REPUBLIC OF ZAMBIA

REPORT

OF THE

COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES ON THE ROLE OF THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY IN THE FIGHT AGAINST CYBER CRIMES

FOR THE

SECOND SESSION OF THE THIRTEENTH NATIONAL ASSEMBLY

Published by the National Assembly of Zambia

FOREWORD

Honourable Madam Speaker, the Committee on Media, Information and Communication Technologies has the honour to present its Report for the Second Session of the Thirteenth National Assembly. The functions of the Committee are set out in Standing Orders Nos. 197(b) and 198 of the National Assembly of Zambia Standing Orders, 2021.

In line with its Programme of Work for the Second Session of the Thirteenth National Assembly, the Committee undertook a study on the topical issue, namely: *The Role of the Zambia Information and Communications Technology Authority (ZICTA) in the Fight against Cyber Crimes*. The Committee held twelve meetings to consider the topical issue. In order to fully interrogate the topical issue, the Committee requested detailed memoranda from various stakeholders. The stakeholders were also invited to appear before the Committee and speak to their memoranda in order to afford the Committee an opportunity to make clarifications on issues contained in the memoranda. The list of stakeholders who provided memoranda and appeared before the Committee is at Appendix II.

The Committee's Report is organised in two parts. Part I presents the Committee's findings from its deliberations on the topical issue, including findings from the tours. Part I further presents the Committee's observations and recommendations on the topical issue. Part II contains the Committee's observations and recommendations on its consideration of the Action-Taken Report on the Report of the Committee for the First Session of the Thirteenth National Assembly.

The Committee is grateful to all stakeholders who tendered both written and oral submissions. The Committee further wishes to thank you, Madam Speaker, for affording it an opportunity to carry out its work. The Committee also appreciates the services rendered by the Office of the Clerk of the National Assembly during its deliberations.

Engineer Raphael Mabenga, MP
CHAIRPERSON

June, 2023
LUSAKA

Table of Contents

List of Acronyms

ACC	Anti-Corruption Commission
BOZ	Bank of Zambia
CCPC	Competition and Consumer Protection Commission
CERT-MU	Computer Emergency Response Team of Mauritius
CII	Critical Information Infrastructure
CIRT	Computer Incidence Response Team
COVID-19	Coronavirus Disease 2019
DEC	Drug Enforcement Commission
DPO	Data Protection Office
FIC	Financial Intelligence Centre
GIS	Government Information Services
HIPAA	Health Insurance Portability and Accountability Act
IBA	Independent Broadcasting Authority
ICAC	Independent Commission against Corruption
ICT	Information and Communication Technology
ICTA	Information and Communication Technologies Authority
IEC	International Electrotechnical Commission
INTERPOL	International Criminal Police Organisation
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
KYC	Know Your Customer
LAZ	Law Association of Zambia
LEAs	Law Enforcement Agencies
MNOs	Mobile Network Operators
MOU	Memorandum of Understanding
NCSACC	National Cyber Security Advisory and Coordinating Council
NPA	National Prosecution Authority
NPKI	National Public Key Infrastructure
PIA	Pensions and Insurance Authority
PII	Personal Identifiable Information
USB	Universal Serial Bus
VPNs	Virtual Private Networks
ZICTA	Zambia Information and Communications Technology Authority
ZM-CIRT	Zambia Computer Incidence Response Team

1.0 MEMBERSHIP OF THE COMMITTEE

The Committee consisted of Eng. Raphael Samukoma Mabenga, MP (Chairperson); Mr Sydney Mushanga, MP (Vice-Chairperson); Mr Masautso Kazungula Tembo, MP; Mr Andrew Lubusha, MP; Mr Munir Zulu, MP; Mr Romeo Kangombe, MP; Mr Walusa Mulaliki, MP; Mr Oliver M Amutike, MP; Mr Andrew Tayengwa, MP; and Mr Christopher Kang'ombe, MP.

PART I

CONSIDERATION OF THE TOPICAL ISSUE

2.0 THE ROLE OF THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY IN THE FIGHT AGAINST CYBER CRIMES

2.1 Background

The Eighth National Development Plan 2022 to 2026 recognised that investments in Information and Communication Technology (ICT) and science and technology would support digital transformation and innovation as key enablers under this strategic development area. ICTs had gained influence in the global development agenda and were essential investments required by all nations to achieve the 2030 Global Agenda.

Despite the Government putting regulations in place to enhance the confidence of ICT users, Zambia had continued to record an increase in cybercrime incidences with financial fraud being a common occurrence. From January to December, 2021, the Zambia Computer Incidence Response Team (ZM-CIRT) recorded 10,718,002 attacks. The cyber threats recorded in 2021 included mobile money reversal scams, social media account hijacking, fake online product promotions and investment schemes. The preceding evidence of cybercrime trends revealed that if not abated, cybercrime would lead to severe financial disruption and loss of productivity. For the period 2020 to the second quarter of 2022, the financial sector suffered losses in excess of K150 million. In the same period, over K6 million was lost due to pyramid schemes or fake financial investments.

The complex nature of cybercrime, which took place in the borderless realm of cyberspace, was compounded by the increasing involvement of organised crime groups. Perpetrators of cybercrime and their victims were often located in different regions and its effects ripped through societies around the world. Cybercrime had a retrogressive effect on the socio-economic wellbeing of constituents, businesses and societies as it mostly involved the loss of money, valuable personal or company data and sometimes reputational damage.

In view of the above, the Committee resolved to undertake a study to understand and appreciate the operations of the Zambia Information and Communications Technology Authority (ZICTA) in the fight against cybercrime.

3.0 OBJECTIVES

The objectives of the study were to:

(a) appreciate the policy and legal framework in which ZICTA operated;
(b) appreciate the role of ZICTA in the fight against cybercrime;

(c) ascertain the collaboration between ZICTA and other investigative and law enforcement agencies in the fight against cybercrime;
(d) appreciate the challenges, if any, in the fight against cybercrime; and
(e) make recommendations on the way forward.

4.0 SUMMARY OF SUBMISSIONS BY STAKEHOLDERS

The submissions made by the stakeholders are summarised below.

4.1 THE LEGAL AND POLICY FRAMEWORK WITHIN WHICH THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY OPERATES

(a) Legal Framework

The Committee was informed that the Zambia Information and Communications Technology Authority (ZICTA) was a statutory body established under the *Information and Communication Technologies Act, No. 15 of 2009* to regulate the ICT sector. The Committee learnt that ZICTA drew its mandate from three pieces of legislation namely:

i. ***the Information and Communication Technologies Act, No. 15 of 2009***, whose objective was to provide for the regulation of ICTs;
ii. ***the Cyber Security and Cyber Crimes Act, No. 2 of 2021***, whose objective was to provide for cyber security in Zambia; and
iii. ***the Electronic Communications and Transactions Act, No. 4 of 2021***, whose objective was to provide for a safe and effective environment for electronic transactions and empower ZICTA to supervise compliance relating to the Act.

(b) Policy Framework

In addition to the legal framework, the authority's mandate was further supported by policy frameworks as set out below.

i. The Information and Communication Technologies Policy of 2006

The 2006 Information and Communication Technologies Policy provided the overarching policy framework for the development of the ICT sector and was premised on capacity building, a competitive and efficient ICT sector, and an effective legal and regulatory framework as its key pillars.

ii. The Cyber Security Policy of 2021

The 2021 Cyber Security Policy provided a governance framework for cyber security in the country aimed at enhancing the confidence of users of ICTs through the establishment of a secure, reliable, and trustworthy cyber environment in order to fully realise the social and economic benefits of ICTs.

4.2 THE ROLE OF THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY IN THE FIGHT AGAINST CYBERCRIME

Stakeholders submitted that ZICTA was the primary institution responsible for promoting cyber security and preventing cybercrime as provided for in the aforementioned legislation and policies. The critical role of ZICTA was also supported by the African Union Convention on Cyber Security and Data Protection, which was intended to strengthen legislation on ICTs in Africa and which was ratified by Zambia.

The Committee was further informed that as part of ZICTA' role, it co-ordinated and oversaw activities relating to cyber security, combating cybercrimes and the disseminating information on emerging cyber threats and vulnerabilities to stakeholders. To this effect, the authority established a Cyber Security Department in August, 2021, to ensure coordinated implementation of the functions stipulated in the Act and appreciate the devastating effects that cybercrimes or attacks might have on the economy if not mitigated.

4.3 COLLABORATION BETWEEN THE ZAMBIA INFORMATION AND COMMUNICATIONS TECHNOLOGY AUTHORITY AND OTHER INVESTIGATIVE AND LAW ENFORCEMENT AGENCIES

While acknowledging the notable efforts that ZICTA had been making to protect the cyberspace, there had been an unprecedented rise in the occurrence of cybercrimes in Zambia such as online scams, fraud and identity theft. In order to protect the cyberspace, stakeholders submitted that ZICTA had been working in collaboration with various stakeholders which included the Zambia Police Service, the Drug Enforcement Commission (DEC), the Anti-Corruption Commission (ACC) and global social media companies. The Authority was also reported to have collaborated with regulators such as the Bank of Zambia (BOZ), the Independent Broadcasting Authority (IBA), the Pensions and Insurance Authority (PIA), the Competition and Consumer Protection Commission (CCPC) and Mobile Network Operators (MNOs).

In a bid to effectively fulfil its mandate, and considering that cybercrimes could not be fought by a single organisation, ZICTA, in its collaborative works with Law Enforcement Agencies (LEAs), also provided technical expertise, technical training and cyber security awareness. However, despite ZICTA having the expertise, it did not have the powers to prosecute, hence it had to work hand in hand with LEAs which had the legal backing to prosecute. Below were some of the areas in which ZICTA collaborated with LEAs:

(a) with the Zambia Police Service when they brought ICT gadgets for forensic examinations;
(b) with Zambia Police Service during the search and seizure of ICT gadgets that contained evidence which needed to be forensically extracted and examined for presentation in the Courts of Law;
(c) with the Zambia Police Service during the cyber security awareness programs;
(d) with the Zambia Police Service during other cyber-related operations;
(e) with the Law Association of Zambia (LAZ) and the National Prosecution Authority (NPA) during "Cyber and the Law" Workshops;
(f) with the CCPC during search and seizure operations;
(g) with the DEC during search and seizure operations;
(h) with MNOs in processing warrants;
(i) with the ACC during search and seizure operations; and
(j) with global social media companies such as Facebook for requests to take down malicious pages.

4.4 STRATEGIES PUT IN PLACE TO FIGHT CYBERCRIME

Stakeholders informed the Committee that ZICTA in the execution of its mandate had put in place strategies to secure the cyberspace and aid LEAs in the fight against cybercrime. They stated that a cyber security strategy, in this context, was a plan of action designed to improve the security and resilience of national infrastructure and services. It was a high-level top-down approach to cyber security that established a range of national objectives and priorities that could be achieved in a specific timeframe. The Committee was further informed that ZICTA had put in place various strategies to tackle the risks which had the potential to undermine the achievements that Zambia had achieved so far. Some of the strategies that ZICTA was reported to have had implemented are set out below.

4.4.1 Cyber Security Sensitisation and Awareness Programmes

The Committee was informed that the sensitisation of the public on cyber hygiene was one of the strategies used to boost cyber security awareness, reduce cybercrime and equip people with information on how to avoid becoming victims of ransomware. This was being done in all the ten provinces of the country through radio talk shows, television programmes and workshops. Sensitisation programmes were also carried out in schools, colleges, churches and markets. During these awareness sensitisation programmes, campaign materials with various messages about cyber security were distributed. ZICTA also took advantage of huge gatherings such as traditional ceremonies to reach out to the public on these matters. Furthermore, a socialite with a large social media following was picked to be a cyber security ambassador and regularly shared with their followers on social media how to be cyber smart.

Considering that an estimated 80 per cent of cyber-attacks could be prevented through better education and awareness among users, the Cyber Security Awareness Programme was a deliberate national public awareness effort done by ZICTA annually aimed at increasing the understanding of cyber threats and empowering the public with information on how to be safe and secure online. The awareness campaign targeted mostly youths, who were the major consumers of ICT services in Zambia.

The Committee was informed that the ZICTA Cyber Security Awareness Month, which takes place annually, was done in October, 2022. During these campaigns, topics such as how to come up with strong passwords, how to leave privacy settings turned on, how to make online purchases from secure sites and how to be cautious on who to meet online were shared. Additionally, as part of end-user education, the stakeholders submitted that the sensitisation programmes addressed how anyone could accidentally introduce a virus into an otherwise secure system by failing to follow good security practices. The trainings also included teaching users to delete suspicious email attachments, advising them not to plug in unidentified universal serial bus (USB) drives, and educating them on various other important lessons which would ensure the integrity of secure systems.

4.4.2 Introduction of Sector-Based Computer Incidence Response Teams

The Committee was informed that as the Zambian economy grew in various sectors such as finance, energy and transport, ZICTA saw the need to move from a generic national Computer Incidence Response Team (CIRT) to a sector-based CIRT. Sector-based CIRTs had the following benefits when compared to generic national CIRTs:

(a) specific information and in-depth knowledge in their sectors;
(b) sector-specific network of contacts;

(c) closer relationships with vendors of the sector;
(d) expertise on sector-specific hardware and systems;
(e) sector-specific conferences, workshops, and trainings;
(f) creation of uniform frameworks for audit documentation at sectoral level;
(g) faster sectoral communication channels due to smaller constituency base; and
(h) sector-specific recommendations.

In addition, the Committee was informed that CIRTs would be an important player to organise sectoral exercises as they had good communication channels and closer relationships with the main sectoral stakeholders at national level.

4.4.3 Provision of Cyber Security Training

Stakeholders submitted that the fight against cybercrime required the upskilling of ICT personnel from ZICTA, LEAs and other investigative wings to equip them with the requisite capacity. The challenges they faced included investigating a broad variety of cybercrimes and threats posed by criminals, hackers, terrorists, and foreign state actors which included phishing scams, website spoofing, ransomware, malware and hacking. The Committee was informed that ZICTA was training LEAs on how to handle cyber-related matters from inception to disposal. These trainings involved chain of custody management to ensure evidence was admissible in the courts of law for the prosecution of offenders. ZICTA also trained officers from LEAs on how to conduct cybercrime awareness programmes. It had, therefore, been collaborating with and providing training and digital forensics equipment to the security wings.

4.4.4 Establishment of a Dedicated Cyber Security Department

The Committee was informed that in the recent past, the Cyber Security Unit at ZICTA was under the Directorate of Technology and Engineering. To give requisite attention to emerging cyber threats and cybercrime, management at ZICTA decided to create a Directorate of Cyber Security, appoint a director and give it a budget line. This was a deliberate move by management to show commitment towards combating cybercrime. This initiative to setup a dedicated department for cyber security was applauded by many stakeholders as it demonstrated top leadership commitment to fighting cybercrime.

4.4.5 Decentralisation Policy

The Committee was informed that in line with the Government's Decentralisation Policy and the 1st to 8th National Development Plans, ZICTA actualised its plans to get closer to its stakeholders by opening offices in four provinces which included the Southern Province, the Eastern Province, the Copperbelt Province and Muchinga Province. The opening of these offices marked a huge milestone in the decentralisation and deconcentration of ICT regulatory services across the country. The strategy was to open offices in all the ten provinces according to ZICTA's 2020 to 2027 Strategic Plan.

4.4.6 Strengthening of Legislation

The Committee was informed that consultations took place around amending legislation regulating the cyber security sphere in Zambia in order to clear bottlenecks and ambiguity, rectify the duplication of functions and align it with international best practices. Stakeholders submitted that a memorandum had been circulated within the ministries seeking input on which pieces of legislation needed to be amended. The three "cyber laws", namely: the *Cyber Security and Cyber Crimes Act, No. 2 of 2021,* the *Electronic Communications and*

Transactions Act, No. 4 of 2021 and the *Data Protection Act, No, 3 of 2021* were identified as needing amending.

4.4.7 SIM-Card Deregistration

Stakeholders informed the Committee that ZICTA started the process of de-registering or deactivating subscriber identity module (SIM) cards with incorrect or poor Know Your Customer (KYC) details. They indicated that scammers used dubiously acquired SIM-cards to scam people as they knew that they could not be easily traced. Consequently, about two million SIM-cards had since been de-registered or deactivated by the second quarter of 2022.

4.4.8 Formulation of Child Online Protection Strategy

Stakeholders informed the Committee that the formulation of the Child Online Protection Strategy had been a collaborative process with various stakeholders involved in the promotion of child protection and the development of children's rights. The Child Online Protection Strategy that was being executed from 2020 to 2024 was developed to spell out modalities with regard to ensuring a safe online experience for children at all times. The strategy gave a clear mandate to the Ministry responsible for ICTs, the Ministry responsible for child development, regulators, the private sector and civil society and other line ministries and institutions to mainstream child online protection across all sectors. The strategy ensured the implementation of programmes dealing with child online risks, the education of children on the safe use of the internet and the provision of practical tools that encouraged various stakeholders to ensure a better online experience for children.

4.4.9 Cybercrime Forensic Laboratory

The Committee was informed that in 2014, ZICTA, in collaboration with the Zambia Police Service, installed and commissioned the first cybercrime forensic laboratory based at the Zambia Police Service Headquarters in Lusaka. The laboratory was meant to provide information that focused on identifying, acquiring, processing, analysing, and reporting on data stored electronically. Digital forensic examiners performed comprehensive technical analysis of digital forensic evidence without altering original data, as well as forensically collected evidence from crime scenes for examination purposes.

4.4.10 Compelling Mobile Network Operators to Support Law Enforcement Agencies

As a regulator of the mobile and internet service providers, ZICTA ensured that these entities supported the LEAs in the fight against cybercrimes. For instance, in cases where LEAs requested customer call records and internet protocol (IP) addresses of suspects of cybercrimes under warrant, ZICTA ensured that there was smooth cooperation between LEAs and the service providers. Where there was a delay to respond to requests, ZICTA could be called upon to intervene due to the rapid nature of cybercrimes.

4.4.11 Collaboration with Law Enforcement Agencies and Provision of Expert Witness in Court

The Committee was informed that in a bid to effectively fulfil its mandate of safeguarding citizens from cyber-related crimes such as online scams, fraud and identity theft, ZICTA worked in collaboration with LEAs in the investigation of cybercrimes and other matters by providing technical expertise, technical training, and cyber security awareness. These LEAs included the Zambia Police Service, the DEC, and the ACC. This collaboration between ZICTA and LEAs was important as ZICTA had no legal powers to arrest or prosecute perpetrators of crime. Through collaboration with LEAs, ZICTA provided expert witnesses in court on cybercrime-related matters because cybercrime cases were difficult to prosecute unless a technical expert such as an officer from ZICTA gave input.

4.4.12 Interaction with the Public as Part of Consumer Protection

The Committee was informed that ZICTA interacted with the public on matters to do with cybercrime through its call centre. The call centre, which was accessed through a toll-free line 7070, enabled people who could not physically walk to ZICTA to interact with its experts. Through the call centre, the public reported cyber-related cases, reported stolen phones, gave feedback to ZICTA and made follow-ups on reported cases. The Committee was further informed that ZICTA, in consultation with BOZ and the Financial Intelligence Centre (FIC), among others, had introduced short codes such as *101# which revealed the number of SIM-cards that were registered under one name as well as the *707# short code for purposes of reporting scams and unsolicited messages.

4.4.13 Obtaining Statistics of Cybercrimes

The Committee was informed that ZICTA had compiled statistics on cyber-related cases and published them in its annual report. These statistics gave the landscape of cybercrime in the country and acted as input in decision making by various organisations as cybercrime was one of the emerging risks for most organisations, particularly those that offered financial services. These statistics were also used to measure the efficacy of current interventions and formed the basis of strategies to be put in place in future.

4.5 CHALLENGES REGARDING COLLABORATIVE WORK IN THE FIGHT AGAINST CYBERCRIME

Stakeholders highlighted the challenges set out below.

4.5.1 Lack of Top Leadership Support

Most stakeholders submitted that cybercrime affected all Government institutions and departments. ZICTA, as a regulator, had put measures in place to fight cybercrime but the various institutions in the country needed to adopt best practices and entrench them in their daily operations. A lack of commitment towards the fight against cybercrime was noticed in the top management of most institutions as demonstrated by the lack of provision of adequate budgets, human resources and institutional frameworks. Several institutions did not have departments, let alone roles, dedicated to the monitoring, detection and remediation of cyber security threats. It was also noted that ZICTA alone could not fight the scourge of cybercrime and that more institutional will was needed.

4.5.2 Lack of Adequate Professional Skills

Stakeholders submitted that the wide range of technologies and vectors of attack available to criminals and the cross-border nature of cybercrimes made investigating them difficult. The fragile nature of digital evidence complicated matters as skilled cybercriminals erased their tracks and left little to no clues behind. The Committee was informed that one major challenge was the limited capacity within some LEAs to effectively and efficiently tackle cybercrime-related cases. The intrusive nature of investigating cybercrimes typically required the removing of computer equipment for analysis by highly skilled cyber security personnel with expertise which were lacking in most agencies. Furthermore, the processes involved in preserving digital information to ensure its admissibility in court required particular forensic skills that the average law enforcement personnel did not possess.

4.5.3 Ineffective Inter-Agency Collaboration

Stakeholders submitted that ineffective inter-agency collaboration was one of the major challenges hampering the fight against cybercrime. To enhance inter-agency collaboration, there was need to develop cross-sectoral collaborative frameworks to effectively address cybercrimes. A formal and permanent task force needed to be set up with team members identified and incentivised appropriately.

4.5.4 Lack of Financial Resources to Support Task Force

To collaborate effectively in the fight against cybercrime, stakeholders submitted that ZICTA, LEAs and other investigative wings required financial resources. These resources would cover meetings, workshops, trainings and allow for the purchasing of specialised equipment needed in the fight against cybercrimes. The lack of financial resources has meant that a task force comprising of members from different agencies to enhance inter-agency collaboration in the fight against cybercrime has not yet materialised.

4.5.5 Process of Obtaining a Warrant

Stakeholders expressed concern regarding the length of the process involved in obtaining a warrant for the lawful interception of electronic communication. The process as it stood required a law enforcement officer to seek the consent of the Attorney General in writing prior to making an application before a Judge for an interception of communication order. However, the process delayed the pace at which investigations relating to cybercrimes took place, despite the fact that such cases required immediate action to obtain and preserve evidence.

4.5.6 Incomplete Cases and Procedural Deficiencies

Stakeholders observed with concern the high number of incomplete cybercrime-related cases involving large sums of money. They noted that the minimum time it took to complete a cybercrime investigation was three months while the maximum could be twelve months, but cases in Zambia took even longer. They also noted that there was a lack of published procedure on how to escalate suspected or successful breaches of information assets, a lack of published procedure on how long cases escalated for further investigation would take and inadequate feedback on investigated cases.

4.5.7 Lack of National Level Security Infrastructure

Stakeholders noted with concern the absence of key National Level Security Infrastructure (NLSI) such as centralised monitoring facilities to enhance visibility over Critical Information Infrastructure (CII) and intelligence sharing. They further noted the lack of National Public Key Infrastructure (NPKI) and a Root Certification Authority (RootCA).

4.5.8 Legal Provisions

Stakeholders informed the Committee that ZICTA was governed by a management board whose functions were to regulate the provision of electronic communication services and products and monitor the performance of the sector as provided for under the *Information and Communication Technologies Act, No. 15 of 2009*. The *Cyber Security and Cyber Crimes Act, No. 2 of 2021* also gave ZICTA the mandate to implement the Act through the National Cyber Security Advisory and Coordinating Council whose functions were separate from the functions of the Board. The Board and the Council were both appointed by the Minister responsible for Technology and Science, but neither was subordinate to the other. This made the management of ZICTA have a dual reporting line. Further, the *Data Protection Act, No. 3 of 2021* put the mandate of data protection and regulation of systems on ZICTA. It made provisions on how personal data would be processed but did not prescribe how it would be stored to avoid unauthorised access. Stakeholders, therefore, recommended the amendment of Section 12 (1) (g) of the *Data Protection Act, No. 3 of 2021*. Stakeholders further submitted that the three "cyber laws" were hurriedly formulated under pressure and passed through the process of scrutiny and finalisation within such a short period of time. The Committee was informed that one piece of legislation should take no less than three months from consultation to enactment, but only two months were allocated to the initial drafting teams to come up with the three Acts.

4.5.9 The Zambia Information and Communications Technology Authority Non-Regulatory Functions

The Committee was informed that the *Cyber Security and Cyber Crimes Act, No. 2 of 2021* conferred upon ZICTA certain non-regulatory functions, thus, presenting a conflict of interest for the authority. In particular, Part VI and Part IX of the Act, which dealt with aspects of the interception of communication, were examples of non-regulatory functions that should be implemented by LEAs or a specialised body charged with such a mandate to do so and equipped with the right expertise and design.

4.5.10 Lack of National Cyber Security Agency

The Committee was informed that Zambia did not have a dedicated cyber security agency unlike countries in different jurisdictions. The Committee was further informed that such an agency was necessary to counter any cyber attacks on the country's CII such as telecommunications systems, payment platforms, and Government databases and to secure cloud storage facilities. Stakeholders stated that this agency was necessary in order to allow ZICTA to continue executing its mandate of being a regulator while the role of cyber security would be taken away from it as it had no powers to arrest or prosecute criminals.

5.0 REPORT ON THE LOCAL AND FOREIGN TOURS

5.1 Local Tour

In order to consolidate its findings from the long meetings on the '***Role of the Zambia Information and Communications Technology Authority in the Fight against Cybercrimes***', the Committee undertook a local tour of selected institutions in Central and Southern Provinces of Zambia.

The sites visited by the Committee included the following:

(a) Zambia Police Service Headquarters – Forensic Department;
(b) Zambia Information and Communications Technology Authority (ZICTA) Forensic Unit;
(c) Zambia Revenue Authority (ZRA) Chirundu and Kazungula Borders;
(d) Zambia information and Communication Technology Authority Choma Office.
(e) Choma Central Police. and
(f) Livingstone Central Police.

The findings of the Committee are as set out below.

5.1.1 Meeting with Zambia Police Service Headquarters – Forensic Department

The Committee was informed that while police officers were capacitated with the skills to fight cybercrime, the Zambia Police Service did not have the requisite specialised equipment. As a result, they had to rely on equipment belonging to other organisations which added to the slow pace at which investigations were concluded and increased the possibility of information leaking. In this regard, Zambia was seen as a weak link in the Southern African Development Community (SADC) as it was not able to contribute as effectively as other neighbouring countries that had the necessary skills and machinery to fight cybercrime. Additionally, the Committee was informed that the Zambia Police Service should be accorded a seat on the board of ZICTA as an interim measure to quicken the pace at which information was exchanged between the two institutions.

5.1.2 Meeting with Choma Central Police Station

The Committee was informed that Choma Central Police Station had received forty-two cases of cyber related crimes in the first quarter of 2023, which represented an increase of twelve cases as compared to the same period in 2022 in which thirty cases were recorded. Among these cases, the most common ones were thefts using mobile money services, fake online financial transactions and impersonation.

The Committee was informed that ZICTA had assisted the police in tracking suspects who were using Facebook to swindle unsuspecting members of the public by creating profiles of prominent people such as Members of Parliament. The Committee was also informed that some of the challenges faced by Choma Police Station included the fact that no officer under the station was trained in cybercrime investigation techniques, the equipment for digital analysis at the digital laboratory was non-functional at times and international protocols were not well explained to officers.

5.1.3 Meeting with Livingstone District Police Headquarters

The Committee was informed that the most common types of cybercrime seen in the district were mobile money theft, identity theft and cyber-bullying. The Committee heard that it was necessary to introduce cybercrime training as part of the curriculum at police training schools as the majority of police officers lacked formal training in that sphere.

5.1.4 Meeting with ZICTA Lusaka Headquarters

The Committee was informed that there had been a 1,000 per cent increase in the amount of money that was being stolen from people using cyber tools. It was, therefore, recommended that more equipment, capacity building and human resources be secured in order to effectively fight cybercrime. In this regard, the Committee was informed that it would take approximately US$2.5 million to US$3 million to set up a fully-fledged cybercrime forensic laboratory.

The Committee was also informed that the Zambia Police Service made approximately ten to twenty information requests to ZICTA monthly, but some requests such as access to call logs did not fall within ZICTA’s jurisdiction. ZICTA and the Zambia Police Service had agreed that all requests for information had to come from the Zambia Police Service Headquarters in order to avoid situations where individual officers tried to access data without authority.

5.1.5 Meeting with ZICTA Choma Office

The Committee was informed that the Choma office was opened in December 2021 and had a staff complement of seven officers, although only four were employed at the time of the visit. The Committee was also informed the ZICTA Choma office serviced the Southern and Western Provinces of Zambia. The Committee further learnt that most crimes were committed through social engineering and that cybercrime manifested through mobile scams, identity theft and psychological manipulation.

During the interaction, the Committee was informed that in order to counter this, the Choma office had been carrying out awareness programmes in markets, schools and churches as well as through radio, television, short messaging system (sms) blasts and the distribution of flyers. In this regard, sixty schools had been visited in the Southern and Western Provinces since December, 2021 and pupils as young as Grade 7 were educated on child online protection as they were usually victims and sometimes even perpetrators of cybercrimes. Lastly, the Committee was informed that ZICTA was considering an internet exchange point (IXP) where internet infrastructure companies such as internet service providers (ISPs), web enterprises and telecommunication service providers could connect to exchange internet traffic.

5.1.6 Meeting with Zambia Revenue Authority Chirundu Border

The Committee was informed that cybercrime was part of the ZRA's mandate, although other agencies took the lead. The Committee was also informed that ZICTA's absence in Chirundu made it difficult to effectively collaborate with them.

The Committee was informed that spam messages were received from time to time but that staff had been adequately trained to avoid them with the help of an IT officer stationed at the ZRA Chirundu office who handled all ICT related matters. Some challenges faced included the delay in the procurement of a baggage scanner that was pledged by the Common Market for Eastern and Southern Africa (COMESA) European Development Fund (EDF) and a lack of local manpower to carryout periodic maintenance.

5.1.7 Meeting with Zambia Revenue Authority Kazungula One Stop Border Post

The Committee was informed that there was collaboration between all stakeholders stationed at the border post which included ZICTA, DEC, Zambia Police Service, Zambia Department of Immigration, ZRA and RTSA. The Committee was further informed that there were some attempts by criminals to hack electronic Government systems while others tried to defraud the Government by generating falsified receipts. However, the Committee was informed that safeguards against this included the addition of quick response (QR) codes to receipts as a means of authentication at entry and exit points.

5.1.8 Meeting with Road Transport and Safety Agency Choma Office

The Committee was informed that RTSA collaborated with LEAs in fight against cybercrime by providing data on vehicle ownership.

5.1.9 Meeting with Road Transport and Safety Agency Kazungula Office

The Committee was informed that RTSA sat on a databank which housed motor vehicle registration and licensing details and collaborated with DEC, ACC, the Zambia Police Service and ZICTA. The Committee was also informed that RTSA was in compliance with the *Data Protection Act No. 3 of 2021*. Additionally, the Committee was informed that recruitment and training of human resources, the running of the latest systems and employing security to guard physical locations housing critical information were some of the strategies that were being employed.

5.1.10 Meeting with Anti-Corruption Commission Choma Office

The Committee was informed that the ACC was a player in the fight against cybercrime and that it worked in collaboration with ZICTA which provided the bio data which was vital for investigations. Additionally, staffs from ZICTA were often used as witnesses in court.

The Committee also heard that the RTSA provided the ACC with motor vehicle registration and ownership details which were used in investigations. The Committee was further informed that the ACC had established a Forensic Department which analysed and extracted digital evidence. The Committee was further informed that although there were no formal meetings that took place with stakeholders, a Community Cooperative Coordination Initiative (CCCI) had been started where stakeholders met informally to discuss matters.

5.1.11 Meeting with MTN Choma and Livingstone Offices

The Committee was informed that criminals had been using MTN platforms to commit mobile scams and that it had received and actioned complaints brought to it by customers. The Committee was further informed that MTN collaborated with the DEC, ACC, ZICTA and the Zambia Police Service. Additionally, the Committee was informed that apart from delays caused by system shut downs, there had been delays in honouring affidavits brought to the Choma office because those affidavits had to be forwarded to the legal office in Lusaka the person with the clearance to pull certain data was based in Lusaka.

The Committee was informed that as a security measure, once a customer registered a subscriber identity module (SIM) card, only the owner of the SIM could reset the password. The Committee was also informed that mobile money agents were engaged everyday to ensure that they did not give customers their phones or expose their pins to them. Sms blasts were also sent to sensitise subscribers on the importance of security and to educate them on how to keep their pins secure.

5.1.13 Meeting with ZAMTEL Choma Office

The Committee was informed that Zamtel collaborated with ZICTA and LEAs in providing information needed for investigations. Zamtel submitted that session initiation protocol (SIP) servers which enabled calls based on the internet were being used by criminals to clone numbers. In this regard, it was proposed that the registration of SIP servers must be made mandatory.

5.1.14 Meeting with ZAMTEL Livingstone Office

The Committee was informed that the first step of Zamtel's security guidelines was to engage with agents on the on boarding process followed by a know your customer (KYC) verification process in which scrutiny of what agents had done to ensure that all procedures were followed took place. If there were mistakes, registration was rejected and customers received a message urging them to visit a Zamtel outlet in order to complete the registration process.

5.1.15 Meeting with AIRTEL Livingstone Office

The Committee was informed that Airtel took cybercrime seriously and that curbing it started at customer acquisition where the customer was required to produce an original NRC in order to complete the registration process. The Committee was also informed that the Airtel money platform was secure and that users were constantly being educated on the need to be alert and avoid sharing their pins at any cost. The Committee was informed that Airtel worked with LEAs when they presented a warrant for information and that this information was usually provided in less than forty-eight hours.

5.2 Foreign Tour

The Committee undertook a benchmarking tour to Mauritius to learn and appreciate the measures it had put in place over the years in the fight against cybercrimes in line with the Committee's topical issue.

The Committee interacted with various stakeholders including the following:

(a) Ministry of Information, Technology, Communication and Innovation;
(b) Computer Emergency Response Team of Mauritius (CERT-MU);
(c) National Computer Board;
(d) Government Information Services (GIS); and
(e) Other senior government officials.

Specifically, the Committee was interested to learn and share experiences on the following issues listed hereunder:

(a) the policy and legal framework governing cyber security in Mauritius;
(b) the role of the agency in charge of cyber security in the fight against cybercrime;
(c) the collaboration between the agency in charge of cyber security and other investigative and law enforcement agencies in the fight against cybercrime;
(d) the challenges, if any, in the fight against cybercrime; and
(e) any other information that would be relevant to the Committee.

The findings of the Committee during its tour are set out below.

5.2.1 The Policy and Legal Framework Governing Cyber Security in Mauritius

The Committee was informed that the *Computer Misuse and Cybercrime Act, 2003* was repealed and replaced by the *Cyber Security and Cybercrime Act of 2021* after analysis of laws from other jurisdictions. The law was also drafted in accordance with the Convention on Cyber Security and Personal Data Protection, also known as the Malabo Convention, and the Budapest Convention on Cybercrime. Further, the Committee was informed that Mauritius had other legislation and policies that were used in the fight against cybercrime including the *Mauritius Emerging Technologies Council Act, 2021,* the *Data Protection Act, 2017,* the *Information Communication Technologies Act, 2001*, the *Electronic Transactions Act, 2000,* the *National Computer Board Act, 1989* and the *Mauritius Research and Innovation Council Act 2019.*

5.2.2 The Role of the Information and Communication Technologies Authority in the Fight against Cybercrime

The Committee was informed that the Information and Communication Technologies Authority (ICTA) was responsible for regulating and supervising the country's telecommunications and Information Communication Technology (ICT) sector. ICTA worked to ensure that ICT infrastructure was secure and resilient against cyber threats and worked with stakeholders to promote good cyber security practices. Its roles were outlined as follows:

(a) Regulating and Supervising the Telecommunications and Information Communication Technology Sector

ICTA was responsible for ensuring that ICT infrastructure in Mauritius was secure and resilient to cyber threats. It set standards and guidelines for the design, operation, and maintenance of ICT systems to ensure that they were secure against cyber-attacks.

(b) Promoting Cyber Security Awareness

ICTA worked closely with other stakeholders to raise awareness about cyber security risks and best practices. It provided training and education to the public, private sector, and government entities on how to prevent cyber-attacks and protect against cybercrime.

(c) Investigating Cybercrime Incidents

ICTA worked closely with LEAs, such as the Cybercrime Unit of the Mauritius Police Force to investigate cybercrime incidents. It collected and analysed digital evidence, conducted forensic analysis, and provided technical support to LEAs in cybercrime investigations.

(d) Establishing Policies and Guidelines

ICTA established policies, guidelines, and regulations related to cyber security and data protection. It worked to ensure that the legal and regulatory framework for cyber security was up-to-date and relevant to the ever evolving threat landscape.

5.2.3 Collaboration between the Information and Communication Technologies Authority and other Investigative and Law Enforcement Agencies in the Fight against Cybercrime

The Committee was informed that the collaboration between ICTA and other investigative and LEAs in Mauritius was crucial in the fight against cybercrime. ICTA worked closely with LEAs such as the Cybercrime Unit of the Mauritius Police Force, the Independent Commission against Corruption (ICAC), and the Data Protection Office (DPO) to address cybercrime incidents.

The Committee was informed that ICTA collaborated with investigative and LEAs in the following ways listed hereunder:

(a) provided technical expertise, equipment, and support to LEAs in their investigations and worked to facilitate communication and information-sharing among stakeholders to ensure that cybercrime incidents were dealt with effectively;

(b) collaborated on capacity-building initiatives such as training programs and workshops to increase the knowledge and skills of investigators in the field of cybercrime with the aim of improving their ability to collect digital evidence, conduct forensic analysis, and prosecute cyber criminals effectively; and

(c) established policies and guidelines related to cyber security and data protection that ensured that the legal and regulatory framework for cyber security was up-to-date and relevant to the evolving threat landscape.

5.2.4 Strategies Put in Place to Fight Cybercrime

The Committee was informed that the following strategies listed hereunder were put in place to fight cybercrime:

(a) Cyber Caravans

The Cyber Caravans Project was used as a sensitisation tool by the National Computer Board and were equipped with desktop computers and internet connection and travelled around the island to deliver training and assistance to the public on the use of ICT with assistance provided by the IT Support Officers.

(b) National Computer Emergency Response Team

The Computer Emergency Response Team of Mauritius (CERT-MU) was a division of the National Computer Board which was tasked with promoting cyber security issues at the national level. The CERT-MU served as a focal point in Mauritius for computer security incident reporting and response.

Services offered by CERT-MU included the following listed hereunder:

(i) information security incident handling and management;
(ii) vulnerability scanning and penetration testing of networks, applications, and devices;
(iii) dissemination of security news and latest security alerts to constituency members;
(iv) advising parents on the issues of child online safety including social networking sites;
(v) security awareness programmes on information security; and
(vi) third party auditing and providing assistance in implementing ISO 27001.

(c) National Cybercrime Strategy

A National Cybercrime Strategy had been developed and approved by the government on 25th August 2017. The objective of the strategy was to enhance the law enforcement capacity and strengthen the legal framework in order to combat cybercrime effectively.

(d) Critical Information Infrastructure Framework

The project aimed at setting up a policy framework for information security assurance and CII protection with the main objective of identifying and protecting the CII of Mauritius. The policy was based on the United Nations Resolution 58/199 which related to creating a global culture of cyber security and protection of CII and focused on leadership, risk mitigation and awareness and defined a plan of immediate actions to strengthen the security and resilience of CIIs.

(e) Setting up of a Centre of Excellence on Cyber Security and Cybercrime

The Ministry of Information, Technology, Communication and Innovation was setting up a Centre of Excellence on Cyber Security and Cybercrime in Mauritius to address the main challenges facing the country such as the harmonisation of cybercrime policies and legislative frameworks; fostering of international co-operation through promotion of information sharing; how to address rapid advances in the deployment of new technologies to fight cybercrime and mapping legal and regulatory instruments with existing regional and international best practices and capacity building for technical managerial expertise. The centre was to serve as a common platform to discuss how law enforcement agencies detected, handled and prosecuted cybercriminals and for the judiciary to understand this highly technical and complex area whenever cases are brought before courts.

(f) Security Operations Centre

The Committee was informed that the Mauritius Security Operations (SOC) was a centralised unit responsible for monitoring, detecting, analysing, and responding to cyber security incidents within the country. It served as the primary point of contact for all cyber security-related incidents and events, and was tasked with protecting Mauritius' CII, including government networks, financial institutions, and other key industries. The Committee was further informed that the SOC operated around the clock and used advanced security technologies and threat intelligence to identify and mitigate cyber threats in real-time.

5.2.5 The Challenges Faced in the Fight against Cybercrime

(a) Inadequate Enforcement

The Committee was informed that the biggest challenge that Mauritius faced in the fight against cybercrime was the enforcement of the existing cyber laws. While the legal and policy frameworks adequately catered for a range of cybercrimes, enforcement of these regulations still proved to be difficult. The Committee further was informed that the use of Virtual Private Networks (VPNs) and posts from Internet Protocol (IP) addresses out the jurisdiction made it difficult to investigate and secure convictions in cybercrime related cases. The Committee was further informed that the police lacked adequate technically proficient staff to fight cyber crimes.

(b) Inadequate Financing

The Committee was informed that central government ICT spending was the share of total central government budgets dedicated to ICTs including investments in hardware and software, running costs of IT infrastructure, salaries for ICT specialists and training. The international standard for central government ICT spending was 10 per cent of the national budget. However, the ICT interventions under various ministries in Mauritius amounted to an estimated 7 to 8 per cent of the national budget with the Ministry of Information, Communication, Technology, and Innovation being allocated only 5 per cent. The Committee was further informed that the Ministry of Information, Technology, Communication and Innovation was engaging with the Ministry of Finance in the hopes to secure more financing in the 2024 national budget to bolster ICT interventions and increase Mauritius' International Telecommunication Union (ITU) ranking in the world from fifty-second to forty-third.

(c) Dynamic Nature of Cybercrimes

The Committee was informed that the dynamic and ever evolving nature of cybercrimes was a challenge as interventions procured at great cost often became obsolete or needed to be updated every few months. The Committee was further informed that the dynamism of cybercrimes required the constant capacity building of technical staff, which was very costly.

(d) Collaboration with Regional Nations and Social Media Websites

The Committee was informed that certain African countries did not have basic cyber protection, had weak policy and legal frameworks regulating their ICT sectors and were not signatories to key international conventions on cyber security. As a result, collaboration with them in dealing with cyber attacks on Mauritian ICT infrastructure launched in their jurisdictions proved to be difficult. The Committee was further informed that the Ministry of Information, Technology, Communication and Innovation had been in contact with Facebook and Tiktok in order to dialogue over the time it took for complaints made about posts by the ICTA. Malicious and defamatory posts that were made on these platforms often stayed online for weeks as the social media sites took too long to resolve them.

6.0 COMMITTEE'S OBSERVATIONS AND RECOMMENDATIONS

6.1 Sector Specific Computer Incident Response Teams

The Committee notes that the management of CII in different sectors is beyond ZICTA's mandate and there are no sector-specific CIRTs to enhance the detection of cyber threats and incidences. In this regard, the Committee recommends that the process of reviewing the *Cyber Security and Cyber Crimes Act, No. 2 of 2021* and the proposed guidelines relating to CII be expedited to ensure that the Authority is able to address cyber threats.

6.2 Inadequately Skilled Personnel

The Committee observes that the fight against cybercrime is a mammoth task that requires a large and highly skilled group of specialists in order to match the efforts of criminals. The Committee notes with concern the insufficient number of adequately qualified personnel to efficiently and effectively tackle cases. In this regard, the Committee recommends that the Executive should ensure that funds are secured to facilitate expert training and continued capacity building of LEAs in order to be able to combat cybercrimes.

6.3 Lack of Consolidated Know Your Customer Systems

The Committee observes a lack of consolidated Know Your Customer (KYC) systems for all mobile network operators. Therefore, the Committee recommends that ZICTA should finalise the implementation of the consolidated KYC systems for all mobile network operators so that mobile scams can be nipped in the bud and perpetrators can be identified using national digital systems.

6.4 Limited Information and Communication Technology Infrastructure Funding

The Committee observes with concern that there is generally inadequate funding towards ICT infrastructure to effectively combat cybercrimes. In this regard, the Committee recommends that more funding be provided to ZICTA, or the institution earmarked to oversee cyber security, to equip cyber security inspectors with required hardware and software tools to fight cybercrimes. The funds are required to incentivise and attract top talent in cyber security. The Committee further recommends that ZICTA should be allowed to keep 100 per cent of the proceeds from the sale of spectrum, as opposed to the 80 per cent that it had been given, as this will enable it to better execute its mandate.

6.5 National Cyber Security Agency

The Committee observes that ZICTA's mandate is that of a regulatory body. Therefore, the Committee recommends that the *Cyber Security and Cyber Crimes Act, No. 2 2021* which gives ZICTA the mandate to be the cyber security regulator in the country needs to be amended and that a National Cyber Security Agency which would be an independent institution focused on cyber security be established. ZICTA should be left to focus on regulating the ICT sector in its broad perspective and not be part of the industry players.

6.6 Cyber Defence and Security Agency under the Defence Forces

The Committee notes that stakeholders have requested an express exemption for the Defence Forces from some of the provisions of the *Cyber Security and Cyber Crimes Act, No. 2 of 2021* as ZICTA, whose mandate under the Act is to register and regulate cyber security service providers, cannot oversee the operations of the Defence Forces. Further, the Committee notes the absence of a cyber defence and security agency under the Defence Forces. Therefore, the Committee recommends that the Executive considers the formation of a Cyber Defence and Security Agency to counter any attacks on the country's critical infrastructure such as telecommunications systems which may paralyse electronic payment platforms.

6.7 Decentralisation

The Committee observes the insufficient number of ZICTA offices in the provinces and districts. The Committee, therefore, recommends that ZICTA operations be decentralised to all provinces and districts to enable LEAs work efficiently.

6.8 Capacity Building in Law Enforcement Agencies

The Committee observes that there is need for continued capacity building of law enforcement officers in the relevant technical fields needed in the fight cybercrime. Therefore, the Committee recommends that ZICTA increases the capacity of law enforcement personnel through periodic specialised training.

6.9 Integrated National Cyber Security System

The Committee observes that there is need for the establishment of an Integrated National Cyber Security System managed by ZICTA, in collaboration with the Zambia Police Service, to improve the early detection, reporting, response to, and thwarting of cybercrimes. Cognisant of the increasing risk of cyber attacks, Rwanda launched a US$3 million cyber security system in 2016 aimed at protecting public and private institutions against cybercrime. The Committee, therefore, recommends that the Government considers procuring a similar centralised monitoring system that will be pivotal in enhancing visibility over CII. It will include, but not be limited to, sensitive installation points such as ZESCO Limited power distribution systems, the national gateways, electronic bank payments and other networks. The system will also secure services like immigration, taxation, and ICT equipment vital to national security.

6.10 Establishment of Cybercrimes Court System

The Committee observes that the complexity of cybercrimes requires specially trained staff at ZICTA and in investigative agencies. The Committee, therefore, recommends that the Government should consider establishing a cybercrimes court system within the Judiciary. This court should be supported by staff with a hybrid of ICT and legal expertise for effective prosecution of cybercrimes, most of which are of are complex and technical nature.

6.11 Compliance Monitoring

The Committee observes that in order to effectively perform the task of overseeing the Zambian ICT sector, ZICTA needs to be capacitated with the necessary staffing levels to monitor compliance and enforce protection of citizens' private digital data in accordance with the *Data Protection Act, No. 3 of 2021*. ZICTA's technical staff need to consistently be on the ground to physically check whether businesses meet the required local and international standards of service provision and data protection. The Committee, therefore, recommends that physical inspection of ICT infrastructure be undertaken before the issuing of licenses to organisations that will be handling citizens' sensitive data. This is to ensure that the said infrastructure is resilient against attacks like phishing, cross site scripting, denial of service attacks, data diddling, computer hacking as well as vandalism and theft.

6.12 Periodic White Hat-Hacker Driven National Systems Resilience Tests

The Committee observes that resilience tests have helped countries like the United States of America to uncover vulnerabilities in their computer networks. The acquired results of these tests allow them to tighten up their cyber defences and close gaps before any real cyber criminals exploit them. Therefore, the Committee recommends that ZICTA spearheads periodic tests of Government systems and CII to check the extent of resilience and vulnerability to attacks.

6.13 Security Operations Centre

The Committee observes that Zambia, unlike other countries in the region such as South Africa and Kenya, does not have a Security Operations Centre (SOC). This is an automated security monitoring and incident response mechanism which organisations such as financial institutions and banks deploy to secure their digital payment systems. Therefore, the Committee recommends that the Government establishes a SOC attached to the national security apparatus in collaboration with ZICTA.

6.14 External Collaboration

The Committee notes that there is need for collaborative efforts and information exchanges with similar organisations in neighbouring countries, regional cyber security bodies and international LEAs like INTERPOL. The Committee, therefore, recommends that ZICTA increases collaborative activities in the region and overseas, strengthens engagement and collaboration with all stakeholders to develop mechanisms and policies, and implements cyber security initiatives that will contribute to a secure and resilient cyberspace in Zambia. The Committee further recommends that ZICTA develops a framework for national, regional and international co-operation and collaboration and establishes a trusted information sharing mechanism for information exchange and incident reporting for national and international stakeholders.

6.15 Need for Updated Statistics

The Committee notes that Page 6 of the National Cyber Security Policy 2021 states that the country has inadequate national statistics on the nature and incidences of cybercrimes. The Committee, therefore, recommends that cyber security and cybercrime statistics should be collected and kept current.

6.16 Amendment of Legislation

The Committee notes that the three "cyber laws", which are the *Information and Communication Technologies Act, No. 15 of 2009*, the *Cyber Security and Cyber Crimes Act, No. 2 of 2021 and* the *Data Protection Act, No. 3 of 2021* are inadequate. Therefore, the Committee recommends that some of their provisions be reconsidered for purposes of weighing them against the rights the Republican Constitution bequeaths to individuals in Zambia.

6.17 Cybercrime Departments in Mobile Network Operators

The Committee observed that there were no dedicated cybercrime departments in the organisational structures of mobile network operators. In this regard, the Committee recommends that each mobile network operator creates a cybercrime department which shall detect and investigate cybercrimes, collaborate with LEAs, ensure compliance with cybercrime laws and enhance incident response capabilities.

6.18 Permanent Communication Structure

The Committee observed the lack of a permanent communication structure among MNOs, ZICTA and the Zambia Police Service. It was further observed that in the absence of this communication structure, the pace at which investigations were completed was delayed as MNOs would take several months to respond to court warrants. In this regard, the Committee recommends that ZICTA comes up with a committee which should include all LEAs and mobile network operators and meet periodically to engage on pressing issues, especially those which hinge on matters regarding cybercrime investigations.

6.19 Specialised Cybercrime Investigation and Prevention Courses in Police Training Curriculum

The Committee observed that the police officers generally lacked specialised training in cybercrime investigation and prevention techniques. The Committee further observed that most officers who managed to successfully investigate cybercrime cases did so using their ingenuity and basic investigation skills. In this regard, the Committee recommends that specialised cybercrime investigation and prevention courses be added to the curriculum of all police training colleges to enhance investigative capabilities of police officers and address the growing cyber threat landscape.

6.20 Collaboration with Social Media Websites

The Committee observed that ZICTA and LEA often encountered delays in receiving responses and cooperation from Facebook and other social media platforms during investigations. The Committee further observed that the Government of Mauritius had threatened to ban Facebook in the country if its concerns regarding cyber bullying, the spread of misinformation and impersonation were not addressed. This move saw the Facebook Africa team reaching out to the Government of Mauritius directly in order to find a more collaborative way of dealing with issues. In this regard, the Committee recommends that the Zambian Government should take a similar approach and engage Facebook more aggressively as the current channels of engagement do not seem to be yield positive results.

7.0 CONSIDERATION OF THE ACTION-TAKEN REPORT ON THE REPORT OF THE COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES FOR THE FIRST SESSION OF THE THIRTEENTH NATIONAL ASSEMBLY

7.1 REVIEW OF THE MEDIA SPACE IN ZAMBIA

7.1.1 Access to Information Legislation

In the previous Session, the Committee had noted with great concern that it had been nineteen years since the access to information legislation was withdrawn from Parliament in November 2002. This meant that if the law was not presented before Parliament by November, 2022, it would be twenty years since it was withdrawn. The Committee was saddened at the inordinate delay especially since the law was not meant for the media but would also enable the general populace to have access to information.

In this regard, the Committee had recommended that, as a matter of urgency, the Executive speeds up the process of enacting the access to information legislation to enable both journalists and members of the public have access to information.

Executive's Response

In the Action-Taken Report, the Executive informed the Committee that the New Dawn Government, through the Ministry of Information and Media, was frantically putting measures in place to ensure that the access to information law was enacted. The Ministry, in conjunction with the Office of the Vice President, and with guidance from Ministry of Justice, was studying the laws that would be affected by the enactment of the access to information law to see how that could be taken care of. To that effect, the Ministry through the Honourable Minister of Information and Media would keep on updating the National Assembly on the progress regarding this matter.

Committee's Observation and Recommendation

The Committee in noting the submission expresses concern on the inordinate time it has taken for the Access to Information Bill to be brought back to Parliament after its withdrawal twenty years ago. In this regard, the Committee urges the Executive to ensure that the process of studying the laws that would be affected by the enactment of the law is expedited and resolves to await a progress report on the matter.

7.1.2 Zambia Media Council Legislation

In the previous Session, the Committee had agreed with stakeholders who observed that the unprofessional conduct exhibited by media houses and journalists could be attributed to the absence of a regulatory body that may offer checks and balances. They were of the view that if the regulatory body was put in place, it would come up with the standard code of ethics against which society could measure the conduct of journalists and media houses. As had been emphasised by media practitioners, the process to establish a regulatory body should be owned and driven by media bodies to ensure an independent process that would be inclusive and transparent.

The Committee, therefore, had recommended that the Executive expedites the process of enacting the Zambia Media Council legislation which would establish a self-regulatory mechanism that would, among other things, provide for a standardised code of ethics, and create an ombudsman's office which would act as a mediator between media houses and the aggrieved persons as well as resolve conflicts between media houses. The continuous delay to establish the Zambia Media Council would perpetuate the unprofessional conduct by media houses and journalists.

Executive's Response

The Executive in its response informed the Committee that New Dawn Administration through the Ministry of Information and Media working together with the Media Liaison Committee was already in the process of enacting the Media Council Law. The final Zambia Media Council Layman's Bill was at the Ministry of Justice for clearance. To that, the Ministry would keep on updating the National Assembly on the progress regarding this matter.

Committee's Observation and Recommendation

The Committee in noting the submission resolves to await a progress report on the matter.

7.1.3 Media Law Reforms

The Committee in the previous Session had noted that the *Penal Code Act, Chapter 87 of the Laws of Zambia*; the *Public Order Act, Chapter 113 of the Laws of Zambia*; the *State Security Act, Chapter 111 of the Laws of Zambia*; the *Printed Publications Act, Chapter 167 of the Laws of Zambia* and the *Cyber Security and Cyber Crimes Act, No. 2 of 2021, were among the laws that* had provisions that were inimical to the practice of journalism. Most of the provisions in the cited pieces of legislation were being used to the detriment of the media in Zambia.

In this regard, the Committee had recommended that the above mentioned pieces of legislation as well as others that contained provisions that were detrimental to the media, be revised and harmonised so as to curtail abuse by those in privileged positions. This would enable journalists to perform their duties without fear of abrogating the laws.

Executive's Response

The Executive in the Action-Taken Report informed the Committee that the enactment of the Access to Information Law would directly trigger the review of many pieces of legislation. Therefore, the pieces of legislation that had been cited by the Committee were among those that would be affected by the enactment of the Access to Information Law and would thus need to be reviewed and/or amended. In that regard, and as alluded to above, the Ministry of Information and Media in conjunction with Ministry of Justice was consulting the Ministries responsible for administering those pieces of legislation to agree on the way they should be dealt with to facilitate the enactment of the Access to Information Law.

Committee's Observation and Recommendation

The Committee in noting the submission urges the Executive to ensure that the pieces of legislation that will be affected by the enactment of the Access to Information Law are reviewed without further delay. The Committee resolves to await a progress report on the matter.

7.1.4 TV Levy

The Committee in the previous Session, had agreed with stakeholders who observed that the TV Levy had not been increased from the time it was introduced when other parastatal bodies such as ZESCO Limited and water utility companies were allowed to increase their tariffs. They also noted that despite the increase in the number of hotels, lodges and households being observed countrywide, the amount of the TV Levy being collected by the IBA had remained the same.

The Committee, therefore, had recommended that the TV Levy should be increased from K5 to K10 or K15 and also proposed the introduction of a radio levy which should be pegged at K2. Further, the Committee was of the view that, in the best interest of the Corporation, the collection of the TV Levy should be reverted to ZNBC.

Executive's Response

The Executive in the Action-Taken Report informed the Committee that, regarding Zambia National Broadcasting Corporation's collection of TV Levy, the collection of TV Levy by the Independent Broadcasting Authority was provided for in the Independent Broadcasting Authority Act. In addition, the Committee was informed that the Corporation had no new system/mechanisms for collecting the said TV Levy. Pertaining to the issue of increasing the TV Levy, the Ministry of Information and Media was carefully studying the matter for possible adjustment and introduction of Radio Levy.

Committee's Observation and Recommendation

The Committee in noting the submission resolves to await a progress report on the matter.

7.1.5 Demotivated Workforce at Zambia National Broadcasting Corporation

The Committee in the previous Session had noted with concern that workers with higher qualifications such as Master's degree in their field of training were supervised by people with lower qualifications who were perceived to be politically connected. Additionally, some qualified workers had been on attachment for more than five years and wonder why officers who opt to go on early retirement were re-engaged on contractual basis. Further, the Corporation was highly understaffed such that some workers only went on leave when they were ill. The Committee, in this regard, had recommended that the Executive ensures that the ZNBC structure was addressed in order to motivate its workforce.

Executive's Response

In the Action-taken Report, the Executive stated that the demotivation of the Corporation's staff was due to the financial challenges that it had continued to grapple with. Therefore, what was required was to improve the financial position (standing) of the corporation. Unfortunately, providing a grant to the Corporation was not a sustainable solution. To that effect, the Committee was informed that the Government's plan was to right-size the Zambia National Broadcasting Corporation and the Ministry of Information and Media was in the process of undertaking this course of action.

Committee's Observation and Recommendation

The Committee in noting the submission urges the Executive to specify when it intends to right-size the workforce at ZNBC. The Committee resolves to await a progress report on the matter.

7.1.6 The Public Order Act, Chapter 113 of the Laws of Zambia

While acknowledging the importance of the Public Order Act, the Committee in the previous Session had bemoaned the lopsided application of the Act alleging that some police officers and political cadres forcibly disrupted radio programmes claiming that the sentiments being made were likely to cause the breach of peace. Sometimes, cadres from the ruling party stormed radio stations claiming that the comments and the tone of language being used by a member of the Opposition were likely to cause the breach of peace. The same happened in Opposition strongholds. However, when similar comments and tones were used by someone from the ruling party, the programme was never disrupted. Clearly, this showed that the law was being applied disproportionately.

In this regard, the Committee had recommended that the law be applied proportionately because Zambia was a democratic nation and the Constitution provided for the free expression of divergent views. Therefore, the Committee further recommended that the Government should ensure that media houses were allowed to host all political leaders so as to ensure that they did not avoid hosting some members of society in a bid to remain on the right side of the law.

Executive's Response

In the Action-Taken Report, the Government stated that it applied the provisions of the Public Order Act in a fair but firm manner to ensure that all citizens enjoyed their rights. In addition, to ensure that the rule of law was maintained, those who infringed on the rights of others were made to answer to the relevant provisions of the law. Further, the Public Order Act was undergoing review to make it adequately respond to new and emerging issues.

Committee's Observation and Recommendation

The Committee in noting the submission urges the Executive to ensure that the Public Order Act is expeditiously reviewed to make it adequately respond to new and emerging issues. The Committee resolves to await a progress report on the matter.

7.1.7 Weak Media Bodies

The Committee in the previous Session, had acknowledged that media bodies were critical influencers of press freedom, media law and policy reforms. However, there was no institution to monitor their activities and operations. In addition, the Committee noted with concern that some media associations and unions were highly polarised making it difficult for them to unite and speak in unison as they campaign for press freedom and media law reforms, among others. As such, media associations had been infiltrated by politicians making them weak. This had also made it difficult for them to agree on any proposed media reform that would benefit the media industry.

In this regard, the Committee had recommended that new media bodies should be put in place to strengthen the ongoing advocacy and campaign for media law reforms to strengthen the media environment. Further, the Committee had recommended that the Ministry of Information and Media puts in place a mechanism that would monitor what was happening in associations in order to strengthen the media industry.

Executive's Response
The Executive in the Action-Taken Report stated that calling media bodies weak was actually an understatement because, if the media bodies were weak, there would have been no need to regulate them. The correct position was that media bodies were very active and, therefore, the need for their regulation as recommended by the Committee. The Ministry of Information and Media was keenly studying this matter to find a lasting solution to it.

Committee's Observation and Recommendation
The Committee in noting the submission urges the Executive to ensure that a lasting solution is attained to enable the regulation of the media bodies without further delay. The Committee resolves to await a progress report on the matter.

7.1.8 Tax Exemption on Newsprint and Broadcasting Equipment

In the previous Session, the Committee had recommended that the Executive should consider waving tax on imported broadcasting equipment such as computers, cameras, recorders and newsprint.

Executive's Response
In the Action-Taken Report, the Executive informed the Committee that the Ministry of Finance and National Planning and other key stakeholders such as Zambia Revenue Authority, Ministry of Commence Trade and Industry, Ministry of Agriculture, Zambia Development Agency among others were conducting Tax Policy Review Committee (TPRC) meetings. The objective of the meeting was to review the tax and non-tax proposals for consideration under the 2023 National Budget. Therefore, the recommendation by the Committee on Media, Information and Communication Technologies to consider waving tax on imported broadcasting equipment such as computers, cameras, recorders and newsprint had been noted and would be duly forwarded to the TPRC Committee for consideration.

Committee's Observation and Recommendation
In noting the submission, the Committee resolves to await a progress report on the waving of tax on imported broadcasting equipment such as computers, cameras recorders and newsprint.

7.1.9 Poor Conditions of Service

In the previous Session, the Committee had observed that poor conditions of service contributed to the unprofessional conduct by some journalists because they sometimes depended on their sources of news to meet their logistical requirements during an assignment.

In this regard, the Committee had recommended that the Executive should put in place a minimum wage for journalists in order to help reduce on the unprofessional conduct exhibited by some journalists.

Executive's Response

The Executive in its response informed the Committee that the Ministry of Information and Media was keenly and closely collaborating with the Ministry of Labour and Social Security to find the best way to address this matter.

Committee's Observation and Recommendation

The Committee in noting the submission urges the Executive to ensure that the matter is urgently addressed and resolves to await a progress report on the matter.

7.1.10 Zambia News and Information Service

The Committee in the previous Session had noted with great concern that the Zambia News and Information Service (ZANIS) offices in all the districts visited were poorly funded and sometimes went for almost a year without receiving the Government grant. Furthermore, the offices had inadequate transport, staff, office furniture, computers, cameras, generators and lacked modern public address systems and internet facilities to enable them operate effectively.

In this regard, the Committee had recommended that the Executive should ensure that ZANIS offices were adequately funded and all operational requirements put in place for the offices to function effectively.

Executive's Response

The Committee was informed that the Treasury had been consistently releasing funds as profiled by all Ministries, Provinces and Spending Agencies (MPSA's). These releases included the Ministry of Information and Media under which ZNBC and ZANIS fall. The Committee was further informed that the Ministry of Information and Media receive monthly profiles from the Treasury in line with their institutional priority areas. In this regard, the Ministry is funded by the Treasury according to their profiles and was expected to carter for the Institutions under it which included ZNBC and ZANIS among others.

Committee's Observation and Recommendation

In noting the submission, the Committee urges the Ministry of Information and Media to prioritise the funding to ZANIS so as to enable it operate effectively. The Committee resolves to await a progress report on the matter.

CONSIDERATION OF THE ACTION-TAKEN REPORT ON THE REPORT OF THE COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES FOR THE FIFTH SESSION OF THE TWELFTH NATIONAL ASSEMBLY

7.2 INVESTIGATIVE JOURNALISM IN ZAMBIA

7.2.1 Access to Information Legislation

In the previous Session, the Executive stated that the Government Communication Policy was approved and launched in 2020 and would give guidance to the information flow. Therefore, the Access to Information Bill was being processed accordingly. In noting the submission, the Committee had resolved to await a progress report on the finalisation of the Access to Information Bill.

Executive's Response

The Executive in response to the Committee submitted that the process towards the enactment of the Access to Information Bill into law had reached an advanced stage and was projected to be presented to Parliament in the first quarter of 2023 for enactment.

Committee's Observations and Recommendations

The Committee in noting the submission urges the Executive to ensure that the Access to Information Bill is presented to Parliament in the first quarter of 2023 and resolves to await a progress report on the matter.

7.2.2 Legal Impediments

In the previous Session, the Committee was informed that the Ministry of Justice was in the process of drafting a Bill that sought to set up a professional body of journalists. The Bill further sought to set journalism standards and address issues related to self-censoring. In noting the submission, the Committee had resolved to await a progress report on the formulation of the Bill which would set journalism standards and also address issues relating to self-censoring.

Executive's Response

The Executive in its response to the Committee stated that the process to enact the Zambia Media Council (ZAMEC) Law that was aimed at regulating the conduct of journalists had advanced. To that effect, the Committee was informed that the Zambia Media Council Bill was projected to be presented to Parliament in the first quarter of 2023 for enactment into Law.

Committee's Observations and Recommendations

In noting the submission, the Committee urges the Executive to ensure that the Zambia Media Council (ZAMEC) Bill is presented to Parliament in the first quarter of 2023 as submitted and resolves to await a progress report on the matter.

7.2.3 Training

In noting the submission, the previous Committee had resolved to await a progress report on the proposal to put in place a dedicated investigative reporting curriculum to be implemented at certificate, diploma and degree levels, so that there was an appreciation of the importance of investigative journalism by students. Journalism trainers should also be adequately capacitated to enable them provide training in investigative reporting.

Executive's Response

The Executive in its response to the Committee stated that one of the measures in the Media Development Policy targeted at developing the media industry was collaboration with institutions of higher learning (both public and private) and one of the aspects in that planned collaboration was the inclusion of modern media-related courses in these institutions of higher learning curricular.

Committee's Observations and Recommendations

The Committee in noting the submission urges the Executive to ensure that the inclusion of investigative reporting and modern media related courses where included in higher learning institutions and resolves to await a progress report on the matter.

7.2.4 Media Ownership

The previous Committee in noting the submission had resolved to await a progress report on the establishment of a journalism professional body that would protect journalists from the influence by media owners.

Executive's Response

In response, the Executive informed the Committee that the process to enact the Zambia Media Council (ZAMEC) Law that was aimed at regulating the conduct of journalists had advanced. To that effect, the Committee was informed that the ZAMEC Bill was projected to be presented to Parliament in the first quarter of 2023 for enactment into Law.

Committee's Observations and Recommendations

The Committee in noting the submission urges the Executive to ensure that the establishment of a journalism professional body that would protect journalists from the influence by media owners should be expedited and resolves to await a progress report on the matter.

7.2.5 Lack of a Minimum Qualification

The previous Committee had noted that the establishment of the Zambia Media Council would address concerns relating to qualifications in the journalism profession. The Committee had resolved to await a progress report on the matter.

Executive's Response

In response to the Committee, the Executive submitted that the process to enact the Zambia Media Council (ZAMEC) Law aimed at regulating the conduct of journalists had advanced. To this effect, the Committee was informed that the ZAMEC Bill was projected to be presented to Parliament in the first quarter of 2023 for enactment into Law. Ordinarily, the enactment of the ZAMEC Law was meant to provide for establishment for an institution that would be responsible for regulating the journalists. Therefore, as soon as the ZAMEC Bill was enacted into Law, the process for the establishment of the said institution would commence.

Committee's Observations and Recommendations

The Committee in noting the submission urges the Executive to ensure that the ZAMEC Bill is presented to Parliament in the first quarter of 2023 as submitted to facilitate the establishment of the Zambia Media Council aimed at regulating the conduct of journalists. The Committee resolves to await a progress report on the matter.

CONSIDERATION OF THE ACTION-TAKEN REPORT ON THE REPORT OF THE COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES FOR THE FOURTH SESSION OF THE TWELFTH NATIONAL ASSEMBLY

7.3 IMPLEMENTATION OF ELECTRONIC GOVERNMENT IN ZAMBIA

While acknowledging the strides that the Government was making to successfully implement the e-Government programme, the Committee made observations and recommendations as set out below.

7.3.1 Inadequate Policy

The previous Committee had resolved to await a progress report on the review and implementation of the 2006 Information and Communication Technology Policy.

Executive's Response

In its update to the Committee, the Executive submitted that the 2006 Information and Communication Technology Policy had undergone revision and was awaiting clearance by Cabinet Office before being tabled in Cabinet for approval. This approval was expected before the end of the year 2022.

Committee's Observations and Recommendations

The Committee in noting the progress urges the Executive to ensure that clearance of the revised 2006 ICT Policy by Cabinet Office is expedited. The Committee resolves to await a progress report on the matter.

7.3.2 Inadequate Infrastructure

The Committee in the previous Session had resolved to await a progress report on the completion of the construction of communication towers under the phase II project.

Executive's Response

In its update to the Committee, the Executive submitted that the construction of the communication towers project was ongoing with 958 towers functional and on air compared to 789 that were operational in the previous update. The Committee was further informed that the delay in the completion had been affected by lack of resources.

Committee's Observations and Recommendations

In noting the submission, the Committee urges the Executive to ensure that resources are mobilised to facilitate the completion of the construction of communication towers under phase II. The Committee resolves to await a progress report on the matter.

7.3.3 Reliance on Foreign Information and Communications Technology Solutions

The previous Committee in noting the submission, had resolved to await a progress report on the matter as the Government in collaboration with the Copperbelt University (CBU) intended to establish a Cyber City which would not only promote growth and development of the ICT sector but also create employment opportunities and provide work experience for many youths and graduates in the country.

Executive's Response

In its update to the Committee, the Executive submitted that the establishment of the Cyber City was a long-term commitment and as such, required careful assessment of the fiscal budgetary implications and consideration of contingent liabilities. In this regard, the Ministry of Technology and Science was leading engagements with Copperbelt University in regard to the establishment of the Zambia Cyber City. Further, the SMART Zambia Institute and the Copperbelt University had an active Memorandum of Understanding aimed at collaborating on the development of digital initiative/solutions in the Public Sector.

The Committee was further informed that interventions had been taken to build digital capacities as drivers of digital transformation through the free online CISCO NetaCad Programme. This was a free online training initiative aimed at bridging the digital divide and training the youths of ICT Industry Certification with partnership and support from

International Telecommunications Union (ITU). The ultimate intention was to impart relevant skills in the local ICT industry to produce relevant local ICT solutions to resolve and bring about efficiency in the Public Service. The SZI was in the process of implementing a Regulatory SANDBOX solution that was expected to incubate especially local ICT solutions and innovations in the Public Service.

The SMART Zambia Institute was engaging key stakeholder with the aim of developing a framework for preferential procurement of ICT solutions from local vendors to support the enhancement of local capacities as well as ensure that cost-effective solutions were implemented.

Committee's Observations and Recommendations

The Committee in noting the submission resolves to await a progress report on the establishment of the Cyber City in Zambia.

7.3.4 Communication Barrier

The previous Committee in noting the submission had resolved to await a progress report on the provision of information in the seven major local languages on Government websites.

Executive's Response

The Committee was informed that the Government through the SMART Zambia Institute was desirous to ensure that Public Bodies provide meaningful access to online public services to people with limitation in English proficiency on different Government Online Platforms including websites. This would require that the Institute collaborates with Public Bodies that have expertise to formulate appropriate, relevant and accurate written translations in order to standardise terminologies in the local languages.

Government is cognisant of the fact that this implementation would require Human Capital Development within the Ministries and Spending Agencies (MPSAs) to ensure that capacity was built to enable them translate content for their websites.

Priority content which include legislation, key policy documents forms and some of the other most visited web pages on Government Official websites will be prioritised for translation. SZI will also leverage the expertise at the Zambia National Broadcasting Corporation and ZANIS to translate content on Government sites. This exercise would require resources to be fully attained.

Committee's Observations and Recommendations

The Committee in noting the submission urges the Executive to ensure that funds are mobilised to facilitate the translation of content on Government sites without further delay. The Committee resolves to await a progress report on the matter.

CONSIDERATION OF THE ACTION-TAKEN REPORT OF THE COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES FOR THE SECOND SESSION OF THE TWELFTH NATIONAL ASSEMBLY

7.4 REVIEW OF THE INFORMATION AND MEDIA POLICY IN ZAMBIA

Arising from its interactions with various stakeholders both during the long meetings and local tour, the Committee made observations and recommendations as outlined below.

7.4.1 Top Star Operations not in line with the Digital Migration Policy

The previous Committee in noting the submission had resolved to await a progress report on the review of the Digital Migration Policy.

Executive's Response

The Executive in its update to the Committee submitted that the Digital Migration Policy had not yet been reviewed. However, the issue of Top Star Telecommunication Company Limited's dealings in both signal distribution and content provision, which was contravening the Digital Migration Policy was being addressed by hiving out the landing and provision of content from the business of Top Star Telecommunication Company Limited so that it was done by a Content Company. To that effect, the process of creating the said Content Company had commenced.

Committee's Observations and Recommendations

The Committee in noting the submission observes with concern the delay by the Executive to review the Digital Migration Policy. In this regard, the Committee resolves to await a comprehensive progress report on the review of the Digital Migration Policy.

CONSIDERATION OF THE ACTION-TAKEN REPORT ON THE REPORT OF THE COMMITTEE ON MEDIA, INFORMATION AND COMMUNICATION TECHNOLOGIES FOR THE FIRST SESSION OF THE TWELFTH NATIONAL ASSEMBLY

7.5 NATIONAL FILM POLICY

Arising from its interactions with various stakeholders both during the long meetings and local tour, the Committee made observations and recommendations as outlined below.

7.5.1 Creation of Faculties and Film Production at Higher Learning Institutions

The previous Committee had noted that the response by the Executive was unrelated to the matter under consideration, which was the construction of the University College of Governance and Arts in Katete District. The Committee therefore, had resolved to await a progress report on the matter.

Executive's Response

The Executive in its response to the Committee submitted that the Executive, through the Ministry of Finance, working with the Ministry of Education, signed Loan Agreements with the Arab Bank for Economic Development in Africa (BADEA); Kuwait Funds for Arab Economic Development; OPEC Fund for International Development and Abu Dhabi, for the construction of three University College in Zambia. The projects were scheduled to begin in 2011 under the then Ministry of Education. The three University colleges were:

i. The University College of Science and Mathematics in Nalolo;
ii. The University College of Applied Arts and Commerce in Katete; and
iii. The University College of Science and Technology in Kabompo.

Project Description

The project involved the construction, equipping and furnishing of three new colleges under university education.

Funding Agencies
The Partners to finance the project with the following amounts were:

1. Abu Dhabi Fund for Development. The Fund would lend the Government an amount equivalent to US $10 Million at one and a half per cent per annum.
2. Arab Bank for Economic Development in Africa (BADEA).
   The Loan amounting to US$5,400,000 was signed on 17 December 2012.
3. Oil Producing and Exporting Countries (OPEC).
   The Loan amounting to US$10,000,000 was signed on 19 August 2013.
4. Kuwait Fund for Arab Economic Development.
   The agency pledged a Loan amounting to the US $13,266,998.34.

To commence the implementation of the project, the Ministry engaged the traditional leadership in the respective districts where the University Colleges were to be constructed, and the land was allocated in the respective Districts. The Ministry also undertook Environmental Impact Assessment Studies at each site to prepare for construction.

However, because of the country's unsustainable debt position, the Ministry of Finance guided that all Projects that were to be implemented under loan support and had not commenced be suspended. In this regard, the projects above were suspended in collaboration with the Ministry of Finance.

Committee's Observations and Recommendations
The Committee in noting the submission resolves to await a progress report on the matter.

7.5.2 Lack of Proper Documentation of Cultural Ceremonies

The previous Committee in noting the submission had resolved to await a progress report on the completion of the provincial broadcasting studios so as to ensure that all traditional ceremonies were documented. The Committee further wanted to know when works on the Solwezi and Choma broadcasting studios would commence.

Executive's Response
The Executive in its update to the Committee submitted that the status of the Construction of the Provincial Broadcasting Studios was such that the Broadcasting Studios for Northern Province in Kasama, Muchinga Province in Chinsali and Luapula Province in Mansa respectively were 100 per cent complete whereas the Broadcasting Studios for Central Province in Kabwe, Eastern Province in Chipata and Western Province in Mongu were at 80 per cent, 82 per cent and 83 per cent complete respectively. The Broadcasting Studios for Southern Province in Choma and North Western Province in Solwezi respectively were both at slab level.

Committee's Observations and Recommendations
The Committee in noting the submission by the Executive observes with concern the inordinate time it has taken for the Broadcasting Studios to be completed. The Committee therefore, urges the Executive to expedite the construction of Broadcasting Studios to facilitate for the documentation of the traditional ceremonies.

7.5.3 Zambia Consolidated Copper Mines Infrastructure

The previous Committee in noting the submission had resolved to await a progress report on the rehabilitation of the Luanshya Theatre Hall.

Executive's Response
The Executive in its update to the Committee submitted that Luanshya Copper mine in consultation with the Committee at RADOS Little Theatre agreed that the rehabilitation works be undertaken in three phases.

The Committee was informed that first Phase had been undertaken and completed at a total cost of K205,731.44. The works were undertaken between April and August 2021. The second phase of the rehabilitation works was anticipated to be undertaken in the first quarter of 2023.

Committee's Observations and Recommendations
The Committee in noting the submission urges the Executive to ensure that the rehabilitation of the Luanshya Theatre Hall commences in the first quarter of 2023 as submitted and resolves to await a progress report on the matter.

CONSIDERATION OF OUTSTANDING ISSUES FROM THE ACTION-TAKEN REPORT ON THE COMMITTEE'S REPORT FOR THE FOURTH SESSION OF THE ELEVENTH NATIONAL ASSEMBLY

7.6 COMMUNITY RADIO STATIONS IN ZAMBIA

Arising from its interactions with various stakeholders both during the long meetings and local tour, the Committee made observations and recommendations as outlined below.

7.6.1 Independent Broadcasting Authority Mandate
The previous Committee in noting the submission had resolved to await a progress report on the repeal of the IBA Act which would address issues of online broadcasting and community radio stations.

Executive's Response
The Executive in its update to the Committee submitted that due to the lengthy process of consultations, the IBA Act had not yet been repealed and replaced. However, the Committee was informed that a Bill to repeal and replace the Act would be presented to Parliament in the first quarter of 2023 and it was projected that before the end of the said quarter, the IBA Act would have been repealed and replaced.

Committee's Observations and Recommendations
The Committee in noting the submission urges the Executive to ensure that the bill to repeal and replace the IBA Act is brought to Parliament within the first quarter of 2023, so that issues to do with online broadcasting and community radio stations are addressed. The Committee resolves to await progress report on the matter.

CONSIDERATION OF THE ACTION-TAKEN REPORT ON THE COMMITTEE'S REPORT FOR THE SECOND SESSION OF THE ELEVENTH NATIONAL ASSEMBLY

7.7 SOUTHERN AFRICAN DEVELOPMENT COMMUNITY REGIONAL DIGITAL SWITCHOVER

Arising from its interactions with various stakeholders both during the long meetings and local tour, the Committee made observations and recommendations as outlined below.

7.7.1 Regulation to Manage Electronic Waste

The previous Committee had resolved to await a progress report on the construction of the landfill in Kabwe, which would have a component for disposal of hazardous waste, including e-waste.

Executive's Response

It was reported through the Action-Taken Report that that Kabwe Municipal Council had managed to secure land for the development of the landfill. The land measured approximately 20 hectares and was located in the excised Mpima Forest. The plan for the landfill had a provision for a component for disposal of hazardous waste as well as E-waste. However, the local authority was unable to proceed in developing the landfill due to lack of financing. The local authority was engaging different cooperating partners in the hope of securing funding.

Committee's Observations and Recommendations

The Committee notes with concern the inordinate time it has taken the Executive to construct a landfill in Kabwe and urges it to urgently secure funds for the construction of the landfill without further delay. The Committee resolves to await a progress report on the matter.

8.0 CONCLUSION

In dealing with the fight against cybercrimes, ZICTA draws its mandate from the *Cyber Security and Cyber Crimes Act, No. 2 of 2021.* ZICTA's involvement in the fight against cybercrimes has yielded some positive results so far but more still needs to be done for the Authority to effectively discharge its mandate. Critical Information Infrastructure in different sectors is beyond ZICTA's mandate and there are no sector specific Computer Incident Response Teams to enhance the detection of cyber threats and cyber incidences. It is, therefore, the view of the Committee that the *Cyber Security and Cyber Crimes Act, 2021* and the proposed guidelines relating to Critical Information Infrastructure be reviewed to keep at pace with the ever-evolving technology sector and ensure that the Authority is able to address cyber threats.

In view of the fact that Zambia is rapidly undergoing digital transformation, it is important to be prepared at both institutional and human resource level to avert any cyber attacks. It is also imperative for collaborative measures to be enhanced among stakeholders to improve legislation, strengthen institutions and increase funding towards supporting cybercrime detection and prevention.

Eng. Raphael Samukoma Mabenga, MP
CHAIRPERSON

June, 2023
LUSAKA

APPENDIX I – List of the National Assembly Officials

Mr Francis Nabulyato, Principal Clerk of Committees (SC)
Mrs Chitalu K Mumba, Deputy Principal Clerk of Committees (SC)
Mrs Angela M Banda, Senior Committee Clerk (SC)
Mrs Media H Mweele, Committee Clerk
Mr Leon J N Haangala, Acting Committee Clerk
Mrs Rachael M Kanyumbu, Typist
Mr Daniel Lupiya, Committee Assistant
Mr Muyembi Kantumoya, Parliamentary Messenger
Ruth Phiri Horemans, Intern

APPENDIX II – List of Witnesses

Anti Corruption Commission
Bank of Zambia
Bankers Association of Zambia
Copperbelt University
Drug Enforcement Commission
Financial Intelligence Centre
Information and Communications Technology Association of Zambia
INFRATEL
Law Association of Zambia
Ministry of Defence
Ministry of Home Affairs and Internal Security
Ministry of Information and Media
Ministry of Justice
Ministry of Science and Technology
MTN Zambia Ltd
Road Transport and Safety Agency
Smart Zambia Institute
University of Zambia
Zambia Information and Communications Technology Authority
Zambia Police Service
Zambia Revenue Authority
Zambia Telecommunications Company Limited