cogent
social
sciences

Taylor & Francis
Taylor & Francis Group

Cogent Social Sciences

ISSN: (Print) 2331-1886 (Online) Journal homepage: https://www.tandfonline.com/loi/oass20

# Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses

Siyanda Dlamini & Candice Mbambo |

**To cite this article:** Siyanda Dlamini & Candice Mbambo | (2019) Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses, Cogent Social Sciences, 5:1, 1675404

**To link to this article:** https://doi.org/10.1080/23311886.2019.1675404

Accepted author version posted online: 03 Oct 2019.
Published online: 09 Oct 2019.

Dlamini & Mbambo, *Cogent Social Sciences* (2019), 5: 1675404
**https://doi.org/10.1080/23311886.2019.1675404**

cogent social sciences

Received: 21 June 2019
Accepted: 26 September 2019
First Published: 03 October 2019

*Corresponding author: Siyanda Dlamini, Criminology, University of Fort Hare, South Africa
E-mail: sdlamini@ufh.ac.za

Reviewing editor:
Will W. K. Ma, HongKong Shue Yan University, Hong Kong

Additional information is available at the end of the article

LAW, CRIMINOLOGY & CRIMINAL JUSTICE | RESEARCH ARTICLE

# Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses

Siyanda Dlamini[1]* and Candice Mbambo[2]

**Abstract:** Cybercrime continues to be a detrimental problem in South Africa and continues to change in nature and sophistication. Innovations and technological advancements aimed at moving the world towards a digital age increase the risks of cybercrime. Concurrently, as the risk of cybercrime increases so does the challenge to police it. The policing of cybercrime is generally an afterthought for several organisations and individuals in South Africa. This type of crime has no regional, national or international boundaries, unlike "traditional crime" which has physical boundaries and limits in relation to jurisdiction. This contributes towards the challenge of detecting, investigating and combating it. Cyber criminals have intercepted vital and essential government, personal and business information online. Therefore, the primary objective of this paper is to explore the obstacles/challenges that hamper the effective and efficient policing of cybercrime in Durban, South Africa. A qualitative research approach was adopted, to explore the challenges of policing of cybercrime in the study area. The findings collected through semi-structured interviews with a total number of twenty (20) participants comprising of SAPS Directorate for Priority Crime Investigation (DPCI) officials, members of Bowline Security and members of the Durban community; suggest that there is

## ABOUT THE AUTHOR

Dr Siyanda Dlamini is a Senior Lecturer in the Criminology Department at the University of Fort Hare; and Miss Candice Mbambo is in the Research Department at SASSETA. Both authors have worked collaboratively to ensure the success of this paper. Both authors have individually and critically worked on, evaluated the quality of the manuscript, and agreed to send it for publication. Candice Mbambo designed the study, participated and led the data collection, analysis and writing of the manuscript
Dr. Siyanda Dlamini did a critical review of the manuscript before submission for publication consideration. Formatting, proofreading, as well as the technical presentation of the manuscript in compliance with author guidelines was put right by Dr. Siyanda Dlamini while editing and typesetting of the final draft were done by both authors. The authors have read and agreed to this manuscript.

## PUBLIC INTEREST STATEMENT

The researchers strongly believe in promoting the prevention and awareness of crime as well as the empowerment of all groups within communities. This compassion has brought the plight of cyber-crimes to the researchers` attention. They discovered that the phenomenon of cybercrimes is mildly researched within the context of South Africa. This study will add value to society as it will establish new ideas concerning better and more effective strategies to respond to cybercrime in Durban. This in turn will promote more effective policing and investigative strategies as the public will be able to provide detailed information to the responsible SAPS DPCI unit in Durban. This will be crucial for the general livelihoods of Durban residents and visitors, as they will live in a safer and more secure environment where cybercrime, and its resultant spin-offs, will be curbed. It is therefore envisaged that the law-abiding residents of Durban will gain confidence in the stakeholders of policing cybercrime.

a shortage of SAPS officials who are knowledgeable in handling cybercrime related cases. Policies and strategies to police cybercrime in Durban are insufficient because of the lack of resources, to adequately implement policy and promote cooperative strategic partnerships. Together, these findings suggest that all relevant stakeholder organisations should assist in minimising the challenge of policing of cybercrime.

**Subjects: Criminology; Social Sciences; Social Policy; Criminal Law**

**Keywords: Cybercrime; policing; technology; South African police service; Durban**

## 1. Introduction

The 21st century has ushered high rates of techno-social change, a moderately new phenomenon has developed which is evident through crimes that were previously unknown and not administered against by law enforcement agencies (Sissing, 2013). Leaving potential victims of crime at the risk of immediate, elusive exploitation and victimisation. This phenomenon can be viewed as a sub-division of crime known as cybercrime or online crimes (De Angelis & Sarat, 2000). Cybercrime takes place in a cyber-environment and is perpetrated by using any form of cyber technology device such as computers, telephones and credit-card machines. Which refers to any criminal activity in which computers and or the Internet function as the primary means to commit a misdemeanour (Booysen, 2011). Cybercrime ranges from cyber pornography, identity theft, hacking and cyber stalking (Higgins, 2010).

The enormous development of the usage of the Internet, effortlessness of availability, and reasonableness, digital innovations are promptly accessible to all people in different settings. The convenience, speed and anonymity of the internet has subsequently caused the expansion of the occurrence of cybercrime. In support of this, Wall (2007) argues that as virtual environments become more established and heavily populated, so does the need to maintain order on them. The maintenance of order on virtual environments can be achieved through the policing of cybercrime. Public and private sector organisations are interested in delivering services innovatively using the internet and measures of safety are an afterthought (Oladipo, 2015). Furthermore, "South African banks, businesses, Government agencies and Internet Service Providers (ISPs) prioritise the performance and features of their websites to entice consumers yet measures to police the internet are of a low standard and quality" (Oladipo, 2015, p. 2).

South Africa is rated among the countries showing highest rates of cybercrimes in the world (Von Solms, 2015). The South African Polices Services Directorate for Priority Crime Investigation (SAPS DPCI) also known as HAWKS highlighted that the occurrence of cybercrime in Durban has gradually increased (Cole, 2013). There is no standard globally accepted definition of cybercrime and this makes this phenomenon more difficult to analyse and counteract. Furthermore, cybercrime does not leave the same physical traces as traditional crime and can be committed from remote locations. This further contributes towards the challenge of policing cybercrime. It is precisely in this context that the primary objective of this paper is to explore the challenges of policing cybercrime in Durban. This paper aims to suggest evidence based strategies to improve the policing of cybercrime and improve the effectiveness and efficiency of the mechanisms in place to police cybercrime in a South African context.

## 2. Policing cybercrime: international perspectives

In the past decade, first world countries have shown great progression in terms of technological developments. According to Minaar (2016), it is very difficult to provide representation on the occurrence of cybercrimes due to high rates of under-reporting or a lack of knowledge on what constitutes a cybercrime. In 2011 a survey conducted by the United States of America (USA) Federal Bureau of Investigations (FBI) in 24 countries indicated that the bill for cybercrimes

**Figure 1. Victims of cybercrime.**

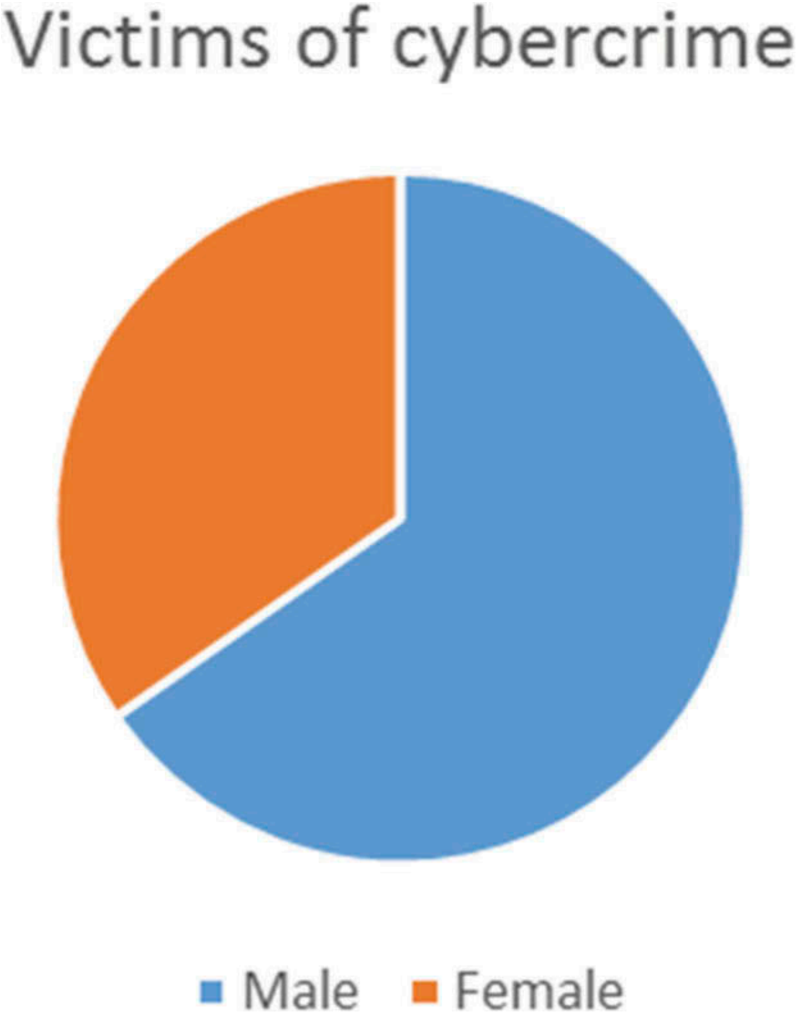
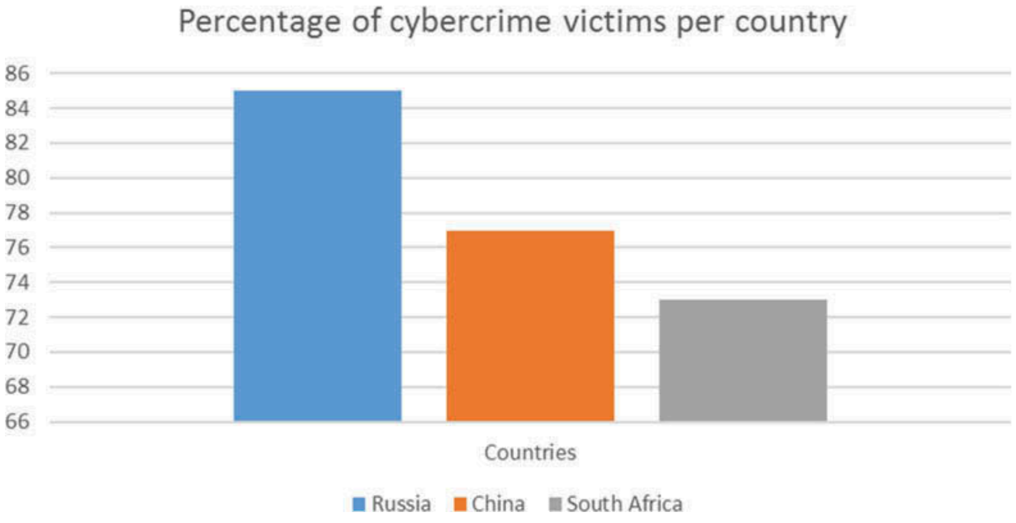


**Figure 2. Percentage of cybercrime victims per country.**



amounted to USD$388 billion ((Lievrouw & Livingstone, 2014; Van Zyl, 2016). As a result, large amounts of revenue have been lost due to cybercrimes globally; the amounts of money lost to cybercrimes are larger than the global black market. The USA FBI in 2013 estimated that "within the next five years the amount that will be lost by the economy because of cybercrimes will be greater than that which is lost to all forms of white collar crimes" (Widsup, Spitter, Hylender, & Basset, 2018, p. 800).

Consequently, in 2016 the USA FBI provided an analysis on victims of cybercrime (Figure 1). The analysis indicated the following:

Victims of cybercrime are more likely to be male (64%, compared to 34% female) and these victims would be mobile device owners and social network users (63%). Moreover, cybercrime is more likely to occur at a public or unsecured Wi-Fi "hotspot", such as internet cafe. These victims are also more likely to live in an "emerging market" country (68%).

In addition, these victims of cybercrime are most likely to have experienced cyberattacks such as malware, viruses, hacking, cyber-fraud and cyber-theft. Interestingly the three highest number of cybercrime victims per country are found in Russia (85%), China (77%) and South Africa (73%) (Symantec, 2016) (Figure 2).

Moreover, in December 2013 the "USA suffered their largest security breach where millions of consumers accounts were hacked" (Fin, 2015, p. 177). It is believed that the cyber criminals responsible for this encounter were from Russia. Russia has an extremely profitable and professional cybercrime industry. This is evident in the work of Rifkind (2011) cited in Fin (2015, p. 180) that in 2013, Russian cybercrime industry made over 1.9 billion dollars that year". Hence, tracing cybercrimes is very difficult due to the borderless nature of virtual reality. Hui, Kim, and Wang (2017) are of the view that "it is often difficult to identify and trace cyber criminals, assess the extent and impact of their offenses, and collect and analyse related digital evidence". From this, there is a need for a collaborative international enforcement that is aimed at policing cybercrime.

Western countries have made significant developments in creating policies that help fight against the plight 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 such countries.

### *2.1. The council of Europe convention on cybercrime (2001)*

The Council of Europe Convention on Cybercrime (ECC) (2001) was the first 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. South Africa has signed but not ratified the treaty. 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 cybercrimes occur it is essential to have international cooperation of laws relating to cybercrimes to combat such crimes (Van de Merwe, 2015). South Africa has also complied with the first part of this convention that sets out the regulations to criminalize acts that amount to cybercrime. The Electronic Communications Transaction Act 25 of 2002 of South Africa substantially deals with the requirements that are set out by this convention.

The Council of Europe Convention on Cybercrime (2001) has been criticized 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 cyber criminals who attack global infrastructure. This is because the enforcement mechanisms of the countries, which form part of this treaty, are not the same. Furthermore, the convention obliges its member countries to:

> *“Co-operate with each other to facilitate the investigation of any computer related offence. 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”* (Van de Merwe, 2015, p. 101).

### *2.2. The United States department of justice*

The United States Department of Justice stated that unlawful computer accessing imperils the health and welfare of individuals, corporations and government agencies that rely on the computers to communicate (Lilley, 2002). 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. This forms part of the very early policies that were developed in America to address cybercrime. In principle, the regulations of the USA are like those of the European Union concerning the law enforcement on the policing of cybercrime.

Moreover, the development of international policies has been relatively moderate as most countries were unable to identify adequate mechanisms to police cybercrimes. India codified its first Act in 2000 called the Information Technology Act 21 of 2000 as a contribution towards the policing of cybercrimes in India. Conversely, it has failed to meet global standards that adhere towards the protection of the community from being victims of cybercrimes (Nappinai, 2010). This Act made recognition of the electronic records and the facilitation of electronic commercial transactions. Furthermore, it referred to primary offences such as tampering with a private source code, deleting, destroying and altering any data on a private computer (Nappinai, 2010). This emphasizes the gradual pace of the developments of legislation aimed at policing and preventing cybercrimes. This Act is aimed to include and protect both the protection of private information and data. This provides a platform for policing cybercrimes promotes the prevention of cybercrime and creates a broader definition of cybercrime to decrease cyber victimization caused by cyber criminals on the community.

## 3. Policing cybercrime in South Africa

Cybercrime is prevalent in South Africa and external attacks are on the rise causing damage to companies and organizations (McNamara, 2012). There are cybercriminal organizations in South Africa that engage in causing damage to individuals, Organisations and government in the form of extortion, blackmail, spreading of viruses, malware and ransom. Many corporations and government infrastructure have poor security control regarding cybercrimes.

The primary challenge facing South Africa is the lengthy development and implementation process of policies and mechanisms that combat cybercrimes. Because of high rates of evolution in cybercrime techniques and advancements in ICT, policy makers must be quick to shorten the gap between development and efficient implementation of policy (Maughan, 2007). Several government departments fail to participate in issues regarding cybercrime. Outdated policies and insufficient training given to stakeholders prevent full and effective policing of cybercrime. However, the cooperation and linkage of academia, the private sector, and the public sector is growing but still needs more work to assist in the policing of cybercrime in South Africa. In addition, spreading Cybersecurity awareness has also been a challenge, increasing the risk of negligent ICT use amongst consumers, citizens, public officials and producers

The challenges faced by South Africans regarding cybercrime are not unique and are evident in other developing countries. According to Mahlobo (2015), the minister of state security presented his budget speech in parliament, the minister identified the security of cyberspace as one of government’s five strategic objectives in the Department of State Security. This department is tasked with improving the Criminal Justice System, border management, domestic stability and reducing corruption. The department further identified a list of Cybersecurity priorities that will assist the policing of cybercrimes (Mahlobo, 2015), which are:

- The need for better approaches to authenticate hardware, software, and data on computer systems and to verify user identities and the creation of methods of monitoring and detecting security compromises.
- The need for a holistic approach in the fight against cybercrime.
- An evaluation of the influence of laws and regulations on the use or abuse of electronic information.
- Increasing the awareness of cybercrimes and Cybersecurity.
- The understanding of social media networks risks and corporate espionage.

The department's immediate priorities, including the enhancement of institutional the cybercrime and Cybersecurity capacity, the finalization of national Cybercrime and Cybersecurity policy and legislation, the promotion of partnerships for public cybercrime awareness campaigns, strengthening cooperation with South African Development Community (SADC), African Union (AU) and BRICS partners, and the establishment of a Cybersecurity Centre (Mahlobo, 2015). Therefore, it is evident South Africa has made significant strides towards policing cyberspace. However, achieving a safe cyberspace, through implementation of policies and strategies of policing cybercrime is a great challenge.

## 4. The challenges of policing cybercrime

Policing of cybercrime encompasses the investigation, detecting and combating cybercrime. Therefore, the challenge of policing cybercrime will be discussed below, considering the above elements:

### *4.1. Investigating cybercrime*

Investigation involving computers often fail due to mistakes made at the initial stage of the investigation process where essential digital evidence being ignored, destroyed, compromised or inappropriately handled. Essentially, during an investigation of cybercrime there needs to be minimal delays in responding to the crime. Delays during an investigation compromise the effectiveness of the investigation and makes the response irrelevant and of no worth when it comes to catching the cybercriminal.

In the past Cybersecurity, responders have been reluctant to act immediately against cyberattacks, as they fear having sufficient evidence of reasonable justification of a crime in progress to react immediately. The assumption that an "intrusion may be caused by the perpetrator unintentionally where he or she is just looking around a computer system without the intent of compromising the organizations data" (United Nations Office on Drugs and Crime [UNODC], 2013, p. 17). For a response to be effective and immediate, it needs to be clear whether the cyberattack in progress is an illegal and fraudulent act (UNODC, 2013).

### *4.2. Detecting cybercrime*

Many organizations encounter the challenge of cybercrime. Law enforcement agencies are deficient or slow to respond when it comes to detecting cybercrimes, "organisations have taken to launching their own counter-attacks and, even if such can be construed to be in 'self-defence', which might be illegal in the eyes of the law or even labelled as an illicit act of Cyber vigilantism" (Kader & Minaar, 2015, p. 69). This sort of counter-attacking appears to be a growing response to detect and combat data breaches experienced by large multinational companies and organizations and is used in the protection of company databases and insuring that sensitive client information is not fraudulently accessed by cybercriminals. The initiation of a stronger cooperative policing strategy by the police, private sector and the community is an answer to curbing these actions.

### *4.3. Combating cybercrime*

Security threats increase and diversify which means that there is a need to improve security strategies and defences must be strengthened to assist the launch of counter attacks for companies and organizations to combat cybercrime. A variety of organizations and companies (those with adequate financial resources) can undertake regular cybercrime risk assessments, and implement advanced cybersecurity technology, secure firewalls, digital evidence preservation, content identification, intrusion detection, cyber intelligence gathering, cyber surveillance of all incoming online traffic and they can monitor their network systems 24/7 (Widsup et al., 2018). Organisations that can afford to implement such security strategies assist specialists who police cybercrime in the rapid response to cybercrime. Hence, "Cyber forensic investigators can detect an intrusion irrespective of the level or criminal intent of the cyber-attack, they can also make use of an existing live connection from a suspect's device to counter attack by deflecting, disrupting or infecting the attacking device(s) irrespective of the criminal's location" (Widsup et al., 2018, p. 600)

The challenge is that these kinds of operations are expensive and small and medium-sized enterprises lack resources to take the necessary and sufficient steps to protect their data systems. Most organizations and individuals are under the impression that they are not a target worth the attention of cyber criminals. According to the UNODC (2013, p. xxvii) this problem is prevalent amongst many government departments as they are normally having insufficient funds for these strategies. As a result, cybercrimes are difficult to combat because of the insufficient resources available to the public and private sectors.

## 5. Methodology

The problem that informed this study is that as technology advances, society is becoming increasingly reliant on computers and the Internet. The sphere of cyberspace facilitates information to be transferred over data lines leaving millions of people vulnerable to cybercrime. This increases the need to implement effective and efficient mechanisms to police cybercrime in South Africa. The study used a phenomenological design that is both descriptive and explorative in nature. Furthermore, the use of a qualitative research approach enabled an in-depth appreciation of the participant responses and a detailed understanding of the policing of cybercrime in Durban, South Africa.

### *5.1. Study population*

The study was conducted using a sample size of twenty (20) participants. Participants were all residents of Durban. The sample consisted of seven (7) detectives from the South African Police Services from the Commercial Crimes Unit who are responsible for investigating cases that involve cybercrimes. The sample also included three (3) participants from Bowline Security. One (1) of the participants is a researcher who has extensive knowledge on cybercrimes within the Durban Metropolitan. Bowline Security is a private company that works closely with the SAPS and Durban Metro Police in the investigating, providing awareness of cybercrimes and they provide cybersecurity. Lastly, the sample includes ten (10) members of the Durban community who have been victims of cybercrime. Three of these participants are part of private cooperation's that have experienced victimization by cybercriminals and the other seven (7) have experienced personal cases of victimization on cyber space (Table 1).

#### *5.1.1. Table of selected study sample*

**Table 1. The selected study sample**

| South African Police Services (Directorate for Priority Crime Investigation): Commercial Crimes Unit Officials (IDIs) | Bowline Security Employees: Cybersecurity and ICT (IDIs) | Members of the Durban Community: Business and Ordinary Citizens (KIIs) | Total |
|---|---|---|---|
| 4 (Detectives) + 3 (Investigators) = 7 | 3 | 10 | 20 |

### *5.2. Sampling procedures*

The selection of participants of this study was conducted using two sampling methods: Purposive sampling and Snow ball sampling. Purposive sampling allowed for maximum variation, which was looking for participants who had different ideas concerning the topic and broad range of experience from each other. This was used to pick participants from the SAPS DPCI and Bowline Security, as these participants are knowledgeable about cybercrimes in Durban. Snowball sampling or chain sampling, is a type of sampling where the researcher gets help from one participant to another. The choice of the participant is guided by the aims and objectives of the study. This method was used to select members of the community who have been victims of cybercrime to ensure that the participants are aware of the phenomenon to be studied.

### *5.3. Data collection techniques*

The study required the participants to be able to express their views and perceptions freely, therefore, it utilised interviews to collect data. Interviews are a method of gathering information through oral transformation using an interview schedule. Shneiderman and Plaisant (2005, p. 314) highlight that using interviews has the following advantages:

- They allow for the obtaining of detailed information.
- Direct contact with the participants leads to specific and constructive suggestions.
- Interviews require a small number of participants to gather rich and detailed data.

The study used a semi structured interview schedule as it allowed the researcher to use the schedule that is pre-planned, and it allowed for elaborate discussions between the participants and the researcher. The interviews where in-depth and done on a one on one this was done to illicit detailed information. The interviews took place at locations that were chosen by the participants and the duration ranged from 20–40 minutes, this was dependent on how much information the participants were willing to share. Overall, the data collection was done over a period of eight (8) weeks.

### *5.4. Data analysis*

Thematic analysis is a method for identifying, analysing and reporting patterns (themes) within data as it organises and describes data in detail (Braun & Clarke, 2006). At the heart of thematic analysis, the familiarisation of data by the researcher is important. Data familiarisation was possible because the researchers personally conducted audio-recorded interviews and transcribed them. This process allowed the researchers to familiarise with the data for an expedited and insightful analysis.

Following this thematic transcription, the scripts were analysed using NVivo version 8 software. This software organised the raw data so that it was possible to link and compare thematic issues within and across documents. The list of “starter nodes” was generated from an initial entry in a project journal in the software where the questions and assumptions brought to the report were outlined. The software gave results that allowed for a deeper examination and management of the qualitative data that might not be possible in traditional coding.

Two distinct types of coding were used in the analysis. The first was *descriptive coding*, which described the cases in the study. This process related both to the coding of information in categories and the creation of attributes to clarify them. The second type *was analytical coding*, which was done by selecting source content to interpret and reflect on the meaning of the data to arrive at new ideas and categories. The process entailed gathering material that could be re-thought and reviewed given the growing understanding of the inter-relationship of the categories in the data.

## 6. Findings and discussion

Data interpretation was conducted with the purpose to establish how the SAPS, private sector and members of the Durban community understand cybercrime. It also sought to explore the policing of cybercrime and understand the challenges that hinder the effective and efficient policing of cybercrime.

### *6.1. Understanding cyber-crime*

The Electronic Communication and Transaction Amendment Act of 2012(1)(o) states that cybercrime "any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them". However, understanding what constitutes a cybercrime is important in the policing of cybercrime. The participants indicated the challenges of understanding cybercrimes amongst members of the Durban community (the end user) pose a great challenge in the policing of cybercrime. According to a participant in an in-depth interview:

> *"My opinion is that the policing of cybercrime is basically the application of law enforcement into the prevention of cybercrime. I think that the police do not have the necessary resources and skill to adequately do this job. Policing does not only rest in the hands of the police although the police should be doing more but we as a community also need to assist. Another problem is actually understanding what is a cybercrime, the only time I was able to understand what is a cybercrime is when I became a victim but other than that we are oblivious to these things."*

### *6.2. Awareness*

This has an impact on the general awareness of cybercrime amongst South Africans. The lack of strategy relating to creating awareness is one of the problems confronting the policing of cybercrime in Durban. There is a need to create public awareness about the dynamic nature of cybercrimes to avoid victimisation. The strategies implemented in Durban to police cybercrime lack proper planning and contribute towards the escalation of crimes of this nature. Considering the responses of the participants, they indicated that the awareness concerning cyber-crime is limited:

> *"We all have joint responsibility to raise awareness, cybercrime is a crime that effects each and every individual. We live in a society where we all practically live on the internet. The SAPS, SABRIC and Government departments need to work together to raise awareness for people to be aware of cybercrime or for them understand what cybercrimes are."*

### *6.3. SAPS and private sector relationship*

Another challenge that was expressed by the Durban SAPS DPCI, was that private sectors and members of the community in Durban were more severe than had been anticipated. This seemed to be exacerbated by an ineffective relationship between the SAPS DPCI and private sector. The private sector has the necessary resources and skills to police cybercrimes. To address these challenges there needs to be a cooperative relationship between these sectors to mitigate the deficiency of skills and resources surrounding the policing of cybercrime in Durban. This study shows that policing cybercrime is the responsibility of everyone who has access to the internet. According to a participant in an in-depth interview:

> *"The police officials do not have adequate skills and knowledge to prevent cybercrime. Only a few of the police officials possess the necessary skills required to investigate cybercrime. Police at local stations lack the experience in handling cyber related crimes. Only few units of the South African Police are trained and the lower ranks still lack experience."*

### *6.4. Strategic partnership*

Crime prevention and the role of the community in South Africa can be ascertained through the following: "community-based crime prevention assumes by creating the perception among potential offenders that the risk of being caught is high in a specific neighbourhood or environment" (Graham, 2013, p. 29). Therefore, the literature that was consulted and the responses supra revealed strategic partnerships between the public and the private sector play a vital role in policing the occurrence of cybercrime in Durban. However, the participants felt that the SAPS bear a greater responsibility to police cybercrimes:

> *"When it comes to solving any crime we as the police need the community to bring proper and effective policing into life. The biggest problem is that people do not report these crimes. We as police work a lot with tip-offs or informers to help solve crimes. When there is suspicious activity on the internet people are quite they do not say anything. These tip-offs are very important to us as they help us identify perpetrators. Then from here we can find people who are working for cybercrime syndicates. We need to understand as police and the community that the DARK WEB is operated by people who are not elite from the law and we need the communities help to catch these people."*

The SAPS needs to train more officials around cybercrime prevention, investigation, prosecution/adjudication and sentencing, in doing so, the officials would be one step ahead of cyber related criminals. The participants indicated that measures to curb the challenges of policing cybercrime in Durban were of poor quality. This advocates for the need for more innovative and proactive programmes that will assist the prevention of cybercrimes. Hence, "cybercrime prevention programs should be properly planned, especially now that recent innovation and technological advancements have added shifts in the method of orchestrating criminal activities such as the crimes committed in the cyber system" (Longinus, 2014, p. 55). The above provision will provide innovative policing of cybercrime because cybercrime is dynamic in nature

These problems reinforce the need for the SAPS DPCI in Durban to be better equipped to gather evidence of the commission of this crime. They should able to prepare and address some myriad issues related to the examination of both physical and digital evidence. This requires specialised cybercrime forensic experts' efforts and computer forensic investigations to maintain a proper chain of custody. Cybercrimes change constantly, and cyber criminals are highly skilled, hence end-users should be taught how to protect themselves from cyberattacks. Like any other criminal activity, those most vulnerable tend to be the first targeted. Hence, working with Cybersecurity and ICT security expert to assess needs and vulnerabilities will assist in the prevention of cybercrime.

## 7. Conclusion and recommendations

In conclusion, the aim of this paper was to suggest evidence based strategies to improve the policing of cybercrime and the effectiveness and efficiency of the mechanisms in place to police cybercrime within a South African context. From the above discussion it is evident that to address the challenges associated with policing of cybercrime in Durban, the SAPS DPCI should conduct fragment cybercrime investigations in collaboration with relevant stakeholders (i.e., SABRIC, SARS and Cybersecurity and ICT companies). This should help in identifying improper conduct by cybercriminals to stop the commission of this crime, help in the facilitation of recovering losses, mitigate other potential consequences, and strengthen internal control weaknesses in other relevant organisations, among others.

### *7.1. Recommendations*

It is noteworthy to address members of the society to be aware of the activities cyber systems, online, computer networks, mobile networks and social network sites. South African inhabitants have been targeted from syndicates across the borders. Therefore, proactive strategies and measures are needed to tackle this problem. It is necessary to sensitise the community, government, big and small organisations and members of the society to join hands in seeking a lasting solution to the problem of cybercrimes in South Africa.

The results of this study might serve as an intervention tool to assist the effective policing of cybercrimes. In addition, it is also believed that this study could provide insight into the management teams of these stakeholders. For the creation of a platform that will initiate, develop and implement intervention measures to combat, if not eradicate, cybercrime. The following recommendations are made regarding the effective policing of cybercrimes:

### *7.1.1. Specialised training for police officials*

Once police officials become experts or specialists in cybercrime, they leave the service to join the private sector as it provides more security of tenure. In addition, the private sector allows cybercrime specialists to hone their skills and knowledge, as resources are readily available, unlike within the police service were resources are scarce. It is recommended that policing cybercrime skills be developed. The police need to be continuously trained always within a cybercrime specific framework. However, training itself is not enough, as those who are already working within the cybercrimes unit constantly need top-up skills, to increase their contribution towards the policing of cybercrime.

### *7.1.2. Effective awareness programmes*

The creation of effective cybercrime awareness programmes will enhance community participation in the policing of cybercrimes in Durban. Cybercrime awareness campaigns must be designed specifically for the audience you are trying to reach, and participants must leave the training with clear instructions on the next steps to take. Those steps must be simple and manageable enough to be embraced, and organizations should follow up with awareness programmes participants to gather feedback on how the process is going and where assistance is needed. This will give end-user a proper understanding of the phenomenon and allow them to make positive contributions towards policing cybercrime.

### *7.1.3. Effective strategic partnerships and cooperation*

Certain tools already exist in the form of laws, conventions, private-sector industry initiatives and information-sharing platforms. However, this does not suffice, as cybercrime cannot be combated by acting unilaterally. Instead, the public and private sectors must combine forces to find mutually convenient ways of dealing with this phenomenon. South African inhabitants have been targeted from syndicates across the borders; members of the society have experienced various attacks personally, in their businesses and infrastructures (including the government). Therefore, proactive strategies and measures are needed to tackle this problem. Closer collaboration among role-players, formal and informal information exchange, community policing, and training requirements should be pivotal research topics in future research projects that will endeavour to contribute to the discourse on the policing of cybercrime locally and internationally.

**Funding**
The authors received no direct funding for this research.

**Author details**
Siyanda Dlamini[1]
E-mail: sdlamini@ufh.ac.za
ORCID ID: http://orcid.org/0000-0002-1110-8418
Candice Mbambo[2]
E-mail: cmbambo@sasseta.org.za
[1] Criminology Department, University of Fort Hare, Alice, South Africa.
[2] Research Department, Safety and Security Sector Education & Training Authority, Johannesburg, South Africa.

**Citation information**
Cite this article as: Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses, Siyanda Dlamini & Candice Mbambo, *Cogent Social Sciences* (2019), 5: 1675404.

**References**

Booysen, K. (2011). Economically motivated crimes: An overview. In C. Bezuidenhout (Ed.), *A Southern African perspective on fundamental criminology* (pp. 143–170). Cape Town: Pearson Education.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*, 77–101. doi:10.1191/1478088706qp063oa

Cole, B. (2013). Cybercrime is real and it's here. *iol News*. Retrieved from https://www.iol.co.za/news/cybercrime-is-real-and-its-here-1583736

Council of Europe Convention on Cybercrime. (2001). Retrieved fromwww.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv.. · PDF file [Accessed 2017/09/05].

De Angelis, G. D., & Sarat, A. (2000). Cybercrimes. In S. Sissing (Ed.), 2013. *A criminological exploration of cyberstalking in South Africa*. Pretoria: University of South Africa. Retrieved from https://uir.unisa.ac.za/hdl.handle.net/10500/13067/

Fin, O. (2015). Cybercrime and punishment: The Russian Mafia and Russian responsibility to exercise due diligence to prevent trans-boundary cybercrime. *Brigham Young University Law Review*. *5*(1), 177–184.

Graham, E. (2013). *Community policing in indigenous communities*. (K. N. Mahesh & R. N. Greame, eds). Parkway, NJ: CRC Press.

Higgins, G. E. (2010). *Cybercrime: An introduction to an emerging phenomenon*. New York, NY: McGrawHill.

Hui, K., Kim, S. H., & Wang, Q. (2017). Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *Information*

*Systems Research*, *28*(1). Retrieved from http://dx.doi.org/10.1007/s10796-011-9339-4

Kader, S., & Minaar, A. (2015). Cybercrime investigations: Cyber-process for detecting cybercriminal activities, cyber-intelligence and evidence gathering. *ACTA Criminologica*, 4(6), 123–134.

Lievrouw, L., & Livingstone, S. (2014). *Handbook of new media: Social shaping and social consequences*. Arnold: London.

Lilley, P. (2002). *Hacked, attacked, and abused: Digital crime exposed*. London, U. K: Kogan Page Limited.

Longinus, E. C. (2014). Combating cyber related crime in South Africa. Magister Technologie Dessertation. Pretoria: Tshwane University of Technology. Retrieved from https://core.ac.uk/display/50982867 [Accessed 2018/09/04].

Mahlobo, D. (2015). Cyber security as a major challenge. *Parliament Reports South Africa* Retrieved from https://www.ujuh.co.za/david-mahlobo-on-cyber-security-as-a-majorchallenge/

Maughan, G. (2007). *Understanding cybercrime: Phenomena, challenges and legal Sector*. Available from: https//ity.int/ITUD/cybersecurity/docs/cyber-crime%20legislation%EVG.pdf [Accesed 2017/11/07]

McNamara, K. (2012). The high cost of cybercrime. *ExpertIP*. Retrieved from https://allstream.com/study¬-the-high-costs-cybercrime

Minaar, A. (2016). Crackers', cyberattacks and cybersecurity vulnerabilities: The difficulties in combatting the 'new' cybercriminals. *Acta Criminologica: Southern African Journal of Criminology*. Special Edition No. 2

Nappinai, N. S. (2010). Cyber crime law in India: Has law kept pace with emerging trends? An empirical study. *Journal of International Commercial Law and Technology*, *5*(1). Retrieved from www.jiclt.com/index.php/jiclt/article/view/97

Oladipo, T. (2015). Cybercrime is the next big threat experts warn. *BBC Monitoring African Security Correspondent*. Retrieved from https://bbc.com/news/world-africa-34830724/

Rifkind, J. (2011). *Cybercrime in russia*. Utah: Brigham Young University Law Review.

Shneiderman, S. B., & Plaisant, C. (2005). *Designing the user interface* (4th ed.). Boston, MA: Pearson Addison Wesley.

Sissing, S. (2013). *A criminological exploration of cyberstalking in South Africa* (Master of Arts Dissertation). University of South Africa, Pretoria. Retrieved from https://uir.unisa.ac.za/hdl.handle.net/10500/13067/

Symantec. (2016). *Internet security threat report* (Vol. 8). Mountview, USA: Author. Retrieved from https://www.insight.com/content/dam/insight/en_US/pdfs/symantec/symantec-corp-internet-security-threat-report-volume-18.pdf

United Nations Office on Drugs and Crime (UNODC). 2013. Available from https://www.unodc.org/unodc/secured/wdr/wdr2013/World

Van de Merwe, K. (2015). *Cybersafety, cellphone security and rotten apps. Cited in South African police services. 2015. Police: 20 years of policing in a democracy*. Pretoria: SAPS.

Van Zyl, G. (2016). *Why Anonymous Hacked the SABC, Gupta websites*. Fin24tech. Retrieved from https://www.fin24.com/companies/financial-services/anonymous2016061244. [Accessed 2018/08/28].

Von Solms, B. (2015). *What is SA doing to tackle cybercrime. The conversation*. University of Johannesburg. Retrieved from https://www.fin24.com/Tech/Opinion/What-is-SA-doing/

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity Press.

Widsup, S., Spitter, M., Hylender, D., & Basset, G. (2018). *Verizon data breach*. Investigations report. Retrieved from https/www.researchgate.net.publication/32445340_2018-verizon-data-breach-investigationreport [Accessed 2017/11/06].