Chapter 66
Cybercrime as a Threat to Zimbabwe's Peace and Security

Jeffrey Kurebwa
https://orcid.org/0000-0002-8371-8055
Bindura University of Science Education, Zimbabwe

Jacqueline Rumbidzai Tanhara
Chinhoyi University of Technology, Zimbabwe

ABSTRACT

The purpose of this study was to understand the effects of cybercrime to Zimbabwe's peace and security. In the 21st century, cybercrime has become an international threat. This has necessitated many states to enact legislation and other measures to curb cybercrime. Primary data was gathered through key informant interviews, while documentary search was used to review scholarly literature on the subject. Key informants for the study were drawn from institutions that deal in combating cybercrime. Zimbabwe does not have adequate and effective legislative instruments to combat cybercrime. Cybercrime is a threat to peace and security as it can be used to bring down critical infrastructure and disrupt communication networks of the country. Some of the measures identified to curbing cybercrime include prevention and awareness, training and development, development of new technology and introduction of new laws, and updating of current and introduction of new legislations.

INTRODUCTION

The 21st century has witnessed a rise in the use of Information Communication Technologies (ICTs). Globally the cost of cybercrime is expected to annually from US$2 trillion in 2019 to US$6 trillion in 2021. Cybercrime is expected to grow as a lucrative industry for criminals. Between 2017 and 2021, countries are expected to spend in excess of US$1 trillion on cyber security (The Herald, 2017). The phenomenal growth in internet use has been linked to factors such as the liberalization of the telecommunications market in Africa, widespread availability of mobile technologies, and the increasing availability of broadband systems.

DOI: 10.4018/978-1-7998-2466-4.ch066

The Global Risks Report (2016) indicated that a significant portion of cybercrime goes undetected. This is particularly true in the case of industrial espionage and the heist of proprietary secrets given that illicit access to sensitive or confidential documents and data is hard to detect. Cyber space vulnerabilities have increased. Cybercrime is now ranked top of the International agenda as high-profile breaches have raised fears that hack attacks and other security failures could endanger economies (Mutisi, 2017). Kizza (2013) highlighted that the spread of ICTs and internet penetration in Africa has raised concerns about cyber security at regional and sub-regional governance forums.

Most African intergovernmental organizations and regional groupings have developed legal frameworks for cyber security (Manarcoda, 2012). The attack on the United States of America on September 11, 2001 provided the impetus for many Western countries to introduce anti-terrorist legislations. These anti-terrorist legislations focuses on criminalising cyber terrorist activities, impose penalties proportional to the act, prevent cyber terrorist activities and mitigating its impact by denying cyber terrorists material and financial support. Zimbabwe as a country has not been spared of cyber crime.

Cyber crime is listed as one of the crimes contributing to the US$1.8 billion estimated illicit proceeds generated from criminal activities annually (National Risk Assessment Report, 2015). The most common types of cyber crime in Zimbabwe include phishing, credit card fraud, identity theft, unauthorised access, hacking, and telecommunications piracy. This study sought to understand the effects of cybercrime on Zimbabwe's peace and security.

Research Objectives

1. To understand the effects of cyber crime to Zimbabwe's peace and security.
2. To examine the effectiveness of the legal frameworks in combating cyber crime.
3. To provide recommendations in curbing cyber crime.

RESEARCH METHODOLOGY

The study used the qualitative research methodology in order to understand and explain cybercrime as a threat to peace and security and Zimbabwe. Priest (1996) contends that when the researcher's goal is to understand people, the social and cultural context in which they live, there is need to use qualitative research methods. This is because it is a holistic and inductive approach which will provide the opportunity to develop a descriptive, rich understanding and insight into the individual's or subject's belief's concerns, motivations and aspirations, lifestyles, cultures and preferences.

Qualitative research also gives room for flexibility hence allows greater spontaneity and adaptation of the interaction between researcher and participants. Data was collected using ten key informants. These were drawn from the Ministry of Information, Communication and Technology, Zimbabwe Republic Police (ZRP), Internet Services Providers, Postal and Telecommunications Regulatory Authority of Zimbabwe, and academics. This study also involved a comprehensive desk study aimed at collecting secondary data from various sources such as peer reviewed journal articles, research reports, policy documents, strategic plans, and newspapers.