INFORMATION BRIEF ON CYBER SECURITY AND CYBERCRIME TRENDS IN ZAMBIA

Research Department, September, 2022

What is cyber security and cyber crime?

Cyber security is the practice of protecting critical systems and sensitive information from digital attacks[1] whereas cyber crime refers to illegal acts which involve the use of Information and Communication Technologies (ICTs)[1] to commit crimes such as financial fraud, extortion, violating privacy or intellectual property.

Zambia's status on cyber security

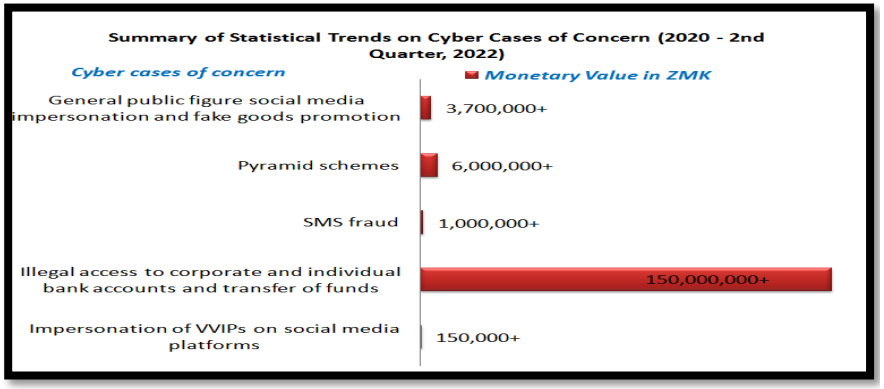
Zambia's rating on cyber security is moderately impressive. The International Telecommunication Union (ITU) and Global Cyber security Index (GCI) that measures the commitment of countries to cyber security in 2020 rated Zambia's progression at 68.88 per cent from 14.7 per cent in 2014[1]. To further improve Zambia's global rating, capacity over CII and intelligence sharing. The would cost K66.76 million to implement.

Cyber crime Trends in Zambia

From January - December, 2021, the Zambia Computer Incidence Response Team (ZM-CIRT) recorded a cumulative number of attacks amounting to 10,718,002. The cyber threats recorded in 2021 included: mobile money reversal scams, social media account hijacking and fake online product promotions and investment schemes.

Figure 1: Summary of Statistical Trends on Cyber Cases of Concern (2020-2nd Quarter, 2022)

The figure highlights cyber cases of concern and corresponding financial losses. The financial sector suffered losses in excess of K150 million and over K6 Million was lost due to Pyramid schemes otherwise known as fake financial investments.



Source: *Constructed from Statistical Trends on Cyber Cases of Concern by Zambia Information and Communications Technology Authority (ZICTA)*

Impact of cyber crime

i. Loss of money, valuable personal or company data and sometimes reputation damage; and

ii. severe financial disruption and loss of productivity.

The Legal and Policy framework

i. ***Cyber Security and Cyber Crimes Act, No.2 of 2021*** which provides for cyber security including protecting persons and Critical Information Infrastructure (CII) against cyber crime.

ii. ***The Electronic Communications and Transactions Act No.4 of 2021*** which provides a safe and effective environment for electronic transactions.

iii. ***The Data Protection Act No. 3 of 2021*** which provides an effective system for the protection and regulation of personal data.

iv. ***The National Cyber Security Policy of 2021*** whose overall objective is to transform the cyberspace into a safer environment in order to fully realise the social and economic benefits of ICTs.

Challenges in dealing with the threat of Cyber crimes

absence of key national level security infrastructure such as a Centralised Monitoring Facility to enhance visibility

i. Lack of a National Public Key Infrastructure (NPKI) and Root Certification Authority (RootCA) whose installation is estimated at K123.8 million.

ii. financial constraints to heighten consumer education and awareness regarding the trends and prevention of cyber crimes.

iii. increased forgery of National Registration Identity Cards and fraudulently registered SIM cards used in the registration of telecommunication and banking services.

The role of Parliamentarians

Parliamentarians are obliged to consider some of the following interventions:

i. scrutinising the legal and policy frameworks on cyber crimes to adapt them to potential cyber threats and also ensure they conform to international agreements and treaties which Zambia is a Party. This includes undertaking period reviews on delegated legislation on cyber crimes with due consideration for human rights and other emerging issues;

ii. appropriating adequate public finances for the installation of CII and undertaking essential programmes aimed at mitigating cyber crimes; and

iii. supporting the dissemination of cyber security information and best practices of mitigating cyber crimes in their constituencies.