence for the purposes of the Criminal Procedure Code.

PART X

7.10 Electronic evidence

Clause 73 – Admissibility of electronic evidence

This clause provided for the admissibility of electronic evidence.

PART XI

General provisions

7.11 Clause 74 – Appeal

This clause provided for a person who was aggrieved with the decision made by Authority to appeal to the Minister. It further provided for the appeal to the High Court where a person was aggrieved with the decision of the Minister.

Clause 75 – Search and seizure

This clause provided for the procedure of search and seizure

Clause 76 – Prohibition of disclosure of information to unauthorised persons

This clause prohibited and made it an offence for a person without consent in writing given by the Authority to publish or disclose to any person the contents of any documents, communication or information, which related to, and which had come to that person's knowledge in the course of that person's duties.

Clause 77 – Assistance

This clause mandated any person with knowledge about the functioning of the computer system that was subject of a search to provide for assistance when reasonably required and requested by the person authorised to make a search.

Clause 78 – Production order

This clause empowered a judge to issue a production order where information was required for the purposes of a criminal investigation or criminal proceedings.

Clause 79 – Expedited preservation

This clause empowered a law enforcement officer to preserve data for a specified period.

Clause 80 – Partial disclosure of traffic data

This clause empowered a law enforcement officer to disclose relevant traffic data about a specified communication.

Clause 81 – Collection of traffic data

This clause provided for the collection of traffic data.

Clause 82 – No monitoring obligation

This clause prohibited an electronic communication service provider to have a general obligation to monitor the data which it transmitted or stored.

Clause 83 – Limitation of liability

This clause provided for the limitation of liability of an electronic communications service provider.

Clause 84 –Extradition

This clause provided that an offence under the provisions of this Act was an extraditable offence for the purposes of the Extradition Act.

Clause 85 – Evidence obtained by lawful interception not admissible in criminal proceedings.

This clause provided that evidence obtained in contravention of this Act shall not be admissible in criminal proceedings.

Clause 86 – General penalty

This clause sought to make provision for the general penalty of an offence under the Act for which no penalty had been provided for.

Clause 87 – Power of court to order cancelation of licence, forfeiture etc

This clause provided for the power of the court to order cancellation or forfeiture of licence.

Clause 88 – Guidelines

This clause empowered the Authority to issue guidelines as were necessary for the better carrying out of the provisions of this Act.

Clause 89 – Exemptions

This clause provided for the exemptions the Authority may make from the requirement to abide by the provisions of this Act.

Clause 90 – Regulations

This clause gave the Minister the power, on the recommendation of the Authority, to make regulations for the better carrying out of the provisions of this Act.

8. CONCERNS RAISED BY STAKEHOLDERS

While supporting the Cyber Security and Cyber Crimes Bill, N.A.B. No. 2 of 2021, stakeholders raised the following concerns and expressed the view that these needed to be addressed before the Bill could be enacted in order to improve the law.

Comments on the Objects of the Bill

Stakeholders noted that the memorandum of the Bill had omitted some of the key objects which were, however, provided for in the Bill. They were of the view that the objects of the Bill should provide for the establishment and define the functions of the governance structures listed below.

(a) The Zambia Computer Incidence Response Team (CIRT);
(b) The Central Monitoring Centre;
(c) The Cyber Security Coordinating Council; and

The stakeholders added that the prevention, detection, investigation, prosecution and punishment of cyber crime should be included in the objects of the Bill.

Clause 2 – Interpretation

Stakeholders noted that under clause 2, "Director-General" meant a person appointed as Director-General under the "Information, Technology and Communications Act, 2009". In this vein, they were of the view that the Act should be reflected correctly as "Information and Communications Technology Act, 2009.

Stakeholders observed that under interpretation the words "anyeletronic" should be separated to read "any electronic".

Stakeholders observed that the definition of "computer system" had the meaning assigned to it in the *Electronic Communications and Transactions* Act, No. 21 of 2009. They wondered whether the term "computer system" included the internet in light of the definition of cyber which incorporated the word "internet". They proposed that the word "Internet" be included in the definition.

Stakeholders observed that "Critical Information Infrastructure" "meant infrastructure declared as critical information infrastructure by the Minister". They argued that the definition referred to what the Minister would declare through regulations. This meant that the identification of the sectors regarded as sensitive for the Republic's security and well-being of the economy, as well as the information and communication technologies systems designed to function in these sectors as elements of critical information infrastructure, would be left to the whims of the Minister.

In this regard, they proposed that the definition of "Critical Information Infrastructure" be redefined to mirror the one provided for in the African Union Convention on Cyber Security and Personal Data Protection Convention 2014, which stated that "Critical Information Infrastructure means the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace".

Stakeholders noted that the definition of "Law Enforcement Officer" meant:

(a) a police officer above the rank of sub-inspector;
(b) an officer of the Anti-Corruption Commission;
(c) an officer of the Drug Enforcement Commission;
(d) an officer of the Zambia Security Intelligence Service; and
(e) any other person appointed as such by the Minister for purposes of this Act.

They argued that whereas there was a standard definition of Law Enforcement Officer, part (e) stated that any other person appointed as such by the Minister for purposes of this Act which they believed was inappropriate. They were of the view that only specified categories of law enforcement officers should be included in the definition and proposed the removal of (e) which provided in this case, that the minister responsible for transport and communications could appoint any other person as a law enforcement officer. They further proposed that the defence force personnel should also be defined as law enforcement officers.

Stakeholders noted that the Bill defined a "cyber security incident" as "an act or activity on or through a computer or computer system that jeopardised or adversely impacted the security or integrity of a computer system or the availability, confidentiality or integrity of a computer or computer system". They argued that although the definition sought to limit the circumstances under which an investigation would be deemed necessary, it did not do so in a way that limited such incidences. They were of the view that the incidence be a result of a deliberate or intentional action attributable to an individual rather than a system failure which could have similar effects.

Stakeholders observed that the Bill did not define a cyber security threat. They were of the view that this opened it to interpretation of what exactly amounted to a threat. In the absence of a clear definition, the provision may be abused to justify wanton surveillance of unsuspecting members of the public.

Stakeholders noted that the words "penetration testing service" appeared in the interpretation but did not appear in the text of the Bill. They proposed that "penetration testing service" be included in clause 5 (1) and should read as "Undertake information security audits and penetration testing services on all critical information infrastructure"

New Definition

Stakeholders noted that the term "Zambia Computer Incidence Response Team" had not been defined, although it had been used in the Bill. They contended that for purposes of clarity, the term should be defined in the Bill.

Clause 3 – Supremacy of Act Chapter 1

Stakeholders noted that clause 3 of the Bill proclaimed that the Act would be subject to the Constitution of Zambia. However, under the functions of the cyber security regulator, this position was not reinforced. Borrowing from other similar laws in the jurisdiction, one of the functions of the Zimbabwean Cyber Security Centre, which appeared to be the equivalent of the Zambian cyber security regulator was to 'oversee the enforcement of the Act to ensure that it was reasonable and with due regard to

fundamental human rights and freedoms.' Stakeholders proposed that under the functions of the Cyber Security Regulator, this position be re-emphasised by the inclusion of a function that required the Authority to have due regard to fundamental rights and freedoms. This would also give comfort that the Regulator would not operate with unlimited independent oversight.

Clause 4 – Cyber security regulator and Clause 5 – Functions of Authority Act, No. 15 of 2009

Stakeholders stated that the seriousness with which any government treated the threat of cyber security was reflected in the placement of the cyber security function in government. The majority of governments across the globe appointed a Cyber Security Commissioner who reported directly to the Head of State. Such a Commissioner would be expected to be the head of an authority such as the National Cyber Security Advisory and Coordinating Council (NCSACC) alluded to in the Bill.

Stakeholders further observed that the Authority being referred to in clause 4 was the Zambia Information and Communications Technology Authority (ZICTA), established by the *Information and Communication Technologies Act, No 15 of 2009*. Under the Bill, ZICTA would, *inter alia,* constitute the Zambia Computer Incidence Response Team (ZCIRT) and also appoint cyber security inspectors, among other functions of collaborating with the Ministry responsible for security and defense. They were of the view that ZICTA's functions were already wide under its constitutive Act. Therefore, adding more power to ZICTA would make it a super-executive institution, which may possibly result into unlimited independent oversight.

In this regard, stakeholders recommended the setting up of an independent cyber security regulator. However, if the Bill retained ZICTA as the cyber security regulator, the National Cyber Security Advisory and Coordinating Council should hold the cyber security regulator to account in order to ensure that it performed its functions in line with the fundamental human rights and freedoms.

Clause 5 – Functions of Authority Act No. 15 of 2009

Stakeholders noted that under clause 5(1)(e), the words "all inclusive" should be separated to read "all inclusive".

They also noted that under clause 5(2), the word "maters" be replaced with the word "matters".

Stakeholders noted that clause 5(2) provided that the Authority shall, in performing it's functions, collaborate with the ministries responsible for security. They proposed that

the Ministry of Defence be included, as well as other relevant agencies on matters relating to cyber security.

Clause 6 – Constitution of Zambia Computer Incidence Response Team

Stakeholders noted that the Authority would constitute the Zambia Computer Incidence Response Team. However, it was not clear whether the Zambia Computer Incident Response Team would be a directorate under the Authority or an independent institution. They, therefore, proposed that the Zambia Computer Incident Response Team should be an autonomous institution comprising officers of Defence Forces and security wings, ZICTA, representatives from Attorney General.

Stakeholders also noted that there was no composition or tenure of office of the Zambia Computer Incidence Response Team. They were of the view that for purposes of transparency and accountability there was need to clearly state how many persons would constitute the Zambia Computer Incidence Response Team and for how long they would hold office. However, the definition of what amounts to a cyber security incident was broad and may be interpreted to encompass any activity unwittingly performed on a computer system which was seen as "jeopardising" security even if such act or activity was not intended to do so. Stakeholders proposed that the definition of "cyber security incident" ought to include that the act or activity must be one performed intentionally by infringing security measures with intent to obtain data or with some other dishonest intent or to misuse a computer system or network.

Clause 7 – Constitution of National Cyber Security Advisory and Coordinating Council

Stakeholders submitted that clause 7(1) provided that the Minister shall constitute the National Cyber Security Advisory and Coordinating Council which would consist of part-time experts in cyber security and cyber crime. They were of the view that the Council should include other relevant professions and also specify the years of experience.

Stakeholders observed that under clause 7(2) (b), the Council would oversee the implementation of cyber security related functions of the Authority. The argued that the Council posed a reporting line challenge with regards to the ZICTA Board. They wondered what the role of the ZICTA Board would be in relation to cyber security functions. Further, the *Information and Communications Technology Act, No. 15 of 2009,* granted complete autonomy to the Authority. It stated that "Except as otherwise provided in the *Information and Communications Technology Act, No. 15 of 2009,* the Authority shall be an autonomous body and shall not be subject to the direction of any other person or authority". They proposed that the Zambia Computer Incident Response Team be constituted as an independent autonomous body with a reporting

line to the Council *whose membership should include representation from the Defence Forces and security wings*, ZICTA and Attorney General.

Stakeholders observed, further, that this clause gave the Minister wide discretionary powers to determine the number and security of tenure of the Council through Statutory Instrument. They proposed that the composition and tenure of the Council be explicit in the Act. This would promote checks and balances and weed excessive power from the Executive and promote good governance.

Additionally, to ensure collaboration with various organisations in the country, stakeholders suggested that among the functions of the NCSACC should be the responsibility for annual "Cyber Drills". A Cyber drill was a "Table Top Simulation service which provided organisations with an opportunity to become experienced with managing real-life cyber security incidents without the risk of actually damaging the organisation."

Clause 8 – Appointment of cyber inspectors

Stakeholders noted that the clause seemed to suggest that one inspector would be appointed. Therefore, there was need for this provision to state clearly that it would give rise to an Inspectorate which required other staff to discharge the mandate under the Act.

Clause 9 – Power to inspect

Stakeholders noted that this clause empowered cyber inspectors to enter and inspect premises. They were of the view that the definition of premises should include "a computer and data messages". This would mean that the inspectors not only have the power to enter upon physical premises but also have uninhibited access to the virtual realm.

Clause 10 – Data retention notice

Stakeholders observed that clause 10 seemed to be misplaced. It did not sit well under Inspectorate. They proposed that the provision be moved to an appropriate section.

Clause 11 – Power to access search and seize

Stakeholders observed that the power to search at reasonable time may be open to abuse. They proposed that the standard provided for under Section 119 of the *Criminal Procedure Code Act, Chapter 88 of the Laws of* Zambia which provided that: "Every search warrant may be issued and executed on a Sunday, and shall be executed between the hours of sunrise and sunset, but a magistrate may, by the warrant, in his discretion,

authorise the police officer or other person to whom it is addressed to execute it at any hour,"should be applied.

Clause 14 on Emergency cyber security measures and requirements

Stakeholders noted that the word "emergency" had not been used in the text of the clause.

Stakeholders noted that in theory, if the Minister prescribed for an act that suppressed communication without an accompanying State of Emergency, it would probably be in contravention of Part III of the Republican Constitution. They, therefore, recommended that a safeguard may be required to clearly set out the limits of a regulation under this Act.

Clause 15 – Powers to investigate

This clause empowered ZICTA to, among other things, investigate cyber security incidents and cyber security threats upon receipt of information regarding an alleged cyber security threat or incident. The provision did not state who was supposed to notify ZICTA of such a threat or incident. It did, however, state that a cyber inspector "may" institute an investigation on this basis. Stakeholders were of the view that the provision was broad enough to cover notifications by ordinary members of the public as well as law enforcement officers. They also argued that this clause had a potential for wanton misuse as members of the public may be required at any given time to make statements and produce documents and records merely on the basis of an alleged cyber security incident. A person who refused to give information or produce any record required by a cyber inspector on the basis of an alleged cyber security incident committed an offence and faced, on conviction, a fine not exceeding K60 000 (200 000 penalty units) and/or imprisonment for two years. Given that a security incident was broadly defined, failure to assist with its investigation or produce information may as well arise from a lack of understanding as to what information was required and whether such information was available. This penalty also had the potential to be abused by law enforcement officers to coerce members of the public into providing information for illegitimate aims.

Clause 18 – Localisation of critical information

Stakeholders noted that clause 18(2)(1) empowered the Minister to authorise a controller of critical information to externalise the critical information outside the Republic as prescribed. They contended that this clause had the ability to make institutions externalise data and defeat efforts towards localisation of data. They, therefore proposed that this provision be removed. Additionally, stakeholders noted that clause 71 of the *Data Protection Bill, N.A.B. No. 28 of 2020,* provided conditions and

criterion to be used by the Controller of Critical Information for externalising information outside the Republic. In the vein, they proposed that the Minister should authorise externalisation of critical information in the similar manner as provided under clause 71 of the Data Protection Bill, N.A.B. No. 28 of 2020. ***In addition,*** exemption needed to be given to the financial sector as most international banks have data savers located abroad and it would be very expensive for them to localize their data.

Clause 22 - Auditing of critical information to ensure compliance

Stakeholders noted that the clause mandated an "information technology auditor to audit the critical information infrastructure as prescribed". However, they were of the view that such audit could also be extended to cyber security service provider. This was because such audit would ensure that cyber security service providers delivered expected and efficient services.

Clause 23 – Duty to report cyber security incidents in respect of critical information infrastructure

Stakeholders noted that clause 23(3) provided that the controller of critical information infrastructure shall submit a monthly cyber security incident and threat report to the Authority. They proposed that this provision should be in the guidelines which the Authority shall issue to controllers of critical information infrastructure. They were of the view that if this was prescribed in the Bill, it would affect the Authority when need arose for the reports to be submitted weekly in the future.

Other stakeholders observed that banks and financial institutions were already submitting monthly reports to the Bank of Zambia (BOZ) and the recent Zambia Interbank Payment and Settlement System (ZIPPS) rules addendum also mandated immediate reporting of incidents to BOZ. They were of the view that there was need to clarify on the provision to report to the Authority because in their view the BOZ was the main regulator for banks and other financial institutions.

Clause 24 – National cyber security exercise

Stakeholders submitted that in the sentence "The Authority may ..." the word "may" should be substituted with "shall" because national security exercises were key.

Clause 27 – Central Monitoring and Coordination Centre

Stakeholders noted that the word "call related" under clause 27(3) should be separated to read "call related".

Stakeholders submitted that under clause 27(2) the use of the word "sole" suggested that the Central Monitoring and Coordination Centre was the only means through which an interception may be allowed under the Act. They argued that this provision had the potential of causing a conflict as there were other allowable avenues for a lawful interception such as those provided under clause 28 which allowed an interception by obtaining a court order.

Stakeholders noted that clause 27(3) provided that the Central Monitoring and Coordination Centre shall be managed, controlled and operated by the department responsible for Government communication in liaison with the Agency. They proposed that interceptions be managed by an independent body and not a Government agency as there might be a risk of invading people's privacy. This, in their view, could enhance accountability and protection of members of the public.

Stakeholders also noted that the clause mentioned an "Agency". They were of the view that reference to the Agency was an error. However, if that was the intention, there would be need to define which Agency was being referred to otherwise it should make reference to the Authority.

Clause 28 – Lawful interception

The clause provided that a law enforcement officer may, where there was reasonable grounds to believe that an offence had been or was being committed or was likely to be committed and for purposes of obtaining evidence, apply ex-parte to a judge of the High Court for an interception of communications order. Prior to making such an application, the law enforcement officer was required to apply for the written consent of the Attorney-General. The basis upon which a law enforcement officer applied for an interception order was that they suspected that an offence was likely to be or was being committed, legally the proper office to which such an application ought to lie was the Director of Public Prosecutions as the office with exclusive jurisdiction to institute and undertake criminal proceedings. For purposes of the Bill and particularly for interceptions, a service provider was defined in clause 2. However, the definition of a service provider was wide enough to encompass network providers that provided access to telecommunications networks, internet service providers and even social media sites. They were of the view that any such entity may, therefore, be the subject of an interception of communications order. This provision presented a possibility for abuse as it gave law enforcement officers wide discretion to address such orders to any entity within the blanket definition.

Further this clause provided that a Judge may grant an interception of communications order if they were satisfied that the written consent of the Attorney-General had been obtained and there were reasonable grounds to believe that the intercepted information related to the commission of an offence or to the whereabouts of a person suspected of

committing an offence. Once granted, an interception order was valid for 3 months and renewable on application for such further period as a judge may determine.

Furthermore, clause 28(5) provided that evidence obtained by virtue of the interception done pursuant to an ex-parte order would be admissible in criminal proceedings for an offence under the Act as evidence of the truth of its contents despite the fact that it contained hearsay. Essentially, the Bill attempted to create an exception to the hearsay rule so that any intercepted communications such as statements made in phone calls and messages could be produced as evidence in court without the need to call the makers of the statements to testify. A person may be charged with an offence and even convicted simply on the basis of a statement made by another person who need not be called to give their evidence and/or be cross-examined by the accused person. This provision was contrary to clause 85 which provided that any evidence obtained by means of interception in accordance with the Bill shall not be admissible in any criminal proceedings except with the leave of court.

In view of the foregoing, stakeholders proposed that interceptions of communications on the basis of orders obtained ex-parte be a subject of inter parte hearings within a fixed period of days such as seven days, after such orders were granted as these orders were only valid for three months. The prerequisite fiat prior to obtaining such an ex-parte order must be that of the Director of Public Prosecutions and not the Attorney General. Furthermore, any person whose data was the subject to an interception ought to be allowed to make submissions on whether the interception was valid and proportional to the supposed threat. In addition, any evidence obtained by any means of interception under the Bill ought only to be admissible with leave of the court and in accordance with the established rules of evidence such as the rule against hearsay.

Clause 29 – Interceptions of communication to prevent bodily harm, loss of life or damage to property

Stakeholders noted that under clause 29(a) (iii), the words "orto" should be separated to read "or to". They also proposed for the addition of part (v) which should state that "has caused or may cause financial loss to banks, financial institutions, account holders or beneficiaries of funds being remitted or received by such account holders or beneficiaries".

Stakeholders noted that owing to the nature of the actions being conducted by law enforcement in clause 29(a), further safeguards were required to prevent abuse and unnecessary access to private information. Despite the emergency connotation, which was actually not stated in this clause, the oral application of a law enforcement officer could not be sufficient to allow access to private information. They proposed the inclusions of safety nets such as:

(a) inclusion of the immediacy of the harm being prescribed. This should only be used in an emergency situation;
(b) request could be directed to a subordinate court for speedy granting of temporal warrant; and
(c) inclusion of a third party to confirm the circumstances alleged by the LEO. This may be a witness, complainant, informant or another institution.

They proposed that an offence for such action must be created to prevent gross infringement of privacy.

Clause 30 – Interception of communication for purposes of determining location

Stakeholders proposed that clause 30(1) should include part (f) which should state that: "or theft of finances from banks or financial institutions".

Some stakeholders noted the clause empowered a law enforcement officer to orally request, without leave or an order of court, that an electronic service provider intercept communication for purposes of determining the location of a person or determine that person's location by some other means where there were reasonable grounds to believe that the person was in danger of injury or death. The provision further obligated an electronic service provider to abide by the request in mandatory terms. However, the provision did not require any sort of proof from the law enforcement officer for the alleged belief of danger or injury. There was, therefore, great potential for the abuse of this provision under the guise of protection from death or injury. It was only after the oral request was made that the law enforcement officer was required to provide a Judge and the electronic service provider with written confirmation of the request. Furthermore, it was only after location and other information was provided that the law enforcement officer was required to submit to a Judge an affidavit setting out the results obtained from the interception. As with interceptions without leave of court, where a Judge was of the view that the interception was unlawful or used for purposes other than those intended by law, they may make such an order as they consider appropriate in relation to the law enforcement officer or the service provider.

Stakeholders were of the view that clauses 29 and 30 be done away with and that no interceptions should be conducted without leave of court regardless of the alleged immediate danger. Ex-parte orders, subject to inter parte hearings soon after, may be promptly obtained in order to facilitate expedient action on the part of law enforcement officers. Any request by a law enforcement officer to a service provider for an interception to be performed must be in writing and pursuant to an order of court. In addition, there ought to be a penalty for law enforcement officers who disclosed information obtained through interceptions.

Clause 34 – Prohibition of random monitoring

Stakeholders noted that under clause 34(3), the words "orrecording" should be separated to read "or recording".

Clause 37 – Penalty for using an interception device

Stakeholders noted that the provision in clause 37(2) of a penalty on conviction, "to a fine not exceeding three million penalty units or to imprisonment for a term not exceeding twenty five years, or to both" for using an interception device was too harsh. They were of the view that there was need to strike a fair balance between penalising and ensuring compliance with the Act.

Clause 38 – Assistance by service providers

Stakeholders noted that under clause 38(1) (d) the words "call related" be separated to read "call related".

Clause 39 – Duties of service provider in relation to customers

Stakeholders proposed the insertion of part 'd' which should state that "a portrait of the applicant taken at the time the application of the service was rendered in addition to the identity document and held as a permanent record thereof". Part 'e' should provide for a penalty for any persons acting as agents for the acquisition of service provider customers who failed to ensure that the provisions of clause 39 were complied with.

Stakeholders contended that this was necessary to regulate the operation of mobile network operator (MNOs) agents on boarding customers for MNOs. They observed that there were a lot of omissions in the know your customer (KYC) information when on boarding was conducted by MNO agents. They proposed the need to place a responsibility on MNOs to ensure that their agents complied with KYC requirements or risk some form of sanction such as fine for on boarding customers with insufficient KYC. They also proposed the need to cross reference the requirements under the *Financial Intelligence Centre (Amendment) Act, No. 16 of 2020* to MNO's.

Clause 40 – Interception capability of service provider

Stakeholders observed that in many countries, the provisions of "Interception" that were provided in the Bill were dealt with in separate legislations such as the "Wire Tapping" Legislations in the United Stated of America (USA). They acknowledged that the provisions of interception were well placed in the Bill, although in future they may call for separate legislations.

Part VII– Licensing of cyber security service providers

Part VII required any person, natural or artificial, to apply for a license from ZICTA before providing cyber security services. However, the Bill did not provide a criterion or requirements that an applicant must meet in order to be granted a licence. Additionally, the licence given would be valid for a period of time yet to be prescribed. Further, the Agency may revoke or suspend a licence on a number of grounds including that the licencee was no longer a fit person or that it was in the public interest to do so. Given that the Bill did not prescribe the qualifications of a cyber security service provider in the first place, the grounds on which a person may be considered not to be a fit person were subject to determination by ZICTA in its sole discretion. This lack of certainty left far too much room for abuse through the denial of registration or renewal on an unlimited number of grounds. Stakeholders proposed that the Bill should specify the qualifications of cyber security providers definitively as well as what amounted to a "fit and proper person" for purposes of granting or renewing a licence.

Clause 41 – Prohibition from providing cyber security services without licence

Stakeholders observed that clause 41(1) (a) provided that no person without a licence shall "engage in the business of providing, for reward or otherwise, cyber security services to other persons". They were of the view that there was need to balance registration with innovation. They proposed that the law should allow for areas where innovation could be practiced for research purposes. Therefore, a waiver for research and innovation activities should be considered.

Clause 43 – Renewal of licence

Stakeholder noted that the Bill had not provided reasons for rejecting to renew a licence. They were of the view that it would be important to give reasons. In the same vein, they proposed that there should be a clause on what would happen when there was no response on the outcome of the application for renewal after the expiry of 30 days.

Clause 44 – Refusal to grant or renew licence

Stakeholders noted that clause 44(5) provided that the" Authority may consider any of the following matters as applicable in deciding, for the purposes of this section, whether a person or an officer of a business entity or the business entity is a fit and proper person" if "(a) that the person or officer associates with a criminal in a way that indicates involvement in an unlawful activity;". They were of the view that the word "criminal" was unclear and could lead to subjectivity in its application. They proposed that the words "a person convicted of a crime with a penalty of more than 6 months with no option of a fine" could be used to replace the word "criminal".

Clause 46 – Revocation or suspension of licence

Stakeholders noted that clause 46(6), provided that "A licensee whose licence has been suspended under clause 46(5) may, within fourteen days after the Authority had served the notice of suspension, apply to the Authority for review of the Authority's decision." They were of the view that the traditional fourteen (14) days period normally given for such actions as proposed in this clause was, in practice, rarely adequate. Consequently, they suggested that the period be increased to twenty one (21) days. Incidentally, clause 46(9) alluded to the same 14 days period. It was further suggested that legislation should compel organisations, whether critical information infrastructure based or not, to carry out organisational risk-assessment instead of waiting for the information technology auditor to pinpoint their cyber weaknesses. The results of such assessment need not be shared with the auditor who was expected to carry out an independent audit whose results were for public consumption.

Part VIII - International cooperation in maintaining cyber security

Stakeholders observed that Part VIII provided for areas of international cooperation in maintaining cyber security. They were of the view that the above provision was important to the Defence Force. This was because the Authority could not have the sole mandate of identifying areas of cooperation with foreign countries and entering into agreements. They proposed that this should be a mandate of the Council or a multi sectoral body to ensure that there was no compromise on national defence and security. Therefore, the Defence Forces must be involved in this process as they normally have a diplomacy and security analysis capability. They added that the international cyber diplomacy was a key tool in the current international security system order which should be done holistically.

Clause 49 – Un authorised access to, interception for or interference with computer system and data

Stakeholders observed that clause 49(4) (a) provided that a person committed an offence if that person, among others:

(a) communicates, discloses or transmits any data, information, program, access code or command to any person not entitled or authorised to access the data, information, program, code or command; and

(b) introduces or spreads a software code that damages a computer, computer system or network.

Stakeholders argued that there was a possibility of unintentional committing of the two offences in (a) and (b), accidentally or due to incompetency. They proposed that

qualifications to the circumstances be included by adding a sentence such as "a person who intentionally and without authority to do so" in (a) and (b).

Stakeholders added that the exception under clause 49**(6)** relating, inter alia, whistleblowers ought to apply to 49(1) as well because unauthorised possession was inextricably bound with unauthorised access. Therefore, leaving out the exception under clause 49(1) opened the possibility of prosecution of whistleblowers and journalists who accessed information and their agents. This proposed amendment was particularly important given the exceedingly high penalty under clause 49(3) where the information that related to critical information infrastructure which was usually the interest of whistleblowers and journalistic pursuits. They proposed that the penalty threshold of two million and five hundred thousand penalty units as a fine and 25 years imprisonment be reduced as it was disproportionately high in comparison with the other offences.

Clause 50 – Illegal devices and software

Stakeholders noted that clause 50(1)(iii) provided that "A person commits an offence if that person: "introduces or spreads a software code that damages a computer or computer system with the intent that it be used by any person for the purpose of committing an offence defined by other provisions under this Part". They proposed that the Bill should adopt the definition in the African Union Convention on Cyber Security and Personal Data Protection of 2014, which stated that "damage means impairment to the integrity or availability of data, a program, a system or information". This would ensure the offence of damage to a computer or computer system included any type of impairment as defined herein.

Clause 51 – Computer related misrepresentation

This clause provided that "A person who knowingly, without lawful excuse, inputs, alters, deletes, or suppresses computer data, resulting in unauthentic data with the intent that it be considered or acted on as if it were authentic, regardless of whether or not the data is directly readable and intelligible commits an offence and is liable, on conviction, to a fine not exceeding seven hundred thousand penalty units or to imprisonment for a period not exceeding seven years or to both".

Stakeholders observed that "Where the offence in clause 51(1) could be committed by sending out multiple electronic mail messages from or through computer systems, the penalty was one million five hundred thousand penalty units or imprisonment for a period not exceeding fifteen years, or to both". Clause 51 (2) provided for a stiffer penalty than clause 51 (1) on account of committing the crime by sending out multiple electronic mail messages. Stakeholders contended that there were many other ways or means and medium that could be used to spread from a computer, mobile device or

even through the internet platform and resulting in unauthentic data with the intent that it be considered or acted on as if it were authentic. They were of the view that the penalty of seven years imprisonment be the same regardless of the medium used. This was to avoid offenders getting lesser punishment due to the use of other means not stated even when their action had a high impact.

Clause 53 – Identity related crimes

Stakeholders were of the view that this could be an appropriate clause in which to include online impersonation. This was because the offence being described under this clause seemed to refer to identity theft and not where one purported to be another person online.

Clause 54 – Publication of information

This clause dealt with publication of information, but that apart from the intent to compromise the safety and security of a person, the element of knowledge that the information was false, inaccurate, or misleading must be included and that the intent to compromise the safety and security of the person must be without lawful excuse to prevent the offence from being strict liability. Stakeholders were of the view that that clause 55 which dealt with aiding, abetting, and counseling etc., should be subjected to clause 49(6) and, if amended clause 49(1), should ensure that persons who legitimately obtained data for journalistic purposes or whistleblowers were not caught under this provision.

Clause 56- Prohibition of pornography

Stakeholders submitted that the scope of the provision on Child pornography should be widened to include the definitions contained in Article 9 (2) of the Budapest Convention.

Clause 62 – unsolicited electronic messages

Stakeholders submitted that under clause 62(3) (a) the words "computer data" should be separated to read "computer data".

Clause 66 – Minimisation, etc, of genocide and crimes against humanity

Stakeholders noted that clause 66 created an offence for crimes of genocide or crimes against humanity. However, the Bill had not stated what constituted genocide or crimes against humanity. They proposed that the Bill should state what constitutes genocide or crimes against humanity or cross reference it to the Convention on Prevention and Punishment of Genocide

Part X – Electronic evidence

This clause provided for cyber crimes and one of which was harassment. However, the term had not been defined. They proposed that the term be defined to also include an element of intention in order to create certainty with regard to the law and to justify prosecution for this offence. They were of the view that without these specifications, any member of the public may be charged with the offence and would be unable to effectively defend themselves because the provision was open to interpretation. They proposed that the term harassment be defined. Similarly, the definition of hate speech should be similar to the one on racism and xenophobia.

Clause 70 – Cyber terrorism

Stakeholders noted that clause 70(1) provided that a person who uses or causes to be used a computer system for the purpose of cyber terrorism commits an offence and is liable on conviction to life imprisonment. They proposed that reference to usage be qualified with the work "knowingly". This was because it was possible for attackers to use one's computer without the knowledge of the owner or users. Other stakeholders were of the view that the proscribed life imprisonment punishment was too heavy even if the offense committed was a felony. Still other stakeholders suggested that the offence be extended to cyber recruitment, promotion and support for terrorism.

Clause 72 – Cognisable offences

Stakeholders noted that clause 72 declared all offences under the Act to be cognizable, but this provision was unjustifiable because some offences under the Act were not cognisable in nature such as unsolicited electronic messages and identity related crimes. These offences could not be placed in the same category as cyber terrorism and child pornography.

Clause 75 – Search and seizure Cap.88

Stakeholders submitted that under clause 75(2) (b)(ii) the words "computer data" should be separated to read "computer data".

Clause 82 – No monitoring obligation

Stakeholders noted that clause 82(2) appeared to be in contrast with …… (1). This was because if the service provider could not monitor, as a general rule, how could it identify a criminal activity. However, if the regulations allowed the service provider to monitor, the provision may be in contravention of the right to privacy minus a court order. As a result, stakeholders suggested that clause 82 (2) be deleted in its entirety.

Clause 89 – Exemptions

Stakeholders noted that the clause 82 (1) provided for exemptions but had not stated the provisions for one to qualify for exemption. They Bill had also not stated what would necessitate the exemption as well as class of persons. They were of the view that the Bill should state what determined who should be given an exemption as well as the time limit. Additionally, it would be important to get an express exemption on matters of defence and security. They proposed that consideration must be given when giving specific departments of the Defence Force exemptions to abide by. This would enhance speed and flexibility to ensure that there was defence and national security in the realm of cyber. Further, - "the Authority may, by declaration, exempt Defence and security or any class of persons, for a limited or unlimited period of time, from the requirement to abide by the provision of this Act".

Clause 90 – Regulations

Stakeholders noted that the Minister was empowered, on recommendation of the Authority, by statutory instrument to make regulations for the better carrying out of the provisions of this Act. However, the clause had not provided for the transition period. They proposed the inclusion of a transition period of at least a year to allow for regulated entities to comply with the new provisions.

9.0 GENERAL CONCERNS

1. Collaboration with other relevant bodies

Stakeholders noted with concern that the Bill did not provide a platform for the cyber security regulator to collaborate and coordinate with relevant bodies, such as the banking sector, mobile network providers, National Anti-Terrorism Centre and the Financial Intelligence Centre, among others. They were of the view that the Bill should provide for interface of the cyber security regulator and other relevant bodies given that cyber crimes were of a cross cutting nature.

2. Mutual legal assistance

While acknowledging that the Bill provided for extradition, they noted that there was no provision for mutual legal assistance. Considering the relative ease with which online offenders could commit criminal acts remotely, the law enforcement response to criminal conduct must rely significantly on trans-border mechanisms such as mutual legal assistance and extradition. As a result, the stakeholders proposed that a provision on mutual legal assistance be inserted in the Bill.

3. Review of critical information infrastructure bases

Stakeholders proposed that there would be need to periodically review organisations that were designated as "Critical Information Infrastructure" bases. This was because the attributes of being a critical infrastructure base may change over time because of the rapid technological developments.

4. Notification of Intrusion

Stakeholders noted that the Bill did not include provisions of entrenchment of the cyber security of the data subjects as well as the right for the subjects to be notified that unauthorised persons or systems had accessed their system. They were of the view that data subjects should be notified that there was an intrusion in their system.

5. Cyber security hubs

Stakeholders noted that the Bill had not provided for the creation of structures such as a 24/7 point of contact to promote reporting of incidents of cyber crimes. They proposed that the Bill should have a provision for the creation of structures such as a 24/7 point of contact, cyber security hub and nodal points to promote reporting, investigation and prosecution of incidents of cyber crime. These points could provide immediate expedited assistance to investigate offences in terms of the Bill.

10.0 COMMITTEE'S OBSERVATIONS AND RECOMMENDATIONS

Having considered the submissions from stakeholders, the Committee makes observations and recommendations set out below.

(a) Memorandum

The Committee notes with concern that a number of governance structures have been established in the Bill. However, they have not been listed among the objects of the Bill.

In this regard, the Committee recommends that the governance structures listed below, which have been mentioned in the Bill, should be listed among the objects of the Bill and their functions defined.

(a) The Zambia Computer Incidence Response Team (CIRT).
(b) The Central Monitoring Centre.
(c) The Cyber Security Coordinating Council.

Additionally, the prevention, detection, investigation, prosecution and punishment of cyber crimes should be listed among the objects of the Bill.

(b) Critical Information Infrastructure

The Committee observes that the definition of "Critical Information Infrastructure" has been left to the discretion of the Minister, who is mandated to identify sectors regarded as sensitive to the Republic's security and the well-being of the economy. The Committee considers this decision as too critical to be left to the discretion of a Minister.

In this regard, the Committee recommends that the model definition of "Critical Information Infrastructure", provided in the African Union Convention on Cyber Security and Personal Data Protection Convention 2014, be adopted. In the Convention, "Critical Information Infrastructure" has been defined as cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace.

(c) Law Enforcement Officer

The Committee observes that the definition of "Law Enforcement Officer" states, in part (e) that "any other person appointed as such by the Minister for purposes of this Act." However, the Committee agrees with the stakeholders that this is inappropriate because only specified categories of law enforcement officers, including members of the defence forces, should be included. In this regard, the Committee recommends that in order to avoid abuse, part (e) should be deleted and that the appointment of defence force officers as law enforcement officers should expressly be provided for in the Bill.

(d) Supremacy of Act Cap. 1

The Committee observes that whereas clause 3 subjects the Act to the supremacy of the Constitution of Zambia, this is not explicitly provided for under the functions of the cyber security regulator. The Committee notes that this is a departure from best practices.

In this vein, the Committee recommends that in order to ensure reasonableness and regard to fundamental human rights and freedoms, the functions of the cyber security regulator should include a requirement for the Authority to have due regard to fundamental rights and freedoms.

(e) Cyber Security Commissioner

The Committee observes that best practices across the globe is that a Cyber Security Commissioner reports directly to the Head of State. This line of reporting reflects the

seriousness with which any government treats the threat of cyber security within its territory. Such a Commissioner is expected to be the head of an Authority such as the National Cyber Security Advisory and Coordinating Council (NCSACC) alluded to in this Bill.

However, the Committee observes that the Authority being referred to in clause 4 is the Zambia Information and Communications Technology Authority (ZICTA), which is established by the *Information and Communication Technologies Act, No 15 of 2009*. This means that ZICTA will, *inter alia,* constitute the Zambia Computer Incidence Response Team (ZCIRT) and also appoint cyber security inspectors, in collaboration with the ministry responsible for security and defense. The Committee observes that ZICTA's functions and powers are already wide under its constitutive Act and that adding more will make it a super-executive institution, which may possibly result in unlimited independent oversight.

In this regard, the Committee recommends that an independent cyber security regulatory institution be set up. However, in the event that ZICTA is maintained as the cyber security regulator, it should operate under the purview of the National Cyber Security Advisory and Coordinating Council in order to ensure that it performs its functions in line with fundamental human rights and freedoms.

(f) Zambia Computer Incidence Response Team

The Committee notes that this Bill mandates the Authority to constitute the Zambia Computer Incidence Response Team. However, it is not clear whether the Zambia Computer Incident Response Team will be a directorate under the Authority or an independent institution. Additionally, the Committee is concerned that the composition and tenure of office of the Zambia Computer Incidence Response Team is not spelt out in the Bill.

The Committee, therefore, recommends that for purposes of transparency and accountability, the composition, qualifications and tenure of office for the Zambia Computer Incidence Response Team should be explicitly provided for in the Bill. The Committee, further recommends that the Zambia Computer Incident Response Team should be an autonomous institution, which should include members from the defence and security wings.

(g) Constitution of National Cyber Security Advisory and Coordinating Council

The Committee observes that whereas clause 7(1) provides that the Minister shall constitute the National Cyber Security Advisory and Coordinating Council comprising part-time experts in cyber security and cyber crime, the Bill does not provide for the inclusion of other relevant professions and does not specify the qualifications or

experience that the experts should possess. Further, the Committee observes that the Council is mandated to oversee the implementation of the cyber security related functions of the Authority. The Committee is concerned that this will pose a reporting structure challenge with regard to the ZICTA Board operations. The Committee wonders what role the ZICTA Board will play in relation to the cyber security functions, particularly that the *Information and Communications Technology Act, No. 15 of 2009,* grants complete autonomy to the Authority.

In this regard, the Committee recommends that in order to avoid creating a conflict of interest, the Zambia Computer Incident Response Team should be constituted as an independent autonomous body with a reporting line to the Council.

(h) Power to access, search and seize

The Committee notes that clause 11 provides for power of the cyber inspector to access, search and seize with a warrant at any reasonable time enter a premises or access information**.** The Committee observes that the power to search at any reasonable time may be open to abuse.

The Committee, therefore, recommends that the standard provision under Section 119 of the *Criminal Procedure Code Act, Chapter 88 of the Laws of Zambia* should be adopted. The provision reads as follows:

> *"Every search warrant may be issued and executed on a Sunday, and shall be executed between the hours of sunrise and sunset, but a magistrate may, by the warrant, in his discretion, authorise the police officer or other person to whom it is addressed to execute it at any hour."*

(i) Emergency cyber security measures and requirements

The Committee observes that whereas the marginal note refers to 'emergency,' the word has not been used in the text in the entire provision. The Committee, therefore, recommends that either the word be dropped in the marginal note or included at an appropriate place in the text.

Further, the Committee agrees with the stakeholders that in theory, if the Minister prescribes an act that suppresses communication without an accompanying State of Emergency, it may be in contravention of Part III of the Republican Constitution. The Committee, therefore, recommends that a safeguard to clearly set out limits outside of the State of Emergency must be provided in the Bill.

(j) Localisation of critical information

The Committee observes that clause 18 empowers the Minister to authorise a controller of critical information to externalise critical information outside the Republic as prescribed. The Committee is of the view that this provision has a potential to cause institutions to externalise data and defeat efforts towards the localisation of data for security purposes.

The Committee, therefore, recommends that this provision be removed and replaced with the one under clause 71 of the *Data Protection Bill, N.A.B. No. 28 of 2020,* which provides conditions and criterion to be used by the controller of critical information for externalising information outside the Republic.

(k) Auditing of critical information to ensure compliance

The Committee notes that whereas clause 22 mandates an information technology auditor to audit the critical information infrastructure as prescribed, the same power has not been extended to the cyber security service provider. The Committee is of the view that to ensure that cyber security service providers deliver the expected and efficient services, this provision should be extended to them.

(l) Duty to report cyber security incidents in respect of critical information infrastructure

The Committee notes that the fact that the period within which the controller of critical information infrastructure shall submit a monthly cyber security incident and threat report to the Authority is prescribed in the Bill might pose an operational challenge as there may be need to revise the period in future. In this vein, the Committee recommends that for ease of revision, this should be provided for in the guidelines which the Authority shall issue to controllers of critical information infrastructure.

(m) Central Monitoring and Coordination Centre

The Committee agrees with the stakeholders' concern that clause 27(3) which provides that the Central Monitoring and Coordination Centre shall be managed, controlled and operated by the department responsible for Government communication in liaison with the Agency**.** The Committee notes that placing this responsibility under a Government agency might engender suspicions that the institution will be violating people's privacy.

The Committee, therefore, recommends that the interceptions be managed by an independent body in order to enhance accountability and protection of members of the public. Further, the clause erroneously makes reference to an "Agency" when it should be making reference to the Authority.

(n) Interceptions of communication to prevent bodily harm, loss of life or damage to property

The Committee observes that owing to the nature of the actions being conducted by law enforcement officers in clause 29 (1)(a) banks have not been included**.**

In this vein, the Committee recommends that in order to provide for the activities of the banks , there should be an addition of part (v) which should read as follows:

> "Has caused or may cause financial loss to banks, financial institutions, account holders or beneficiaries of funds being remitted or received by such account holders or beneficiaries".

Further, in order to prevent abuse and unnecessary access to private information, the oral application of a law enforcement officer should not be sufficient to allow access to private information. In this regard, the safeguards listed below should be added.

(d) Inclusion of the immediacy of the harm being prescribed. This should only be used in an emergency situation;

(e) Request could be directed to a subordinate court for speedy granting of temporary warrant; and

(f) Inclusion of a third party to confirm the circumstances alleged by the law enforcement officer. This may be a witness, complainant, informant or another institution.

(o) Penalty for using an interception device

The Committee, agrees with stakeholders that the provision in clause 37(2), of a penalty on conviction for using an interception device, of a fine not exceeding three million penalty units or to imprisonment for a term not exceeding twenty five years, or to both is too harsh. In this regard, the Committee recommends that the penalty be revised downwards in order to strike a fair balance between penalising and ensuring compliance with the Act.

(p) Duties of service provider in relation to customers

The Committee observes that clause 39, does not adequately cover mobile network operators, agents and on-boarding customers where there are a lot of gaps in the Know Your Customer (KYC) information when on-boarding is conducted by mobile net work operators' agents.

In this regard, the Committee agrees with the stakeholders for the insertion of parts (d) and (e). Part (d) should state that "a portrait of the applicant taken at the time the application for the service is rendered in addition to the identity document and held as a permanent record thereof," while part (e) should provide for a penalty for any persons acting as agents for the acquisition of service provider customers who fail to ensure that the provisions of clause 39 is complied with. The Committee recommends further that there be cross reference to the requirements under the *Financial Intelligence Centre (Amendment) Act, No. 16 of 2020,* to mobile network operators.

(q) Refusal to grant or renew licence

The Committee observes that clause 44(5) cites the applicant's association with a 'criminal' as ground for refusal to grant or renew a licence. The Committee notes, however, that the word 'criminal' is very vague and may lead to subjectivity in application.

In this vein, the Committee recommends that the word 'criminal' be replaced with the phrase, "a person convicted of a crime with a penalty of more than 6 months with no option of a fine"

(r) Revocation or suspension of licence

The Committee observes that clause 44 provides for fourteen days within which, a licensee whose licence has been suspended under clause 46(5), to apply to the Authority for review of the Authority's decision. The Committee is of the view that the traditional fourteen-day period normally given for such actions as proposed in this clause is, in practice, rarely adequate.

In this regard, the Committee recommends that the appeal period be increased to twenty-one days. The same should also apply to clause 46(9) which also alludes to the same number of days.

(s) Unauthorised access to, interception of or interference with computer system and data

The Committee observes that, while providing for offences, clause 49(4) (a) does envisage inadvertent commission of these crimes, which is quite common in computer technology.

In this regard, the Committee recommends that circumstances in which these offences can be committed be qualified by the insertion of a provision such as, "a person who intentionally and without authority to do so" at (a) and (b).

(t) Illegal devices and software

The Committee observes that clause 50 provides that "A person commits an offence if that person: "introduces or spreads a software code that damages a computer or computer system with the intent that it be used by any person for the purpose of committing an offence defined by other provisions under this Part". However, the word 'damage' has not been defined in the Bill.

In this vein, the Committee recommends that the definition in the African Union Convention on Cyber Security and Personal Data Protection of 2014, be adopted. The provision defines damage as 'impairment to the integrity or availability of data, a programme, a system or information."

(u) Computer related misrepresentation

The Committee observes that although clauses 51(1) and 51(2) are both providing for penalties of similar offences, clause 51(2) prescribes a higher penalty merely on account of sending multiple mail messages. The Committee observes that there are many other ways or means and medium that can be used to spread messages from a computer, mobile device or even through the internet platform and resulting in unauthentic data with the intent that it be considered or acted on as if it were authentic, which must equally be penalised.

In this regard, the Committee recommends that in order to avoid offenders getting lesser punishment due to the use of other means not stated even when their action has a high impact, a standard penalty of seven years imprisonment be applicable regardless of the medium used.

(v) Identity related crimes

The Committee observes that clause 53 does not cover online impersonation, even though the offence being described under this clause seems to refer to identity theft rather than where one purports to be another person online.

In this regard, the Committee recommends that online impersonation be included in the crimes provided for in this clause.

(w) Minimisation, etc, of genocide and crimes against humanity

The Committee notes that the term 'crimes against humanity,' referred to at clause 66, has not been defined in the Bill.

The Committee is cognisant of the ratification of the Convention on the Prevention and Punishment of Genocide and, therefore, recommends that reference should be made to the definition therein.

(x) Cyber terrorism

The Committee is in agreement with the stakeholders that clause 70(1), which provides that a person who uses or causes to be used a computer system for the purpose of cyber terrorism commits an offence and is liable on conviction to life imprisonment be qualified with the word "knowingly". This is because it is possible for attackers to use a computer without the knowledge of the owner or users. Further, the prescribed penalty of life imprisonment is too heavy even if the offence committed is a felony.

The Committee, therefore, recommends the inclusion of the word 'knowingly' in the clause 70(1) of the Bill and the reduction of the penalty. The Committee further recommends that the offence be extended to cyber recruitment, promotion and support for terrorism.

(y) No monitoring obligation

The Committee observes that there is a contradiction between clause 82(1) and (2) given that if the service provider cannot monitor, as a general rule, they may not be able to identify a criminal activity. In any case, if the regulations allow the service provider to monitor, the provision may be in contravention of the right to privacy in the absence of a court order.

In this vein, the Committee recommends that clause 82 (2) should be deleted in its entirety.

(z) Exemptions

The Committee observes that whereas clause 82 (1) provides for exemptions, it has not provided the grounds for exemption nor does it state what will necessitate the exemption as well as class of persons or institutions to be exempted.

The Committee, therefore, recommends that the Bill should state the grounds for exemption and the categories of individual, groups of persons or institutions eligible for such exemption.

(aa) Regulations

The Committee notes that whereas the Bill empowers the Minister, on the recommendation of the Authority, by statutory instrument, to make regulations for the

better carrying out of the provisions of the Act, it does not provide for the transition period. The Committee, therefore, recommends that a transition period of at least a year be provided to allow for regulated entities to comply with the new provisions.

(bb) Collaboration with other relevant bodies

The Committee notes the absence of platform for the cyber security regulator to collaborate and coordinate with relevant bodies such as the banking sector, mobile network providers, the National Anti-Terrorism Centre and the Financial Intelligence Centre, among others.

In this, regard, the Committee recommends that the Bill should provide for interface of the cyber security regulator and other relevant bodies given that cyber crimes are of a cross cutting nature.

(cc) Mutual legal assistance

In noting that the Bill provides for 'extradition', the Committee observes that there is no provision for 'mutual legal assistance'. Considering the relative ease with which online offenders can commit criminal acts remotely, the law enforcement response to criminal conduct must rely significantly on trans-border mechanisms such as mutual legal assistance and extradition.

In this vein, the Committee recommends that a provision on mutual legal assistance be included in the Bill.

(dd) Review of critical information infrastructure bases

The Committee agrees with the stakeholders that there should be a periodic review of organisations that are designated as "critical information infrastructure" bases. The Committee recommends that there be periodic reviews because the attributes or qualifications of being a critical information infrastructure base may change over time because of the rapid development of technology.

(ee) Cyber security hubs

The Committee notes that the Bill does not provide for the creation of structures such as a 24 hour point of contact to promote reporting of incidents of cyber crimes.

In this regard, the Committee recommends that the Bill should provide for the creation of structures for 24 hour point of contact, for cyber security hub and nodal points to promote reporting, investigation and prosecution of incidents of cyber crime. This is

because these points could provide immediate expedited assistance to investigate offences in terms of the Bill.

11. CONCLUSION

The National Assembly recently ratified the African Union (AU) Convention on Cyber Security and Personal Data Protection. In this regard, it is necessary that the Convention is domesticated for it to have the force of law in Zambia. The Cyber Security and Cyber Crimes Bill, N.A.B. No. 2 of 2021, will provide for the use, security, facilitation and regulation of electronic communications and transactions, and promote legal certainty and confidence, and encourage investment and innovation in relation to electronic transactions. The Bill is therefore domesticating the African Union (AU) Convention on Cyber Security and Personal Data Protection. Its enactment will ensure that there is regulation on the collection, use, transmission and storage of personal data.

While noting that the Bill is a progressive one, given the threats of terrorism and other cyber crimes, the Committee acknowledges the concerns raised by stakeholders and therefore, recommends that the Bill be deferred in order to allow the Ministry of Transport and Communications, the sponsor, and the Ministry of Justice to attend to the concerns raised

The Committee wishes to express its gratitude to all stakeholders who appeared before it and tendered both oral and written submissions. The Committee also wishes to thank you, Mr Speaker, for affording it an opportunity to scrutinise the Bill and appreciates the services rendered by the Office of the Clerk of the National Assembly.

We have the Honour to be, Sir, the Joint Committee of the Committee on Media, Information and Communication Technologies and the Committee on National Security and Foreign Affairs mandated to consider the Cyber Security and Cyber Crimes Bill, N.A.B. No. 2 of 2021, for the Fifth Session of the Twelfth National Assembly.

Dr M Malama, MP
(CHAIRPERSON)

Mr G M Imbuwa, MP,
(Member)

Ms P C Kucheka, MP
(Member)

Ms A M Chisangano, MP

(Member)

Mr D M Kundoti, MP
(Member)

Mr M Mukumbuta, MP
(Member)

Dr E I Chibanda, MP
(Member)

Mr M K Tembo, MP
(Member)

Dr F Ng'ambi, MP
(Member)

Mr D Mumba, MP
(Member)

Mr C D Miyanda, MP
(Member)

Mr G K Chisanga, MP
(Member)

Mr E J Muchima, MP

(Member)

Brig Gen S M Sitwala, MP (Rtd)

(Member)

Mr K Mbangweta, MP

(Member)

Mr L Nyirenda, MP

(Member)

Ms M Miti, MP

(Member)

Mr A Malama, MP

(Member)

Ms M Lubezhi, MP

(Member)

February, 2021

LUSAKA

APPENDIX I – National Assembly Officials

Ms C Musonda, Principal Clerk of Committees
Mr F Nabulyato, Deputy Principal Clerk of Committees (SC)
Mr H Mulenga, Deputy Principal Clerk of Committee (FC)
Mr C K Mumba, Senior Committee Clerk
Mr C Chishimba, Committee Clerk
Ms C R Mulenga, Committee Clerk
Mrs R Kanyumbu, Typist
Mr D Lupiya, Parliamentary Messenger

APPENDIX II – The Witnesses

1. Ministry of Justice
2. Ministry of Communications and Transport
3. Ministry of Defence
4. Ministry of Home Affairs – Zambia Police Forensic Section
5. Ministry of Youth and Sport and Child Development (Child Protection Unit)
6. Ministry of Information and Broadcasting Services
7. Financial Intelligence Centre (FIC)
8. Zambia Security Intelligence Services (ZSIS)
9. Human Rights Commission (HRC)
10. National Prosecution Authority (NPA)
11. Bank of Zambia (BOZ)
12. Zambia Revenue Authority (ZRA)
13. Zambia Telecommunications (ZAMTEL)
14. Airtel
15. Smart Zambia Institute (SZI)
16. Drug Enforcement Commission (DEC) (Anti Money Laundering Investigations Unit)
17. Zambia Centre for Accountancy (ZCAS)
18. National Anti-Terrorism Centre
19. Infratel
20. University of Zambia (Centre of Information and Communication Technology – Quality Assurance and Security Department)
21. Bankers Association of Zambia (BAZ)
22. Copperbelt University (School of Humanities)
23. Law Association of Zambia (LAZ)
24. Chapter One Foundation