American Journal of Humanities and Social Sciences Research (AJHSSR)
e-ISSN :2378-703X
Volume-3, Issue-1, pp-146-154
www.ajhssr.com
Research Paper Open Access

An Exploratory Study on Mechanisms in Place to Combat Hacking In South Africa: A Criminological Perspective.

[1]Siyanda Dlamini, [2]Candice Mbambo
[1]*Senior Lecturer, Criminology Department, College of Social Sciences and Humanities. University of Fort Hare, South Africa.*
[1]*M.A candidate, School of Applied Human Sciences, Criminology & Forensic Studies Discipline, University of KwaZulu-Natal.*

ABSTRACT: In the past two decades, third world countries such as South Africa have made steadily developments towards combating hacking as a form of Cybercrime. The developments made by the South African Criminal Justice towards the prevention of hacking have been mildly progressive. The Council of Europe Convention on Cybercrime is the treaty that all South African legislation and policy with regard to hacking is required to be in line with this convention. This treaty has also been the cornerstone to first world countries such as the United States, when preventing cybercrime such as hacking. In order for South Africans to have a safe and secure cyberspace that is free from hackers; there needs to be a co-operative system put in place by the South African Criminal Justice System that involves the government, non-profit organizations and the community. A Criminal Justice system that works closely with the community is able to properly guide its members and correctly prosecute the crime of hacking. Therefore, using qualitative secondary data this paper explores the existing measures put in place by the South African Criminal Justice to combat hacking. The findings of this paper indicate that conceptual understanding of this crime (hacking) can play a pivotal role in addressing the manifestation of this crime in a large extent as the nature and extent can be established, the use of technological means also contribute to hacking, this is also linked to individuals (victims) ignorance. For recommendations, the use of technology and conventional method in awareness can help in responding to the scale and consequence of hacking in South Africa.
***KEYWORDS**: South African Criminal Justice System, Hacking, Cybercrime and Cybersecurity.*

I. INTRODUCTION

Computer crimes such as hacking showed great growth during the 90s in South Africa, because the internet became a popular way for users to connect worldwide. The internet is one of the greatest sensations in contemporary society. It has become a symbol of technological ingenuity and has offered humankind the greatest of benefits. The internet has been one of the most helpful networks concerning the access to information and communication.As much as the internet has made positive contributions towards human relations, this high-tech existence of the internet came with risks. According to Lilley (2002), "the internet has the capacity to liberate and imprison persons simultaneously". The internet has the power to enable individuals who have not had any special computer training education to become the biggest threat to humankind, through the ability to provide details of how to access sensitive classified information.

According to Lilley (2002), "the threat of the hacker is often perceived as being one of the major threats of the digital age". Hackers will carry out an attack on cyberspace for financial gain or either just to prove the severe security flaws in the Web site or system being attacked (Lilley 2002: 49). This means that hackers will not only hack an organization for financial gain, hackers will also intend to expose the weaknesses of a particular organization. Those individuals who hack into websites for their own financial gain and those with the intention to gain confidential personal information are crackers.

In South Africa, the developments that are designed address hacking as a form of cybercrime have been relatively slow. It is essential to investigate the existing policies of the South African Criminal Justice System that ensure the prevention of hacking. In order to derive prevention measures that will decrease the high rates of hacking attacks that the community reports. The South African Law Commission in 2001 published a discussion paper on Computer-related crime. The paper was in the form of proposal that was aimed at dealing with any persons who access stored communications with the absence of sufficient or correct authority; it also proposed that persons found guilty of such activity were liable for a criminal offence (Cybercrimes & Cybersecurity Bill 2015: 2). This led to Cybercrimes and Cybersecurity Bill of 2015, the Bill provides for various cybercrime

offences. This Bill establishes the creation of a Cyber Response Committee in parliament that will promote, guide and coordinate activities aimed at improving cybersecurity measures by all role players, which includes the strengthening of intelligence collection and improved State capacity to investigate, prosecute and combat cybercrime such as hacking.

Government institutions such as the South African Criminal Justice system are not the only contributors towards the prevention of hacking. Various non-profit organizations have made insightful contributions in the combat of hacking in South Africa. The Internet Safety Campaign (2007) is an institution that works together with the criminal justice system to create awareness of hackers. In partnership, they are able to create awareness that will protect government and private institutions and protect people's personal information. The Internet Safety Campaign (2007) has helped the criminal justice system "create an awareness catalogue 'The Cybercrime survival guide' that protects the public from hackers". The prevention of a crime such as hacking that involves digital technology and computer networks that require prevention strategies that allow the government, non-governmental organizations (NGOs) to work together. Broadhurst (2006: 4) asserts that,"the police and other agencies within government, networks between police and private institutions and networks of police across national borders should be the drivers of prevention strategies with regard to hacking". South Africa has made use of international policies that are guidelines in the creation of hacking prevention policies, such as the Council of Europe's Convention on Cyber-crime of 2001."South Africa has signed the convention but did not ratify the Convention. South Africa has complied with only the first part of the convention" (Van de Merwe 2008: 101). It provides a foundational framework in the creation of current laws that enhance the prevention of hacking (Snail 2009: 9). As a member state of this treaty Snail (2009) highlights that South Africa is obliged to criminalize:

- The accessing or intercepting data unethically and illegally on a computer system.
- The interfering without rightful authority of acomputer system and computer data.
- The misusing of computer-related devices such as "hacker tools", which include production, sale, procurement for use, import or distribution of computer-related devices.

It is important that countries learn from each other's efforts to deal with cybercrime and create an international cyber-crime code to be used universally if any significant success is to be achieved in combating hacking (Snail 2009). Therefore, the main aim of this paper is to explore the international and national policies that contribute towards combating Hacking, and explore the effectiveness of the contributions made by the South African Criminal Justice System together with the NGO`s in preventing hacking. This paper employs qualitative secondary data to critically identify and analyze the policies put into place by the South African Criminal Justice System to combat hacking as a form of cybercrime. It provides insight on the contribution of non-governmental institutions towards the prevention of hacking. Then further highlight the contributions of international policies.

Hacking refers to a successful or an unsuccessful attempt to gain unauthorized use or unauthorized access to a computer system (Howard 1997). According to Bainbridge (2000),hacking is "the accessing of a computer system without the express or implied permission of the owner of that computer system". This term "hacking" is not be confused with the term "cracking" which is a component of hacking and can be defined as an individual who enters a computer system with a fraudulent motive, for instance obtaining other persons' credit card numbers for their own financial gain (Sinrod& Reilly 2000).Hacking is part of the broader term of cybercrime, these types of crime are difficult to police and prosecute as they occur in cyberspace. Cyberspace allows for the action of illegal electronic trespassing and virtual breaking and entering, which amounts to hacking (Bainbridge 2000: 307).It falls within the scope and function of the South African Criminal Justice System to protect South Africans from the criminal activity of hacking. The South African Criminal Justice System consists of various role players and stakeholders who share the mandate of preventing crime in South Africa (Dyson 2010).

II. THEORETICAL FRAMEWORK

A theoretical framework can define and clearly illustrate a topic (Strafford&Lesham 2008). The structure that holds or supports a theory of a topic is a theoretical framework and provides a particular perspective, or lens, through which to examine a particular topic.

The use of a theory that directly deals with crimes committed in cyberspace such as hacking is necessary, as it will address the aims and objectives of this paper head on. The Space Transition Theory is a model that explains the causes of crimes in cyberspace (Jaishankar 2007: 7). The theory argues that people behave differently when they move from one space to another. According to Jaishankar (2007), the model provides key elements that explain the perpetration of cybercrimes such as hacking:

- A persons' status or position in the physical space will not allow them to participate in criminal activity in the physical space if they have repressed criminal behavior, the individual will transfer this behaviour to cyberspace.
- The element of anonymity and flexibility of identity encourages offenders to commit crime on cyberspace.

- An offender's criminal behaviour will move from the physical into cyberspace as cyberspace provides the offender with a chance to escape.
- Persons who are strangers can come together in cyberspace to commit crime in physical space and individuals who are associates are likely to unite to commit crime in cyberspace.
- Conflicting norms and values that can prevent one from criminal activity in physical space can allow one to commit crime in cyberspace.

This Space Transition Theory is able to identify that persons who are likely to become unethical hackers are less likely to have the ability of physically initiating a violent crime. Hacking is committed in a confined hidden space and the identity of the hacker remainshidden, which makes hacking more appealing to hackers. Morals and values that a personwill hold in the physical space is overridden by the hacker cyberspace due to the non-disclosure of identity.

For the purpose of this paper, it is necessary for the South African Criminal Justice System to identify the reasons, why and how hackers would hack particular institutions. This way there is direct information regarding the causes of hacking attacks, making it possible to implement morepolicies that will prevent hacking. The theory also explains why the Criminal Justice Systemhas made mild progressions in developing policies and measures that are to prevent hacking. Hacking occurs in a different space, which you cannot access physically making the policing of hacking difficult. The internet provides individuals with a platform where you can perform various commands without having to change locations, showing the borderless nature of cybercrimes. The theoretical framework shows that it is necessary to implement measures that prevent hacking as a form of cybercrime.

III. LITERATURE REVIEW

A literature review is essential to analyse literature was previously written by scholars to understand the substance of the measures that have been put in place by the South African Criminal Justice System to combat hacking. Literature reviews help us gain insight on a particular topic and understand it more (Neuman 2011:124). This literature review will explore the various policies that are in place by the South African Criminal Justice System to prevent hacking as a form of Cybercrime. Address the influence that international policies have had or still have on domestic policies that fight against cybercrime such as hacking in South Africa.

Cybercrime has shown a great increase in South Africa because the internet is the most commonly used network by humans. The drastic increase is a result of the fact that cyber criminals now have access to all information on the internet. Cyber criminals are now able to gain access to sensitive information if they possess the ability to gain access to restricted information (Snail 2009: 2). The position on convicting cyber criminals in the past has been unclear, as the law has failed to define cybercrimes such as hacking clearly. They have been definitions of theft ofproperty, but this did not include the theft of property that is accessed unethically using a computer. Prior to policies enacted to address cybercrimes, a cybercrime must link with another crime in order to amount to a criminal offence. Cybercrimes such as hacking could not prosecuted on their own as a criminal offence they had to connect to another deviation of the law (Snail 2009: 6). For instance, using the internet to defame a particular person would not amount to a criminal offence of cyber-harassment, to charge person for a wrongful act their offence would have to amount to a charge defamation of character.

Hackers will carry out an attack on cyberspace for financial gain or either just to prove the severe security flaws in the Web site or system being attacked (Lilley 2002: 49). Essentially this means that hackers will not only hack an organization for financial gain. Hacking can expose the weaknesses of a particular organization. This reinforces the pillars of the Space Transition Theory because hackers move from one space to another and will commit a hacking attack just to expose their expertise in hacking. An individual who does so would not necessarily be involved in criminal activity in public space but will do so in cyberspace(Jaishankar 2007: 8). This exposes how the advancements in Information and Communication Technologies (ICT) have created a range of new crime problems (Jaishankar 2007: 8). This creates a duty on the South African Criminal Justice to facilitate prevention, detection, investigation, prosecution and punishment for cybercrimes such as hacking.

According to the South African Cyber Hub (2016),three stakeholders need to work together in order to assist the South African Criminal Justice System with their duty to prevent hacking. The Government, private institutions and the South African Community are required to work together in order to ensure the effectiveness of the measures put in place by the South African Criminal Justice System to combat hacking.

IV. INTERNATIONAL DEVELOPMENTS

Western countries have made significant developments in creating policies that help fight against the plight of hacking as a form of cybercrime because national legislation and policies can be limited in what it can achieve. Domestic legislation only applies to the country of implementation and the implementation of such policies is highly dependent on that countries interpretation. Therefore, it is essential to provide an overview of international convention, which aims to combat hacking.

The Council of Europe Convention on Cybercrime (2001)

The Council of Europe Convention on Cybercrime of 2001 is an international convention that attempted to tackle the problem of Cybercrimes on an international platform. The aim of this policy was to establish a common ground that will foster international cooperation when dealing with cybercrimes such as hacking. "South Africa has signed but not ratified the treaty" (Snail 2009:8). The convention requires its parties to establish jurisdiction over the offences that are committed that are enshrined in the treaty. Because of the borderless nature of cyberspace where hacking occurs it is essential to have international cooperation if laws relating to cybercrimes such as hacking are deemed to be successful (Van de Merwe 2008: 101). South Africa has also complied with the first part of this convention, which sets out the regulations to criminalize acts that amount to cybercrime (Snail 2009: 9). According to Snail (2009), "The Electronic Communications Transaction Act 25 of 2002 of South Africa substantially deals with the requirements that are set out by this convention".

According to Van de Merwe (2008), The Council of Europe Convention on Cybercrime (2001) faces criticism for obligating its parties to enforce the requirements of the treaty. Critics argue that the convention should limit itself to protecting global infrastructure and only criminalize those hackers who attack global infrastructure (Van de Merwe 2008: 101). The enforcement mechanisms of the countries that form part of this treaty are not the same. The convention obliges its member countries to co-operate with each other in order to facilitate the investigation of any computer related offence. Van de Merwe (2008) asserts, "Parties may find it difficult to reach sufficient international consensus on how to criminalize "content-related offences" where countries would not agree with the criminalization of certain cybercrime acts".

The Computer Misuse Act of 1990, Chapter 18: Access to Computer Material states: "Any person is guilty of an offence if he or she intentionally causes a computer to perform any function with the intent to secure access to any private stored data held by a computer or website. Persons found guilty of such an offence will be liable of conviction to imprisonment of period not exceeding 6 months or a fine that is proportionate of the offence committed". This part of the Act criminalizes hacking, provides a necessary offence for hackers and complies with the Council of Europe Convention on Cybercrime.

The United States Department of Justice

The United States Department of justice stated that unlawful computer hacking imperils the health and welfare of individuals, corporations and government agencies that rely on the computers to communicate (Lilley 2002: 49). To address this, the United States Developed federal legislation The United States Code of 1996 under title 18 Crimes and Criminal Procedures, chapter 47: Fraud and False Statements section 1030. This policy aims to address any: "Fraud and related activity in connection with computers and impose fines and sentences on those who are perpetrators of such activity as defined by the Act" (The United States Code of 1996). This forms part of the very early policies in America that addressed hacking as form of cybercrime. In principle, the regulations of the United States are similar to those of the European Union concerning the law enforcement of the cybercrime of hacking.

The development of international policies has had major effects on domestic legislation regarding hacking.For example,India codified its first Act in 2000 called the Information Technology Act, the problem with this Act is that "it failed to meet global standards that adhere towards the protection of the community from being victims of hacking" (Nappinai 2010: 22).

SOUTH AFRICAN DEVELOPMENTS

In South Africa,the developments made to address hacking as a form of cybercrime have also been a reflection of the developments made in the international sphere. There has been no actual special legislation has been implemented to deal with hacking current legislation uses the broad term of cybercrime, which includes hacking amongst other offences a component. In 2001, The South African Law Commission published a discussion paper on Computer-related crime. The paper was a form of proposal aimed at dealing with any persons who access stored communications with the absence of sufficient or correct authority; it also proposed that persons found guilty of such activity were liable for a criminal offence. This led to the Cybercrimes and Cybersecurity Bill (2015), the Bill provides for various cybercrime offences including hacking.

The Draft of the Cybercrimes and Cybersecurity Bill (2015)

The South African Criminal Justice System faced the same obstacle as other international countries, due to that there were no laws that defined cybercrimes such as hacking. The Cybercrime Cybersecurity Bill is still under discussion, only a draft of this Act has been included in the gazette in 2015. The aim of this Draft Bill is to properly define offences and create penalties for the commitment of these particular offences. Also, to further, regulate the jurisdiction of the courts and regulate the powers to investigate and seize information regarding any report of cybercrime (Cybercrime and Cybersecurity Bill 2015: 2). Chapter 2 section 4 of this Bill address the offences by stating that; "Any person who unlawfully and intentionally accesses the whole or any part of data, a computer device, a computer network, database and a critical database is guilty of an offence" (Cybercrime and Cybersecurity Bill 2015:14). The Bill highlights the offence of anyone found in possession of software that is for unethical purposes is guilty of an offence. For instance, when hackers use emails as a virus to breakdown the computers firewall in order to gain access to a person's personal information this is an offence.

This Bill has made provision for the creation of infrastructure within the South African parliament to deal with Cybercrime such as hacking. Government department such as the Department of Correctional Services, Department of Defense, Department of Home Affairs, Department of Justice and Constitutional Development, National Prosecuting Authority, South African Police Services, State Security Agency, Department of Finance and the Finance Intelligence Centre have all come together to form committees in parliament to combat hacking (Cybercrime and Cybersecurity Bill 2015: 74). The Bill provides for the following committees that best address the phenomenon of hacking with reference to the South African Community:

The Cyber Response Committee

The objectives and functions of this committee are the implementation of government policies regarding cybersecurity. Identify and prioritize areas that require great intervention, provide a central contact mechanism that will facilitate cybersecurity and national security (Cybercrimes and Cybersecurity Bill 2015: 760). "Also to promote, guide and coordinate activities aimed at improving cybersecurity measures by all role players, which includes the strengthening of intelligence collection and improved State capacity to investigate, prosecute and combat cybercrime and to deal with cyber threats" (Cybercrimes and Cybersecurity Bill 2015: 78).

National Cybercrime Centre

The objects and functions of the National Cybercrime Centre are to facilitate the operational coordination of cyber security and incident response activities with reference to the prevention. Ensure that the inhabitants of the Republic of South Africa uphold the law and maintain order (Cybercrimes & Cybersecurity Bill 2015: 91). Develop measures in order to deal with cyber security matters affecting law enforcement (Cybercrimes & Cybersecurity Bill 2015: 91). Analyze cybersecurity trends, vulnerabilities, sharing of information and threats in order to improve the response to cybercrimes such as hacking. Establish the necessary capacity to deal with cybersecurity threats and response to incidents that jeopardizing cybersecurity."Develop and maintain cross-border law enforcement cooperation in respect of cybercrime and promote, establish and maintain public-private cooperation in order to fight cybercrime" (Cybercrimes and Cybersecurity Bill, 2015: 92). Promote, establish and maintain international cooperation in order to in order to comply with the international standards of combating cybercrimes using cybersecurity (Cybercrimes and Cybersecurity Bill, 2015: 92).

The formations of these committees show how the government has taken the initiative to address the cybercrime of hacking.

The Electronic Communications Transaction Act 25 of 2002

The Electronic Communications Transaction Act, Act 25 of 2002 provides new provisions that will combat hacking as a form of cybercrime. This Act made it possible for the prosecution of online offenders. Previously the position had been unclear on what grounds to prosecute an individual who had been guilty of a cybercrime, the Act makes clear definitions of cybercrimes such as hacking (Snail, 2009: 3). The Interception and Monitoring Prohibition Act is another policy that put in place by the Criminal Justice System to prevent the deviant behavior of hacking. This Act prohibits the unlawful interception or monitoring of any data message used by hackers (Snail 2009: 3).

Commercial Organizations and Hacking

A number of international private financial institutions have reported a number of hacking attacks but South Africa has had under reporting of hacking attacks (Herselma&Warren 2004: 253). Financial institutions are at a greater risk of hackers due to the fact that majority of their information is on computer databases.

The major problem with hacking is when people hack into websites or restricted database without the intention to affect harm to the website. A number of people find themselves in spaces they ought not to be, "people hacking into systems are often just going in to have a look around (spying) without intending to do any damage to the system or its integrity" (Herselma& Warren 2004: 254. This is not always the case in all cases of hacking, usually cracking also occurs. Cracking is when an individual hacks into a particular database with the intent to damage the systems integrity with fraudulent motives. The growth of technological information has led to a decrease of the ability to copyright your information. The main problem with intellectual property is that they can be more than one owner of intellectual property (Herselma& Warren 2004: 255).

A number of commercial institutes are interested in ensuring in delivering services in a faster and innovative platform using the internet. South African banks, government agencies and Internet Service Providers (ISPs) priorities what their websites performance and how fast it can perform new features to entice the public, cybersecurity is normally an afterthought (Oladipo 2015). In November 2015, The Sunday Times newspaper reported that hackers launched 6000 cyber-attacks on South African infrastructure such as businesses and Internet Service Providers in the month of October 2015. This is due to fact that software development companies feel pressured to work under short periods when developing websites, resulting in the creation of websites that are of a sub-standard that hackers can easily attack (Oladipo 2015). For many commercial institutes it is very difficult to detect they have been attacked by hackers, so it can take a period of about a year till a hacker is detected and the company could lose its integrity and large amounts of revenue without knowing the individual responsible (Oladipo 2015). South Africa has recently launched a Cybersecurity Hub in Pretoria aimed at assisting commercial institutes and civil society work together in reporting hacking incidents.

V. CTIMIZATION CAUSED BY HACKERS

Since the beginning of the technological revolution of computers,reports of unethical activities have increased in South Africa. The illegal and unethical use of electronic technology is difficult to preventbecause cyber space is a very large network that placed on a very small access point for example a computer, cell phone and other communication devices (Hollinger 1991: 6). The major problem with cybercrimes is that various policies and legislation failed define cybercrimes, describe the offence and provide a just and equitable fine. Observing the activities that have occurred within our communities it is evident that computer crime especially in the form of telecommunication and system hacking is on the rise (Hollinger 1991: 8).

This means that victimization can occur on a micro level or on a macro level. These exploitations or victimization can occur in two ways; firstly, "it creates the impression that personal computer (PC) related exploitations are happening with some normality among a little be that as it may, critical number of organizations and associations every year, bringing about generally substantial scale fiscal misfortunes" (Hollinger 1991: 9). Secondly, "roughly three-fourths of these occurrences are commonly executed by workers and not untouchable programmers"(Hollinger 1991: 9). It would create the impression that defrauded associations consider personal computer wrongdoing as essentially as an example of worker robbery (Hollinger 1991: 9). The problem with cybercrime it has been highly defined as business related crimes meaning that normally an individual who has been employed by the by the particular institution that will later cause a threat to that same institution.

The Colluminate Research Firm has identified South Africa as one of the hotspots for Cybercrimes. Government agencies, commercial institutes and the community have lost millions of rands due to hackers (Herselma& Warren 2004: 255). Hackers are not involved in hacking only to gain an income; in some instances, they seek to defame individual by accessing confidential information. The threat of hackers has the ability to cause victimization of all types of crime to the South African community. This makes it necessary to create awareness and increase the measures that are in place by the Criminal Justice System to prevent hacking. The eradication of hacking attacks is difficult to achieve but is relevant to develop practices to curb this type of cybercrime.

NON-GOVERNMENTAL ORGANISATIONS DEVELOPMENTS

Non-government organizations have major contributions towards the prevention of hacking because, these organizations seek to the bridge the gap made by the South African Criminal Justice System. This creates smaller and more intimate platforms to combat cybercrime. Such organizations look at the specific needs and can communicate with the community directly on how to protect themselves from hackers.

Alert Africa

Alert Africa is a public awareness initiative that is in the form of a website created to protect average internet users from hackers. The aim of this site is to educate and protect Africans from the threats that can occur over the internet (Wolfpack 2015: 20). The Alert Africa website aims to educate the average internet users about different cyber threats that exists online, provides useful tips on how to not become a victim as well as where to report cybercrime to (Wolfpack 2015:20).

Wolfpack Risk Awareness Campaign

This campaign adopted by the South African Police Services to combat hacking as a form of cybercrime. This campaign is intensive, provides various mechanisms to protect individuals from cybercrimes such as hacking, and creates awareness for these sorts of crimes. The South African Police have made great reference to the Wolfpack's Information Security Awareness Catalogue of 2015.

The Internet Safety Campaign 2007

The Internet Safety Campaign (2007) is an institution that works together with the criminal justice system to create awareness of hackers. In partnership, they are able to create awareness that will protect government and private institutions and protect people's personal information. The Internet Safety Campaign (2007) has helped the criminal justice system create an awareness catalogue 'The Cybercrime survival guide' that protects the public from hackers. This campaign consists of a public awareness portal. The site provides access to relevant and trusted local and international resources aimed at educating individuals at all levels. The site also features help for reporting suspected activities. It is part of an independent, non-commercial initiative borne out of the needs identified over this past decade for pooling resources to address the criminal exploitation of Information and Communication Technology in South Africa

Anonymous Africa

Anonymous Africa is group of hackers that known as 'hacker-activist' this is a group of individuals that use hacking to address agents of corruption, racism and fraud (Van Zyl 2016). Political parties such as the Economic Freedom Fighters (EFF) of South Africa and the Zanu-PF of Zimbabwe have been victims of this group of hackers. Recently the hackers have targeted websites in South Africa, which belong to Gupta owned companies such as the broadcaster ANN7, The New Age newspaper, Sahara and Oakbay (Van Zyl 2016). The hackers of Anonymous Africa use hacking to lead a mass protest of the injustices that occur in various countries, their aim is to bring attention to these issues using a peaceful and non-destructive protest through hacking (Van Zyl 2016). The ANN7 and The New Age belong to the South African Broadcasting Company (SABC), which is a

national key point. The Criminal Justice System has the onus to protect the integrity of national infrastructure such as the SABC from intruders. According to the South African Constitution Act 108 of 1996 South Africans have the right to freedom of speech, therefore the protests of Anonymous Africa are within the scope of their constitutional rights. Non-governmental organizations of this nature must not expose sensitive data of national key points in order to protect government websites from hackers who are not advocates of justice and harmony, who only see to destroy.

In South Africa the development of these policies have been relatively slow due to the problem faced internationally of defining what will construct a hacking. The Criminal Justice System has created policies that address cybercrimes that would also encompass hacking. The problem with these policies and measures they are a work-in-progress, as they do not specifically define hacking. In conclusion, internationally and nationally various strides have been made towards creating a safe cyberspace. In order for the South African Criminal Justice System to combat hacking there needs to be system for government agencies, commercial institutions, non-governmental institutions and the community need to work together to create a safe cyberspace.

VI. METHODOLOGY

This paper is a secondary qualitative study conducted as a desktop research project. According to Travis (2016), "a secondary research study requires the researcher to read recent scholarly works that have made contributions towards answering the research problem". This process involves collecting data from either the originator or a distributor of primary research. In other words, accessing information already gathered. This means finding information from third-party sources such as research reports, websites, magazine articles, and other sources (Travis 2016).

This paper is a literature based research project, conducted through various searches using the internet. Firstly, using Google as a search engine to find out to what extent the cybercrime of hacking has affected South Africa, by looking closely at current newspaper discussions surrounding this topic. Secondly, using the University of KwaZulu-Natal libraries search engine called World Cat, which allows one to locate books in any of the University of KwaZulu-Natal libraries and other libraries. WorldCat also provides one with e-books. WorldCat provides with books and e-books that addressed the policies implemented by the South African Justice System to prevent hacking as a form of Cybercrime. These books addressed the development of policies from international policies that prevent hacking in other countries. Thirdly, Google Scholar located the various international policies and to seek further books and articles that address the research topic. Fourthly, a search using EbscoHost located journal articles that address international and national policies developed to combat hacking as a form of cybercrime. Lastly, governmental organization websites where used to locate non-governmental websites that also contribute to the prevention of hacking.

VII. DISCUSSION

Analysis for this paper required the researcher to conduct a secondary data analysis. The researcher is not involved in the actual primary collection of the data(Braun and Clarke, 2001: 6). This research paper consists of various perspectives defined and researched by other scholars. This makes it essential to use an unstructured analysis, through logical reasoning, comparative analysis and synthesis of the facts gathered from the literature collected.

From the literature collected from the study, the researcher finds that the South African Criminal Justice System has made progress towards the creation of policies that promote the prevention of hacking as a form of cybercrime. The formulation of such policies is something that is very new to the world as many countries where faced with the problem of not being able to define a crime that is committed on cyberspace. Internationally the growth of technology and the internet has been much faster as opposed to South Africa, hence the formulation of such policies in first world countries is more established. South Africa has adopted international treaties and policies in order to prevent such criminal activity.

The South African Criminal Justice System has made various commitments to the creation of programs that protect the community from hackers. The draft of the Cybercrimes Bill of 2015 has shown a greater progression in the South African Criminal Justice Systems prevention of hacking. It has made it possible for the creation of committees in parliament that will hold responsibility and accountability in the creation of various programs that will prevent cybercrimes such as hacking. The Bill is still in draft form and shows the mild progression the South African government has made in order to assist the Criminal Justice in its fight against hackers.

Non-governmental organizations have also made positive contributions towards the combat of hacking as a form of cybercrime. These organizations help create awareness among communities at a more personal level. They provide individuals with easy to use manuals to protect their computers and cell phones from hackers. The South African Police Services works closely with non-government organizations that seek to contribute towards the prevention of hacking and assist with the implementation of the national policies.

It is evident that current policies and legislation do not specifically define hacking as they make more reference to cybercrime as a broad criminal offence. Legislation does not specifically define hacking but refers to

activities that would amount to hacking. It is essential to create policies and legislation that correctly defines hacking.

Organizations seek mostly to make the internet more effective in order to reach their own financial and competitive goals. Cybersecurity should be the central key point of any organization that uses the internet as it can expose the business and the community to great amount of criminal activity.

VIII. RECOMMENDATIONS AND CONCLUSION

"You can never stop cyber-attacks but you can employ the best practices to curb them," –Bright Mawudor 2015

South Africa Criminal Justice System faces a major challenge with regard to hacking. South African laws have shown mild progression towards dealing with cyber threats such as hacking. Prevention measures of cybercrimes such as hacking have shown great increase in most countries in the world, the challenge has been the implementation of such policies and projects. The problem of not having efficient cyber capacity skills is prevalent around the world this makes it difficult to address the threats caused by hacking.

The Cybercrimes and Cybersecurity Bill of 2015 is a step forward towards a safer cyberspace for South Africans. The Bill has been criticised for being vague and unrealistic, as South Africa does not have the necessary resources to implement the requirements of the Bill. The South African CyberHub (2016) has made it easy for South African to work together in creating awareness and reporting cases of hacking. It is evident that South Africa has created a legal platform to fight hacking but nothing aimed at policing cybercrimes such as hacking.

The cybercrime of hacking has mirrored across the world and South Africa. It is necessary to create a forum bringing together cyber-security experts, from university to corporate level, to discuss how to take the initiative on these issues, rather than wait for the exploitation of security gaps. It is essential to work with young people with newly acquired computer skills who might otherwise be tempted to use them for illegal activity online.

This makes it necessary for the South African Criminal Justice to create measures that police cybercrimes such as hacking. In order to make the prevention more attainable the government, commercial institutes and non-government organisations should work together in creating awareness programmes that protect the End user (members of the community). It is also necessary to for the South African Criminal Justice System to advocate for the creation of the necessary expert skills to combat hacking through the training of young computer experts in the art of combating and detecting cyber threats such as hacking. The creation of an effective cyber-response team is necessary in the South African Police Services to protect South Africans from the threat of hackers.

In conclusion, the Criminal Justice System of South Africa is making progress with regard to developing policies that prevent hacking as a form of cybercrime. It is essential that government agencies work together in order to prevent the growing phenomenon of hacking. The Council of Europe Convention on Cybercrime is a key treaty in shaping global laws and policies aimed at combating hacking. The treaty is central to South African laws and policies as it is a key element in the formation of legal documents used to form South African Cybersecurity policies.

The Draft of the Bill of Cybercrime and Cybercrime 2015 accounts for the slow development of legislation in South Africa with regard to hacking. This is the main policy that forms committees in parliament that address cybercrimes, these committees ensure that parliament is accountable in the creation of policies and measures that prevent hacking as a form of cybercrime. Parliament is the central to law making in South Africa it is essential that parliament forms part of organizations that assist the South African Criminal Justice System in making policies that assist with preventing hacking.

It is evident that victimization through hacking has shown an increase in South Africa. It is necessary to develop measures that will protect individuals from hackers. The internet allows hackers the ability to become a threat to all types of communities, it is also essential to equip members of the public on methods to protect themselves from hackers.

Due to the relatively slow developments made towards making South Africans safe over the internet it is relevant to for Non-governmental organization to contribute towards the combat of hacking as a form of cybercrime. Cybercrime South Africa is an organization that has made great strides towards assisting the South African Police Services in ensuring that they provide members of the community with the necessary prevention strategies to decrease victimization. Various institutions are interested in making their institutions more accessible using the internet and are oblivious to how vulnerable the organization becomes to hackers

REFERENCES

[1]. Broadhurst, R. 2006. Developments in the Global Law Enforcement of Cybercrime. *International Journal of Police and Management* 29(3): 403-433.

[2]. Hollinger, R. G. 1991. Hackers, Computer Heroes or Electronic Highwaymen. *Computer and Society* 21(1): 6-17.

[3]. Howard, J. 1997. Analysis of Security Incidents on the Internet. Unpublished Doctoral Dissertation. Pennsylvania: Carnegie Mellon University.

[4]. Jaishankar, K. 2007. Establishing a Theory of Cybercrimes. *International Journal of Cyber Criminology* 1(2): 7-9.
[5]. Mawudor, B. 2015. BBC News 17 November 2015
[6]. Nappinai, N. S. 2010 Cybercrime Law in India: Has Law kept Pace with Emerging Trends. *Journal of International Commercial Law and Technology* 5(1): 22-28.
[7]. Oladipo, T. 2015. Cybercrime is Africa's Next Big Threat Experts warn. *BBC Monitoring Africa Security Correspondent* 17 November 2015.
[8]. Snail, S. 2009. Cybercrime in South Africa: Hacking Cracking and other Unlawful Activities. *Journal of Information Law and Technology* 3(2): 35-48.
[9]. Van Der Merwe, D. 2008.*Information and Communication Law* (Ed). Pretoria.
[10]. Van Zyl, G. 2016.*Why Anonymous Hacked the SABC, Gupta Websites*. Available from www.fin24.com/companies/financial-services/anonymous2016061244 (Accessed 03 July 2016).
[11]. Wolfpack 2015.*Information Security Awareness Catalogue*. Available from www.wolfpackrisk.com. (Accessed 20 July 2016).
[12]. Travis,D. 2016. *Desk research: the what, why and how*. (Online). Times Live. Available from: www.userfocus.co.uk (Accessed on 20 September 2016).
[13]. Neuman, L.W. 2011.*Social Research Methods: Qualitative and Quantitative Approaches*. 7th ed. Boston, MA: Allyn and Bacon.
[14]. Bainbridge, D. I. 2000. *Introduction to Computer Law* 307.
[15]. Sinrod, E. J & Reilly, W. 2000. Hacking Your Way to Hard Time: Application of Computer Crime Laws to Specific Types of Hacking Attacks. *Journal of Internet Law*. 4(3): 3.
[16]. Dyson, M. 2010.*The Criminal Justice and You: A Guide to the South African Criminal Justice System.* Independent Projects Trust. Print Expression. Available from www.justiceforum.co.za. (Accessed 21 September 2016).
[17]. Internet Safety Campaign. 2007. Available from www.cybercrime.org(Accessed 20 July 2016).
[18]. Lilley, P. 2002.*Hacked Attacked and Abused: Digital Crime Exposed*. Koagn Page. Great Britain: Biddles Ltd.
[19]. Strafford, V. and Lesham, S. 2008.*Stepping Stones to Achieving your Doctorate*. Mainhead: Open UP.
[20]. Prestorious, H. and Prestorious, E. 2008.*Calumniate Online and Market Research Agency in South Africa*. Available at https://www.columinate.com/(Accessed 13 August 2016).

Cited Legislation

[21]. The Draft of Cybercrime and Cybersecurity Bill, 2015 (RSA). Available from http://www.justice.gov.za/legislation/invitations/cybercrimesbill2015. (Accessed 20 March 2016).
[22]. The Electronic Communications Transaction Act, 2005 (RSA), 25. Available from http://www.up.ac.za/media/shared/409/(Accessed 20 March 2016).
[23]. The Council of Europe Convention on Cybercrime, 2001 (UK). Available from http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/ (Accessed 20 March 2016).
[24]. The Constitution of South Africa, 1996 (RSA). Available from http://www.justice.gov.za/legislation/constitution/saconstitution-web-eng.pdf (Accessed 20 March 2016).
[25]. The United Kingdom Computer Misuse Act, 1990 (UK). Available from http://www.legislation.gov.uk/ukpga/1990/18/contents (Accessed 20 March 2016).
[26]. The United States Code of 1996 title 18 Crimes and Criminal Procedures. Available from https://www.gpo.gov/fdsys/pkg/USCODE-2009-title18/ (Accessed 20 March 2016).
[27]. India Information Technology Act, 2000 (India). Available from www.wipo.int/wipolex/en/text.jsp?file_id=185998 (Accessed 20 March 2016).
[28]. The Interception and Monitoring Prohibition Act, 1992 (RSA), 127.Available form https://www.imdin.org/doc/amlid. (Accessed 20 March 2016).