CSCanada
Canadian Social Science
Vol. 16, No. 12, 2020, pp. 1-10
DOI:10.3968/11946

ISSN 1712-8056[Print]
ISSN 1923-6697[Online]
www.cscanada.net
www.cscanada.org

Multilateral Responses to Cybercrimes in the SADC Region: The Case of Zimbabwe and South Africa

Muzariri Jenalda[a]; Jeffrey Kurebwa[a],*

[a] Department of Peace and Governance, Bindura University of Science Education, Zimbabwe.
*Corresponding author.

Received 23 September 2020; accepted 19 November 2020
Published online 26 December 2020

Abstract

This study sought to understand the multilateral responses to cyber crimes in the SADC region with specific reference to Zimbabwe and South Africa. The research examined the concept of cybercrimes, its causes, motivations, and implications. The research further examined mechanisms and legislative frameworks available to curb cybercrimes. The qualitative research methodologies were used for the study. Data was purposively collected from information technology experts, academia, the security sector, lawyers, law enforcement agencies, journalists, and diplomats. The key findings of the research revealed that the understanding of cybercrimes is not consistent as the term has no specific referent in law. The study deduced that although cyber espionage, extortion, fame and entertainment are some of the motivations behind cybercrimes in the SADC region are attributed to high unemployment rates, especially among educated ICT graduates and poverty in general. The study also established that SADC countries lack a comprehensive legal framework to combat cyber crimes.

Key words: Cybercrime; Multilateral responses; SADC; Cyber terrorism; Zimbabwe; South Africa; Cyber security; Security threats; ICT; Computer fraud

Jenalda, M., & Kurebwa, J. (2020). Multilateral Responses to Cybercrimes in the SADC Region: The Case of Zimbabwe and South Africa. *Canadian Social Science, 16*(12), 1-10. Available from: http://www.cscanada.net/index.php/css/article/view/11946
DOI: http://dx.doi.org/10.3968/11946

1. INTRODUCTION

Cybercrime has become one of the most interesting fields of International Relations scholarship (Valeriano & Maness, 2018). Ebert and Maurer (2017) opine that the Internet has expanded rapidly since its commercialization in the mid-1990s. In the early 21st century, a third of the world's population had access to the technology, with another 1.5 billion expected to gain access by 2020. Moreover, the "Internet of Things" will lead to an exponential number of devices being connected to the network. As a result, the economic and political incentives to exploit the network for malicious purposes have also increased, and cyber security has reached head-of-state-level attention.

Gala (2017) also argued that cybercrimes have once or twice strained sensitive relations between states. Russian hacking of the Democratic National Committee during the 2016 US Presidential Election is no exception. Secret emails were published, and relationships between nations were strained. This incident has elevated cyber security in the context of international affairs to an unprecedented level in the public's consciousness, not only in the United States but around the world. According to Norse Security (2018) the U.S. receives over 5,000 cyber attacks an hour, with most originating from China. This outpouring in attacks from the Far East has become a big point of contention between the White House and Beijing (Gabe Duverge Intelligence, 2015). The reality is that the scope of Chinese attacks on American targets is massive. In 2010, Google was among the first to report that Chinese hackers were targeting attacks on its cyber infrastructure. Since then, several companies have reported attacks, including Northrop Grumman, Symantec, Yahoo, Dow Chemical, and Adobe Systems. These attacks are focused on both military and commercial interests and tend to focus on sectors in which the Chinese lag behind the US. Increased usage of modern information and communication technologies (ICTs) in the Southern

African Development Community (SADC) has also made cybercrime a growing crime problem in the region. In Zimbabwe towards the 2018 elections, Zimbabwe Electoral Commission (ZEC) chairperson Justice Priscilla Chigumba admitted that suspected hackers broke into the electoral management body's database and stole crucial information on the biometric voters' roll, the hackers cloned the Commission's domain, which hosted the voters' roll complete with phone numbers and splashed the data on the internet escalating fears of electoral manipulation ahead of the polls which she alleged was a serious cyber security breach (Newsday July 19 2018).

Orji (2015) argues that Africa in general has witnessed a phenomenal growth in Internet penetration and the use of Information Communications Technologies (ICTs), he adds that the spread of ICTs and Internet penetration has also raised concerns about cyber security at regional and sub-regional governance forums. This has led African intergovernmental organizations to develop legal frameworks for cyber security. At the sub-regional level, the Economic Community of West African States (ECOWAS) adopted a Directive on Cybercrime, in contrast the Common Market for Eastern and Southern Africa (COMESA) and the Southern African Development Community (SADC) have come up with model laws. At the regional level, the African Union (AU) has adopted a Convention on Cyber Security and Personal Data Protection. This research seeks to examine these legal instruments with a view to determining whether they provide adequate frameworks for mutual assistance and international cooperation on cybercrime control. This study sought to understand multilateral responses to cyber-crime in the SADC region

2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

This section presents The Routine Activity Theory, as the theory underpinning this study. The Routine Activity Theory connects a range of criminological theories (Cohen and Felson, 2003). Though Ekblom & Tilley (2015) are the first to emphasize on exploring the theoretical significance of the offender concept, it was Cohen and Felson (1979) that originally recognized the role of offender's abilities in their routine activity theory as they refer to the use of tools and appropriate skills that make possible for the offender to engage in crime.

Accordingly Ekblom & Tilley (2000) drew attention to the significant resources can play in the offending process and criminal opportunity. From their view, an offender would need to be resourced, or supplied with the necessary means, in order to realise a crime. Largely based on the routine activity theory of Cohen & Felson (1979), which states that crimes are ultimately committed when the opportunity arises, the resourceful offender would also need to have the ability, know-how and tools to carry out a crime successfully. In some situations, collaboration with co-offenders is necessary. The basic tenet of the theory establishes that a crime occurs, or is very likely to happen, when a motivated offender being adequately resourced and a potential victim converge in the same area at the same time. Based on the view of offenders as rational thinking and hedonistic individuals, perpetrators are viewed as opportunistic deciding whether to engage in a crime by weighing-up the rewards and risks. This describes offenders that may simply seize the opportunities that are present. Other offenders, traditionally associated with organised crime, are more measured in devising or discovering new opportunities that require the exertion of effort or thoughtful planning. In such a case, opportunity is created where it did not exist previously. In either case it is therefore plausible that certain resources can potentially play a role in whether a crime is to occur and succeed. It will be later revealed in the findings of the research that convergence alone is insufficient to explain why cyber crime occurs, a key result with direct implications for crime prevention.

2.1 Definitions of Cyber Crime

The major challenge in the analysis of cybercrime is the absence of a consistent current definition, even amongst those law enforcement agencies charged with tackling it (NHTCU/NOP 2002: 3). As Wall (2001) notes, the term 'has no specific referent in law', yet it has come to enjoy considerable currency in political, criminal justice, media, public and academic discourse. Consequently, Wall argues that the term might best be seen to signify a range of illicit activities whose common denominator is the central role played by networks of information and communication technology (ICT) in their commission.

Thomas & Loader (2000) conceptualize cybercrime as those computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. The specificity of cybercrime is therefore held to reside in the newly instituted interaction al environment in which it takes place, namely the 'virtual space' often dubbed 'cyberspace generated by the interconnection of computers into a worldwide network of information exchange, primarily the Internet (Castells, 2002: 177).

Poonia (2014) defines cybercrimes as "Unlawful acts wherein the computer is either a tool or target or both". He defines a Cyber criminal as a person who commits an illegal act with a guilty intention or commits a crime in context to cyber crime. A Cyber criminal can be motivated criminals, organised organized hackers, discontented employees, cyber terrorists. Poonia also highlighted that Cybercrime can include everything from non-delivery of goods or services and computer intrusions (hacking) to intellectual property rights abuses, economic espionage (theft of trade secrets), online extortion, international

money laundering, identity theft, and a growing list of other Internet-facilitated offences. Further, it is not easy to identify immediately about the crime method used, and to answer questions like where and when it was done. The anonymity of the Internet makes it an ideal channel and instrument for many organized criminal activities.

Halder & Jaishankar (2011) have provided a definition of cybercrime from a holistic perspective as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Blue tooth/SMS/MMS).

As proposed by Sussman & Heuston (1995), the term 'cybercrime' can best considered as a series of criminal acts, 'based on the material offence object and modus operandi that affect computer data or systems.' The U.S. Department of Justice (2019) defines cybercrime as any crime that uses or targets computer networks. The United Kingdom Association of Chief Police Officers (2018) classifies cybercrime as any crime facilitated or committed using networked computers telecommunications, or Internet technology.

The Council of Europe's Convention on Cybercrime (2019) delineates cybercrime as offences ranging from criminal activity against data to content to copyright infringement. However, the most widely adopted and accepted definition of cybercrime is: any crime committed using computers, computer networks, or hardware devices (Gordon & Ford, 2006).

2.2 Types of Cyber Crime

Furnell, Gordon & Ford (2006) classify cyber crime into two distinct groupings, namely those of a predominantly type I (also referred to as computer-focused) and type II (also referred to as computer-assisted) nature. Type I cyber crimes are almost entirely technological in nature. They are committed using computer-related and enabled technologies; they take place on computer-related and enabled platforms and rely primarily on computer-related and enabled technologies for their successful execution. Type II group of cybercrimes are said to be more deceptive as they are almost always people-related. Although these types of crimes are committed using computer-related and enabled platforms and take place on computer-related and enabled platforms, their success is dependent on human frailty, susceptibility, and potential errors in judgements include cyber stalking, cyber bullying, cyber harassment, child predation, extortion, and blackmail (Furnell, Gordon & Ford, 2006).

In the case of Type II cyber crimes the underlying crime or offence either predates the emergence of computers or could be committed without them. Distinguishing between the two types of cybercrimes will not always be possible, or precise. Not all cybercrimes will present themselves as being purely Type I or Type II in nature, they represent either end of a continuum.

2.3 Classification of Cybercrimes

Emigh (2004) studied that fighting cybercrime like any other crime requires three important elements namely: identification, classification and the actual deployment of effective counter-measures. Cybercrime has been clearly identified as a clear menace (Emigh, 2004) and fairly defined over the years (McCaskey, 2007).

However, the classification of cybercrime which is an important step to fighting it, has been grossly limited to whether these crimes are "computer-assisted" or "computer-focused" (Furnell, 2001), or simply by directly naming these crimes (Audit Commission, 1998). Only few, for example, Furnell (2001) attempted a classification based on a different view motivation. However, his "categorizations of hackers" only addressed a small subset of cybercrimes, and never the whole. It was based on the above classifications that Furnell (2001) posited a model in which cyber crimes at a high level were classified simply as "computer-assisted" and "computer-focused" crimes.

Based on the object of legal protection and the method used to commit the crime, the 2001 COE Convention on Cybercrime lays down four criteria to be used for classifying cybercrimes. The convention's section on substantive criminal law, lists them as follows: Offences against the confidentiality, integrity, and availability of computer data and systems; Computer-related offences; Content-related offences and offences related to infringements of copyright, and related rights.

These classifications of cybercrimes is also adopted and referenced within East Africa's draft EAC legal framework for cyber laws. Similarly, Article 29 of the African Union's Convention on Cyber Security and Personal Data Protection identifies four classifications of cybercrime, referred to in the Convention as offences specific to information and communication technologies:

- Attacks on computer systems;
- Computerised data breaches;
- Content related offences; and
- Offences relating to electronic message security measures

2.4 Categories of Cybercrimes

Having classified cybercrimes, this section delves into the categorization of these acts of cybercrime and their various forms and instances. According to Poonia (2014) there are, in general, four main categories of cybercrime that forms cyber criminal and activities may be categorised into.

2.4.1 Cybercrimes Against Persons

Poonia (2014) highlighted that this category of cyber crimes involves cyber criminal attacks, through computers

or computer networks, where the target of the attack is an identifiable individual or a group of persons. Examples of these crimes include insults, harassment, acts of a racist, and xenophobic nature, assault by threatening, through to cyber-defamation.

2.4.2 Cybercrimes Against Property

Poonia (2014) states that this category of cyber crimes are cyber-attacks that cyber criminals direct at the property belonging to a person and involve varying degrees of violation of, or, tampering with another's property. These cybercrimes are also known as crimes affecting the economy. They range from cyber-vandalism and cyber-squatting through to computer related fraud.

2.4.3 Cybercrimes Against Governments and/or Organisations

With this category of cybercrime, according to Poonia (2014) the attackers seek the critical information infrastructure and confidential military information of a country or the confidential mission-critical information that an organisation runs on. Crimes that make up this category are crimes such as cyber warfare, cyber espionage, industrial espionage, and cyber fraud.

2.4.4 Cyber Crimes Against Society

These unlawful acts of cybercrime are committed with the intention of causing harm to the broader society at large through using cyberspace to cause widespread harm, to disrupt societal balance and dis-harmonize the moral well being of society. These offences include: possession and exchange of child pornographic materials, sale of illegal articles, and illegal auctions on the internet and cyber terrorism. (Viswanathan, 2001)

2.5 Forms of Cybercrime

According to a COE Convention on Cyber crime report (2012) most of the cybercrime legislation developed and adopted by countries between the years 2000 and 2010 was based on the traditional principles of substantive cybercrime and as defined by the COE Convention on cyber crime. This cybercrime legislation commonly outlaws the following acts of cybercrime and regards them as offences:

a) Illegal access
b) Illegal interception
c) Data interference
d) System interference
e) Misuse of devices
f) Computer forgery
g) Computer fraud, and
h) Offences related to child pornography.

However, the Convention and subsequently the legislation that is based on it, does not address or cater for the new methods of cybercrimes that must be covered by criminal law, such as phishing, botnets, spam, identity theft, crime in social networks, internet of things, terrorist use of internet, and massive and coordinated cyber-attacks against information infrastructures.

2.6 Motivations and Causes of Cybercrimes

Li (2008) established that a study of cybercrime would not be complete without a cyber-criminal. To understand this calibre of criminal, it is essential to understand that, like many criminals who commit traditional crimes 'the production of crime requires the presence of both motivated offenders and suitable targets (individuals or their property), in the absence of effective guardians'. Successful combating and prevention of cybercrime relies heavily on understanding the profile and motivation of the perpetrator seeking to overcome cyber defences which is known as psychological incident handling .The intentions of digital culprits could be exceptionally broad and cover many different sorts of offences (Li, 2008). Although it is complex to unearth a motive under illegal cyber activities (Philip, 2002), abundant different studies and research have drawn wide-ranging conclusions on the classification of motives.

Jordan & Taylor (1998) outlined six common attitudes amongst hackers which are addiction, curiosity, thrill of information searches, and ability to access, peer recognition, and identifying security loopholes. Maiwald (2003) has concluded that hacker motivations had fell into three groups, including the quest for challenge, greed, and malicious intent or vandalism.

Kiger (2004) summarized the motivations of illegal cyber activities as money, entertainment, ego, cause, entrance to social groups, and status. Pipkin (2002) indicated that hackers might hack from a sense of intellectual motivation, such as educational experimentation, harmless fun, as a wake-up call; personally motivated, such as disgruntled employees, cyber-stalking; socially motivated, such as cyber-activism; politically motivated, such as cyber terrorism, cyber-warfare; financially motivated; and motivated by ego.

Kremen (1998) classified hackers into ten types with 'different sizes, flavours and colours,' including curious hacker, thrill seeker, the person who wants information about computers, and their flaws, power seeker, vandal, the person who steals industrial information, secrets and/or intellectual property, the person who steals money, the person who performs industrial espionage, terrorist, and international spy. Li established that, the motives of illegal cyber activities may differ in a manner that is outside the imagination.

If we articulate that various perpetrators have similar motives, we can also articulate that virtually each perpetrator has his or her own. Bequai (1983) summarized different kinds of motives that push the probable perpetrators to run the risk of committing illegal cyber activities (Li, 2008). Illegal cyber activities affect several scientific disciplines.

Poonie (2014) outlines the causes of cybercrimes such as for the sake of recognition; quick money; fight a cause one thinks he/she believes in; low marginal cost

of online activity due to global reach; limited chance of being caught by law, and enforcement agency is less; new opportunities to do legal acts using technical architecture; official investigation and criminal prosecution is rare; no concrete regulatory measures; lack of reporting and standards; difficulties in identification, and limited media coverage.

Van der Hulst & Neve (2008), based on a literature review, distinguish between three basic offender types associated with the different motivations such as young male criminals who hack for fun, curiosity, or peer respect; ideological hackers who are intelligent and eager to learn, some of whom are obsessive, antisocial, or have a minority complex; financially-motivated hackers, from various backgrounds.

Cybercrimes are also attributed to weak legislation and law enforcement. Most African economies are characterized by permissiveness of regulatory regimes that provide a fertile ground for cybercrime activities. According to a November 2016 report of the African Union Commission (AUC) and the cyber security firm Symantec, out of the 54 countries of Africa, 30 lacked specific legal provisions to fight cybercrime and deal with electronic evidence. Law enforcement officials in some countries do not take major actions against hackers attacking international websites. For instance, it was reported that government officials in Nigeria claimed that they were ignorant of cyber crimes originated from the country and some labelled it as Western propaganda. Some elected high-level State officials were also reportedly involved in cybercrimes. In 2003, Nigeria's Economic and Financial Crimes Commission (EFCC) arrested Maurice Ibekwe, a member of Nigeria's House of Representatives for his alleged engagement in cyber crime-related activities (Kshetri, 2013).

2.7 The Legal Framework in Combating Cybercrimes

Group of Eight (G8) is made up of the heads of state of eight industrialized countries: the U.S., the United Kingdom, Russia, France, Italy, Japan, Germany, and Canada (Felson, 2019). Felson also states that in 1997, the G8 released a Ministers' Communiqué that includes an action plan and principles to combat cybercrime and protect data and systems from unauthorized impairment and in addition the G8 also mandates that all law enforcement personnel must be trained, and equipped to address cybercrime, and designates all member countries to have a point of contact on a 24 hours a day/7 days a week basis

2.7.1 The Budapest Convention

The Budapest Convention is the first International legal response to cybercrimes (The Council of Europe Website September 2019). It is the first and one of the most important multilateral treaties addressing the issue of cybercrime and international cooperation. Frizel (2019) notes that the Convention seeks to address Internet and computer crimes by 'harmonising national laws, improving investigative techniques and increasing cooperation among nations.' It was drawn up by the Council of Europe in Strasbourg, France, with the active participation of the Council of Europe's observer states Canada, Japan, Philippines, South Africa and the United States of America. The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2001. It was opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004. As of September 2019, 64 states have ratified the Convention, while a further four states had signed the convention but not ratified it. The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and lawful interception (The Council of Europe, 2019).

2.7.2 The International Telecommunication Union (ITU)

The International Telecommunication Union (ITU), as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunications and cyber security issues. The ITU was the lead agency of the World Summit on the Information Society (WSIS). According to the ITU (2019), its mandate is to work on cyber security comes from the 2003 Geneva Plan of Action, one of the key outcome texts of the World Summit on the Information Society (WSIS), which tasked the ITU – and other organisations – with "Building confidence and security in the use of ICTs" (action line C5). Since then, ITU member states have given the ITU a more specific mandate to work on capacity-building on a range of cyber security-related issues, mostly through the ITU's Development Sector (ITU-D). This mandate is limited; a fact acknowledged in Resolution 130, which was adopted at the ITU Plenipot in 2014: "[The] ITU shall focus resources and programmes on those areas of cyber security within its core mandate and expertise, notably the technical and development spheres, and not including areas related to Member States' application of legal or policy principles related to national defence, national security, content and cybercrime, which are within their sovereign rights." Within that scope, the ITU's most significant mandated activities include maintaining a "cyber security gateway" as a means of sharing information on national, regional and international cyber security -related initiatives; Developing reports and recommendations which address existing and future threats and vulnerabilities affecting efforts to build confidence and security in the use of ICTs (ITU-T);

Supporting ongoing regional and global cyber security projects (ITU-D); Facilitating member states' access to resources developed by other relevant international organisations that work on national legislation to combat cyber crime (ITU-D); Supporting member states' national and regional efforts to build capacity to protect against cyber threats and cybercrime (ITU-D); Assisting member states, in particular developing countries, in elaborating appropriate and workable legal measures relating to protection against cyber threats at the national, regional and international levels (ITU-D); Establishing technical and procedural measures, aimed at securing national ICT infrastructures (ITU-D); Establishing organisational structures, such as Computer Incident Response Teams, to identify, manage and respond to cyber threats, and cooperation mechanisms at the regional and international level (ITU-D); and Building the capacity of member states to protect against cyber threats and cyber crime, as well to develop their national and/or regional cyber security strategies (ITU-D) (ITU, 2019).

2.7.3 The Southern African Development Community (SADC) Model Law on Cybercrime

According to Kshetri (2018) the increased usage of modern information and communication technologies (ICTs) in the Southern African Development Community (SADC) has made cybercrime a growing crime problem in the region. This has prompted regional-level and country-level efforts to tackle the problem by, inter alia, adopting cyber crime-related legislations. Thus, at regional level, SADC adopted the SADC Model Law on Cybercrime in 2012 to guide and facilitate the harmonization of domestic laws on cybercrime. At country level, as of July, 2017, nearly all member states of the grouping had enacted, or were in the process of enacting, cybercrime-related legislation. Terby (2016) indicated that in March 2012, the SADC adopted the Model Law on Computer Crime and Cybercrime to serve as a guide for the development of cyber security laws in SADC Member States. However, Grobler & van Vuuren (2012) affirm that it does not impose any obligations on Members to establish cybercrime laws. It does not establish any provisions to guide the development of international cooperation regimes in Member States and neither does it establish any international cooperation obligations on Member States. Orji argues that members that have established cyber security laws may rely on the SADC Protocol on Mutual Legal Assistance in Criminal Matters and the Protocol on Extradition to obtain international cooperation from other Members. He further argues that Under the SADC Protocol on Mutual Assistance, Member States are required to provide each other with "the widest possible measure of mutual legal assistance in criminal matters". The Protocol also requires that such assistance shall be rendered without regard to whether the conduct which is the subject of the mutual assistance request by a Requesting State would constitute an offence under the laws of the Requested State. On the other hand, the Protocol on Extradition requires that SADC States can only obtain cooperation amongst themselves on the basis of dual criminality.

3. RESEARCH DESIGN AND METHODOLOGY

The study used qualitative methodology. The selected key respondents comprised of the security sector, from the South African Police Service, the Zimbabwean Republic Police, the Zimbabwe Defence Forces and the South African Defence forces, for their knowledge in cyber crimes in relation to peace and stability in their respective countries and to get an oversight on their role in responding to cyber crimes as a threat to national infrastructure. The study incorporated ICT technocrats from Regulatory Authorities such as PORTRAZ for their expertise as stakeholders in the drafting of cyber legislation. The study sample also brought in the Ministry of ICT Zimbabwe as the cyber policy makers. The purposive study sample also included International Multilateral agencies in the field of cyber crimes which included, the UNODC representative in South Africa, INTERPOL officials in Harare to get an overview on how mmultilateral Institutions are fighting to combat cyber crimes in the SADC region.

This study also relied on documentary sources. It analysed data gathered from newspapers, constitutions, conventions on cyber crimes, cyber crime treaties, websites and bills to analyse data gathered from key informant interviews.

4. DATA PRESENTATION, ANALYSIS AND DISCUSSION OF FINDINGS

This section presents and analyses the key findings of the study.

Understanding of cyber crimes

A senior officer at INTERPOL defined cyber crime as;

> The use of a computer as an instrument to further illegal ends, such as committing fraud, is trafficking in child pornography and intellectual property, stealing identities, or violating privacy.

A Head of Department at the The Ministry of Information Communication Technology and Courier Services defined cyber crime as;

> *Crimes against computers and information systems, where the aim is to gain unauthorized access to a device or deny access to a legitimate use*r.

A POTRAZ IT expert opined that:

> Cybercrime in a broader sense (computer-related crimes) covers any illegal behaviour committed by means of, or in relation to,

> a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

A UNODC representative in South Africa was of the view that:

> There is no international definition of cybercrime or of cyber attacks. Offences typically cluster around the following categories: i) offences against the confidentiality, integrity and availability of computer data and systems; ii) computer-related offences; iii) content-related offences; iv) offences related to infringements of copyright and related rights.

This study noted that the respondent's view are consistent with the mostly widely accepted definition in the literature of cybercrime, by Gordon and Ford (2006) who noted that cyber crime is: any crime committed using computers, computer networks, or hardware devices. This study also noted that the term cyber crime has no 'referent in law' (Wall, 2001), as responses even from law enforcement agencies were not consistent. Wall argues that the primary problem in the analysis of cyber crime is the absence of a consistent definition. However, the study deduced that cybercrimes are not confined to the computer as a tool only, as opined by Poonia (2014) "Unlawful acts wherein the computer is either a tool or target or both". The study noted that cybercrimes can also be committed using devices such as phones, tablet devices, play station etc.

Motivations and causes of cyber crimes

A UNODC SA representative highlighted that;

> Increasing cyber attacks in the continent can be attributed to vulnerable systems and lax cyber security practices. Two countries with the world's highest software piracy rates in 2017 were from Africa: Libya and Zimbabwe. The proportions of unlicensed software in the two countries were 90% and 89% respectively. Since pirated software products cannot take advantage of updates from manufacturers, they accelerate the spread of malware.

A senior ZRP officer claimed that;

> The driving and motivating factors that compel would-be perpetrators of cyber-attacks to carry out their illicit acts are complex, varied and not absolute. However, cyber crime rates are tightly linked to a lack of economic opportunities.

A Cyber lawyer argued that;

> The intentions of digital culprits could be exceptionally broad and cover many different sorts of offences. However, consistent with history and theory cyber-criminals tend to be from locations where high-paying legitimate IT jobs are unavailable. In industrialised countries, people with IT skills can usually find legitimate IT jobs. In many developing economies, IT job growth is lower than internet penetration growth. The primary reason why some people are attracted to cyber-crime in Zimbabwe and South Africa could be high unemployment and low wages. Organised crime groups are thus tapping into the technical skills available to expand their operations.

A senior officer at INTERPOL had aptly said that;

> The combination of over-educated and under-employed computer experts has made South Africa and Zimbabwe fertile ground for hackers. In these economies the growth rate of IT industries is far from enough to absorb the IT workforce. Beyond all that, a financial crash in Zimbabwe 2008 left many computer programmers unemployed. Some of these university graduates are paid up to 10 times as much as they would earn from legitimate IT jobs by organised criminals".

A SAPS official opined that;

> The South African Police Service suffered a hack in 2013 that resulted in the release of approximately 16,000 details of whistle blowers and victims. The attack appeared to be by the group Anonymous in response to the police killings of striking mineworkers at the Marikana mine in South Africa.

An official at the SA embassy said that:

> Although it is complex to unearth a motive under illegal cyber activities, some of these hackers are cyber espionage campaigners.Servers hosting the espionage tool FinFisher, usually employed by governments to track dissent, and were detected in South Africa in 2013. Also in 2013, the Sednit/ APT28 cyber espionage campaign, attributed to Russian hackers, targeted South African embassies via an infected document sent to the embassies purporting to be from the Department of International Relations and co-operation.

Implications of Cyber Crimes in Zimbabwe and South Africa

A POTRAZ IT Expert highlighted that:

> The significance of the Stats SA hack in 2016 was that it had the potential to inflict reputational damage on state institutions and harm on the country's image and economy. The Stats SA's official website provides statistics on the country's population, crime, consumer price index and GDP figures, to name just a few. Manipulation of the information can influence investors and, therefore, effect economic implications.

A Colonel at SANDC mentioned that;

> Cyber espionage can if not handled cautiously may result in cyber wars, and here in South Africa it also become a reality, back in 2013, we discovered that the British Government Communications Headquarters (GCHQ) has been conducting a sustained campaign to penetrate South African computers, and gained access to the network of their foreign ministry; and retrieved documents including briefings for South African delegates to G20 and G8 meetings in 2009.

The Cyber lawyer was of the view that;

> One of the least predictable risks of cyber attacks is the leakage of personal data. Privacy is a fundamental human right that must be protected, and its breach has significant personal consequences. Beyond that, data breaches carry financial costs as well. Many companies are increasingly facing lawsuits filed by their clients or employees for insufficient data protection. The impacts associated with these proceedings, like the possible compensation of millions of victims, or other legal and regulatory penalties, as in the case of the credit card payment industry, can quickly become insurmountable for a company. In South Africa, the Information Regulatory Authority is currently investigating the cause of the biggest data leak in 2017—during which the personal data of more than 60 million people was stolen—and has made formal requests for explanations from the companies concerned.

The response highlighted above corresponds with secondary data gathered which revealed that he leaking of the cables revealed a number of security weaknesses within the South African government and intelligence services (Van Heerden, Von Solms & Mooi, 2016, p.16). A secret security assessment by South African intelligence in the leaked cables identified "serious deficiencies in the security integrity of the government's information systems, with "far-reaching strategic implications (Jordan, 2015a).

SADC Response to Cyber crimes

The Independent consultant opined that;

> The problem in Zimbabwe is that there is no cyber security framework in place. The current criminal legislative framework, chiefly manned, inter alia, by the Criminal Law (Codification and Reform) Act (Chapter 9:3) does not adequately address the crime related challenges emanating from the cyberspace, which is a unique and instantaneous data revolution where information can be shared across the world's boundaries at the click of a button.

The Interpol Rep added that;

> In addressing the challenges related to cyber crimes in Zimbabwe, the current legal framework has been codified in terms of the Criminal Law Codification Reform Act, the Interception of Communications Act, and the provisions of Income Tax Act, Postal and Telecommunications Act which remains the backbone of all telecommunications, internet, and electronic based communications. Acts like the Criminal Procedure and Evidence Act, the Civil Evidence Act have been put in place to deal with issues of adducing of evidence in criminal and civil matters have noticeable shortcomings on how computer related evidence or a crime committed through the computer or against a computer can be adduced in the courts. The complexity and the complicated part of crimes committed through and against computers requires a very close attention, but further more speed and spread of such crimes presents difficulties, which has caused many governments across the globe to revoke certain rights and freedoms which are enshrined in their constitutions and in the international law documents in the pursuit of security and safety.

The PORTRAZ IT Expert highlighted that;

The Bill covers data protection with due regard for constitutional rights and public interest; establishment of a Data Security Centre and a Data Protection Authority under POTRAZ; and investigation and collection of evidence relating to Cyber Crime and unauthorised Data Collection The provision and approval of codes of conduct and ethics to be observed by all categories of data controllers; while data protection with due regard to constitutional rights and public interest will be under the Postal and Telecommunications Regulatory Authority of Zimbabwe. ".

A Cyber security Lawyer added that:

According to the bill, a data security centre and a Data Protection Authority will be established. There will also be investigation and collection of evidence relating to cybercrime and unauthorised data collection and breaches. The police should be trained on cyber-crime and detecting of the same. The new law should allow the admissibility of electronic evidence for cybercrimes offences and penalties on all offences committed under the act. There will also be measures to address the production and dissemination of racist, tribalist, hatred, and xenophobic material using language that tends to lower the reputation or feelings of persons for the reason that they belong to a group of persons distinguished on the grounds set out in section 56 subsection 3 of the Constitution of Zimbabwe.

The UNODC Representative from South Africa opined that:

The law will come with untold advantages which identify standards of acceptable behaviour for information and communication technology (ICT) users; establishes socio-legal sanctions for cybercrime; protects ICT users, in general, and mitigates and/or prevents harm to people, data, systems, services, and infrastructure, in particular; protects human rights; enables the investigation and prosecution of crimes committed online (outside of traditional real-world settings); and facilitates cooperation between countries on cybercrime matters. Cybercrime law provides rules of conduct and standards of behaviour for the use of the Internet, computers, and related digital technologies, and the actions of the public, government, and private organizations; rules of evidence and criminal procedure, and other criminal justice matters in cyberspace; and regulation to reduce risk and/or mitigate the harm done to individuals, organizations, and infrastructure should a cybercrime occur. Accordingly, cybercrime law includes substantive, procedural and preventive law. So the action taken by Zimbabwe is plausible and commendable.

The responses from the research participants concur with Mawarire (2018) who indicated that the Bill was a necessary piece of legislation that helps to regulate a currently poorly regulated sector. The Bill also attempts to give the data subject some control over the information collected on him or her. However, this study deduced that a lot more could have been done to ensure that the data subject has a stronger say in the whole process. Independence of the Board could also have been promoted by, for example, allowing the public to participate in the nomination of Board members.

CONCLUSIONS

The study concludes that the real causes of cyber crimes are so complex and difficult to study the patterns as they occur. Philip (2002) agrees with this notion when he stated that it is not easy to unearth a motive under illegal cyber activities the routine activity theory of However this study also concludes that Cohen and Felson (1979)] views on the Routine Activity Theory that crimes are ultimately committed when the opportunity arises, the resourceful offender would also need to have the ability, know-how and tools to carry out a crime successfully are euro centric

and do not apply to the real causes of cyber crimes in the SADC were the major cause of concern is the lack of a robust legislation aided by economic deprivation, extreme poverty driving the surge in cyber crime rates.

Southern Africa still lacks efficient capacities and resources for cybercrime governance. This absence of capacities and resources remains a major factor that has contributed to creating an enabling environment for rising cybercrime trends in the SADC. The research ascertained that SADC countries are at different levels of crafting cyber laws and not all the SADC countries have adopted the SADC Model Law in its original form for domestication. Hence, this affects the harmonization of the laws which in turn has an effect on the region's vulnerability as cybercrimes is transnational in nature. These findings are consistent with Orji (2015) and Grobler & van Vuuren (2012) proclamations that overall the legal framework is inadequate in enhancing cyber security in the SADC region.

REFERENCES

Agba, P. C. (2002). *International communication principles, concepts and issues*. In C. S. Okunna (Ed.) (2010). Techniques of Mass Communication: *A Multi-dimentional Approach. Enugu*: New Generation Books.

Baken, D. N., & Mantzikos, I. (2013). *Exploring Nigeria's Vulnerability in cyber warfare, modern diplomacy.*Retrieved from www.moderndiplomacy.eu

Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Social & Legal Studies, 10*, 229-42.

Castells, M. (2002). *The internet galaxy: Reflections on the internet, business, and society*. Oxford: Oxford University Press.

Clarke, R., & Felson, M. (Eds). (1993). *Routine activity and rational choice*. London: Transaction Press.

Clough, B., & Mungo, P. (1992). *Approaching zero: Data crime and the computer underworld*. London: Faber & Faber.

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*, 588-608.

Cohen, L., Felson, M., & Land, K. (1980). Property crime rates in the United States: A macro dynamic analysis, 1947-1977; with ex ante forecasts for the mid-1980s. *American Journal of Sociology, 86*, 90-118.

Cohen, L., Kluegel, J., & Land, K. (1981). Social inequality and predatory criminal victimization: An exposition and a test of a formal theory. *American Sociological Review*, *46*, 505-24.

Dodge, M., & Kitchin, R. (2001). *Mapping cyberspace*. London: Routledge.

Ehimen, O. R., & Bola, A. (2010). *Cybercrime in Nigeria. Business Intelligence Journal*, *3*(1), 35-45.

Felson, M. (1986). R*outine activities, social controls, rational decisions and criminal outcomes*. In D. Cornish and R. Clarke (Eds.), *The reasoning criminal.* New York: Springer Verlag.

Felson, M. (1998). *Crime and everyday life*. Thousand Oaks, CA: Pine Forge Press.

Felson, M. (2000). *The routine activity approach as a general social theory*. In S. Simpson (Ed.). *Of crime and criminality: The use of theory in everyday life.* Thousand Oaks, CA: Sage.

Felson, R. (1996). Big people hit little people: Sex differences in physical power and Inter-personal violence. *Criminology*, *34*, 433-52.

Furnell, S. (2002). Cybercrime: *Vandalizing the information society*. London: Addison Wesley.

Grabosky, P. (2001). Virtual criminality: Old wine in new bottles*? Social & Legal Studies*, *10*, 243-9.

Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies. In D. Wall (Ed.), *Crime and the internet.* London: Routledge.

Harvey, D. (1989). *The condition of post-modernity*. Oxford: Blackwell.

Hollis, M. (1987). *The cunning of reason*. Cambridge: Cambridge University Press.

Jacobs, J. (1961). *The life and death of great American cities*. New York: Random House.

Johnston, N. (2003). *Plan approved to save U.S. digital history.* Washington Post, 15 February, 2003.

Joseph, J. (2003). Cyberstalking: An international perspective. In J. Jewkes (Ed.), *Dot.cons: Crime, deviance and identity on the internet*. Cullompton: Willan Press.

Katz, J. (1988). *The seductions of crime*. New York: Basic Books.

Kramer, F. (2009). *Cyber power and National Security*. Washington, D.C: Center for Technology and National Security Policy.

Kshetri, N. (2013). *Cybercrime and Cyber security in the Global South*. Palgrave Macmillan: London.

Kushner, D. (2013, Mar.). The real story of Stuxnet, *IEEE Spectrum, 50*(3), 48-53.

Leadbetter, C. (2000). *The weightless society*. New York: W. W. Norton.

Levy, M. (2015). The role of qualitative approaches to research in CALL contexts: Closing in on the learner's experience. *Calico, 32*(3), 554-568.

Lynch, J. (1987). Routine activity and victimization at work. *Journal of Quantitative Criminology*, *3*, 275-82.

Massey, J., Krohn, M., & Bonati, L. (1989). Property crime and the routine activities of individuals. *Journal of Research in Crime and Delinquency*, *26*, 378-400.

Newman, G. & Clarke, R. (2003). *Superhighway robbery: Preventing ecommerce crime*. Cullompton: Willan Press.

Newsday (2017). *Zim-hackable-country.* Retrieved from www.newsday.co.zw

NHTCU/NOP (2002) *Hi-tech crime: The impact on UK business.* London: NHTCU.

Ohlin, J.D. (2015). *Law and ethics for virtual conflicts.* Oxford University Press: New York.

Orji, U. J. (2015). *Multilateral legal responses to cyber security in Africa: Any hope for effective international cooperation?* Paper presented at the *Cyber conflict: architectures in*

cyberspace (CyCon), (pp.105-118). 2015 7th International Conference. IEEE.

Pool, P. (2014). War of the cyber world: The law of cyber warfare. *The International Lawyer*, *47*(2), 299-323.

Poster, M. (1995). *The second media age*. Oxford: Polity.

Shields, R., (Ed). (1996). *Cultures of the internet: Virtual spaces, real histories, and living bodies*. London: Sage.

Smith, C., McLaughlin, M., & Osborne, K. (1997). Conduct control on Usenet. *Journal of Computer-Mediated Communication, 2*(1), 23-43.

Snyder, F. (2001). Sites of criminality and sites of governance. *Social & Legal Studies*, *10*, 251-6.

Thomas, D., & Loader, B. (2000). Introduction to Cybercrime: Law enforcement, security and surveillance in the information age. In D. Thomas and B. Loader (Eds.), *Cybercrime: Law enforcement, security and surveillance in the information age.* London: Routledge.

Turkle, S. (1995). *Life on the screen: Identity in the age of the internet.* New York: Simon & Schuster.

United Nations Office on Drugs and Crime. (2012). *The use of the Internet for terrorist purposes*. Vienna: United Nations.

Wall, D. (2001). *Cybercrimes and the internet*. In D. Wall (Ed.), *Crime and the internet.* London: Routledge.

Webster, F. (2002). *Theories of the information society*. London: Routledge.

Zukin, S. (1988). *Loft living: Culture and capital in urban change*. London: Radius.