



Investigating the Cybersecurity Threat Landscape for Botswana

by

SAREFO SETH MOSIMOLODI

Reg. No: 18100008

BSc Honors Computer Systems Engineering (University of Sunderland)

Department of Computer Science and Information Systems,
Faculty of Science,
Botswana International University of Science and Technology
Ss18100008@studentmail.biust.ac.bw

A Thesis Submitted to the Faculty of Science in Partial Fulfilment of the Requirements for the Award
of the Degree of Master of Science in Computer Science of BIUST

Supervisors

Dr Banyatsang Mphago

Computer Science and Information Systems,
Faculty of Science
BIUST

mphagob@biust.ac.bw

Signature: _____

Date: 24/06/2022

Professor Maurice Dawson

Assistant Professor of ITM, Director Center for
Cyber Security and Forensics Education
Illinois Institute of Technology

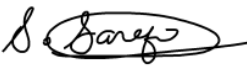
mdawson2@iit.edu

Signature: _____

Date: 24/06/2022

DECLARATION AND COPYRIGHT

I, **SETH MOSIMOLODI SAREFO**, declare that this thesis is my own original work and that it has not been presented and will not be presented to any other university for a similar or any other degree award.

Signature 
24/06/2022

This thesis is copyright material protected under the Berne Convention, the Copyright Act of 1999 and other international and national enactments, in that behalf, on intellectual property. It must not be reproduced by any means, in full or in part, except for short extracts in fair dealing; for researcher private study, critical scholarly review or discourse with an acknowledgement, without the written permission of the office of the Provost, on behalf of both the author and the BIUST.

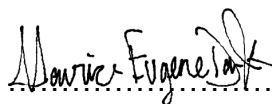
CERTIFICATION

The undersigned certifies that he/she has read and hereby recommends for acceptance by the College of Science a thesis titled: **INVESTIGATING THE CYBERSECURITY THREAT LANDSCAPE FOR BOTSWANA**, in fulfilment of the requirements for the degree of Master of Science in Computer Science of the BIUST.



.....
Dr Banyatsang Mphago
(Supervisor)

Date: . 24/06/2022.....



.....
Prof Maurice Dawson
(Co-Supervisor)

Date: 24/06/2022.....

ACKNOWLEDGEMENTS

I thank Professor Maurice Dawson for his guidance and the faith that he had in my work. His dedication to this work and his contributions to the entire cybersecurity field was always an inspiration for me. It was both fun and exciting to work with him and I always found his advice to be wise and insightful. He is the best in the world. His openness in sharing knowledge was also a huge game changer for me. This thesis would not have been a success without his expertise and support.

I also thank my other supervisor Dr Mphago for his support.

And to all the others who supported me, my family, friends, and well-wishers, I cannot think of a better way to say thank you than to put it in Nigel Amos's words at the 2020 Tokyo Olympic games when he said:

"I felt all the support and love and saw all the well wishes... I am proud to have experienced it with you all. Tomorrow is another day. Another day for me to be better than I was yesterday. Now it's time for me to regroup and move forward on to the next step.

Peace and love to all who supported me".

God bless!

DEDICATIONS

To my Parents, for your sacrifices and undying support kept me going. My soon to be wife and son. And to my siblings, nephews and nieces.

Blank page

ABSTRACT

Movement restrictions introduced by the coronavirus pandemic have incentivized the rollout of online services globally. Additionally, more employees were telecommuting throughout the pandemic and remote work has become the new normal. This has provided nefarious actors with lucrative opportunities. Hence there has been an increase in online criminal and terrorism activities. The weaponization of the cyberspace is also a concerning trend in the ongoing geopolitical tensions. This is because states see the cyberspace as a tool for engaging in asymmetrical warfare. In Botswana, government services are being transitioned to online services through the digital transformation strategy. As a result, the cyber-attack surface area in Botswana has also increased. Botswana has establishments for mitigating the impact of cyber-attacks such as the Computer Incidents Response Team (CIRT) and the Digital Forensic Lab. However, there is a lack of publicly available empirical datasets on the occurrence of cyber threats in the country. Such a dataset is important for organizations, and individuals to benefit from the knowledge shared by the broader community on threats and their mitigations. This study therefore investigated the cybersecurity threat landscape for Botswana by analysing the threats, countermeasures and cybercrime legislation. Data triangulation and exploratory data analytics were the methods used for data collection and analysis in this study. The data sources were a United Kingdom (UK) cybersecurity incidents dataset, a questionnaire, online articles, and government documents and speeches. Findings in Botswana were also compared to South Africa and the UK. This dissertation concluded that the cyber threats in Botswana are similar to those identified in developed countries and regional countries. As such strengthening already existing cooperative measures with cybersecurity stakeholders will help improve the cybersecurity posture of Botswana. Other cybersecurity measures that have potential for growth are organizational and technical measures.

Table of Contents

ABSTRACT	1
1. INTRODUCTION	4
1.1 Problem Statement.....	5
1.2 General Objective	6
1.3 Specific Objectives	6
1.4 Research Questions	6
1.5 Hypothesis.....	7
1.6 Significance of Study	7
2. LITERATURE REVIEW.....	8
3. BOTSWANA CYBER LANDSCAPE	29
4. METHODS.....	43
4.1 Data Collection	43
4.2 Data Analysis	45
4.3 Dataset pre-processing and cleaning	45
4.4 Web and Document Scraping.....	46
5. RESULTS	47
5.1 UK Dataset Analysis.....	47
5.2 Botswana Questionnaire Results	53
5.3 Online Discussions and Cybersecurity News in Botswana.....	62
5.4 Analysis of Cybercrime Acts.....	72

6.CONCLUSIONS..... 84

References..... 87

1. INTRODUCTION

Botswana is one of Africa's most stable and peaceful democracies with a sustained growing Gross Domestic Product (GDP) since independence in 1966 [1,2]. While Botswana enjoys peace and serenity, there has been some instabilities in the Southern Africa region [3]. An example is the ongoing war in Mozambique that is linked to the Islamic State of Iraq and Syria (ISIS) [4,5]. The recent spike of criminal and terrorism activity on the internet [6–8] is also concerning. This is because these threats require technical expertise that is still in short supply globally [8–12]. Additionally, cyber threats are not deterred by military guards' patrols along the national borderline as these crimes are borderless [13–15] [14]. Cyber threat actors also know how to conceal their identities successfully [13]. As such cybercriminal activities have the potential to unsettle the peace and security in a state if they go undeterred [16–18]. With the ongoing geopolitical power tensions, states see the cyberspace as an opportunity to achieve such objectives using asymmetrical warfare tactics [19–22]. This means that threat actors now include well-resourced entities that are backed by states with capabilities to cause widespread damages.

Cyberattacks increase during pandemics and crisis situations such as the Coronavirus outbreak [23–25]. This is because criminals take advantage of people's fears that are brought by the uncertainties of a crisis situation [6,26]. Movement restrictions introduced to mitigate the spread of the coronavirus, have motivated the delivery of everyday services through online platforms. These services cover multiple domains such as digital currencies, social movement, government elections, learning and culture [27]. As a result this new normal has increased the attack surface and cyber risk in Botswana.

The ongoing cyber threat in Botswana has been displayed through social media manipulation, and attacks on essential services in nearby countries such as South Africa [28–30]. These services such as online banking, citizens of Botswana are dependent upon. In 2016 Botswana was number 8 on the Top 10 Source African countries for Attacks [7]. According to the report Botswana accounted for 37,880 incidents in 2016 [7]. An investigation by [8] also revealed that there is a shortage of skillsets in cybersecurity in the country. At the same time, attracting foreign

workers is still a problem. Botswana has been mainly focused on investing in mining diamonds, tourism, and agriculture as these are the main contributors to GDP [31]. As such, in 2018 Botswana only had 250 professionals with certifications in the cybersecurity area [8].

Botswana continues to invest in Information Communications Technologies (ICTs) as this will create employment for the youth. However, there is potential for Botswana to improve its cybersecurity initiatives, especially in its technical measures and cooperative measures [32]. The national cybersecurity strategy is at a high-level concept and needs to be further developed. This is necessary so that the engineers can implement security controls into their systems. The recent Presidential Directive 30(B)/2020 to approve the strategy indicates strong commitment by the government to continue investing in cybersecurity initiatives. This is because alignment of the executive branch of government to the strategy is important for its successful implementation [33].

The International Telecommunication Union (ITU) measures the commitment to cybersecurity initiatives by states using the Global Cybersecurity Index (GCI) [32]. The GCI is based on six pillars and these are legal measures, technical measures, organizational measures, capacity development measures, and cooperative measures [32]. Botswana ranked 5th in the Southern Africa region [32]. The country also showed relative strength in its legal measures. With the recently established national Computer Incidence Response Team (CIRT) and Digital Forensic Lab, Botswana will be better positioned to mitigate cyber threats. As such information sharing and cooperation between government, private sector, and international organisations is of paramount importance in the cybersecurity response.

1.1 Problem Statement

There are opportunities for improving cybersecurity technical measures and stakeholder collaboration in Botswana [32]. The problem however is that there is a lack of publicly available information on cybersecurity incidents in Botswana. This is an obstacle to proactive, reactive and potentially offensive cybersecurity countermeasures. Cybersecurity depends on timely and actionable information about threats and strategies needed to successfully combat them [34]. As such

organizations in Botswana can benefit from timely alerts on threats shared by the CIRT. This will improve their situational awareness and defensive agility [34]. It is therefore important to investigate the cybersecurity threat landscape for Botswana and identify strategies that can be used to mitigate them. This study builds on the information and intelligence developed by other countries regionally and internationally.

1.2 General Objective

- ❖ The main objective of this study is to investigate the cybersecurity threat landscape for Botswana by analysing cybersecurity threats, countermeasures, and the cybercrime legislation in Botswana. To avoid mirror imaging the abilities of threat agents to our abilities here in Botswana, a dataset from publicly available data on cybersecurity incidents in the UK was also analysed. Additionally, the South African Cybercrime Act of 2020 and the United Kingdom's (UK) Computer Misuse Act of 1990 was analysed alongside the Botswana Cybercrime Act of 2018.

1.3 Specific Objectives

- ❖ To analyse a cybersecurity incidents dataset from the UK.
- ❖ To conduct a questionnaire on the cybersecurity threats and strategies in Botswana.
- ❖ To analyse data collected from the questionnaire.
- ❖ To analyse online news and posts related to cybersecurity in Botswana.
- ❖ To compare cybercrime acts from Botswana, South Africa, and UK.

1.4 Research Questions

- ❖ RQ 1: What are the cyber threats and strategies observed in the UK?
- ❖ RQ 2: What are the cybersecurity threats and strategies in Botswana compared to the UK?
- ❖ RQ 3: How do cybercrime acts in Botswana, South Africa and the UK compare to each other?

116 1.5 Hypothesis

- 117 ❖ HY 1: Cybersecurity threats and strategies analysis in a developed country
118 such as the UK, with an advanced CIRT will reveal trends that less
119 developed nations like Botswana should look out for.
- 120 ❖ HY 2: An analysis of threats and strategies in a country with a less developed
121 CIRT such as Botswana will reveal gaps in cybersecurity responses
122 compared to the UK.
- 123 ❖ HY 3: Analysis of cybercrime legislation from the three countries will reveal
124 some areas where Botswana can improve its cybercrime law.

125 1.6 Significance of Study

126 Well-timed information on threats and their mitigations increases situational
127 awareness. This facilitates coordinated responses to cybersecurity incidents. This
128 study provides a horizon scan of the cyber threat landscape for Botswana.
129 Botswana does not have publicly available datasets on cyber threats. Therefore this
130 dissertation draws from information collected from a questionnaire on cybersecurity
131 in Botswana. Online reports on cybersecurity related activities in Botswana, and a
132 publicly available dataset on cyber incidents from the UK is analysed. The
133 Botswana national cybersecurity strategy of 2016 [35] identifies cybercrime
134 legislation as one of its strategy for cybersecurity. As such the cybercrime act of
135 Botswana is analysed and compared to similar legislation in South Africa and the
136 United Kingdom. The findings of this study will go a long way in increasing
137 situational awareness and threat intelligence. As such this study is beneficial to the
138 cybersecurity industry in Botswana as it adds to the body of knowledge. The
139 recommendations of this study can be used to inform decision-making at both policy
140 and implementation levels. Additionally, this study helps to mitigate new threats
141 such as criminal activity and terrorism activity that have seen significant growth on
142 the Internet [6–8,36–38].

2. LITERATURE REVIEW

2.1 Cybersecurity

The National Institute of Standards and Technology (NIST) defines cybersecurity as the ability to protect or defend the use of cyberspace from cyberattacks [39]. It includes the process of detecting cyberattacks, prevention of damage to, and restoration of electronic devices, systems and communication, including information contained therein, to ensure confidentiality, integrity, availability and nonrepudiation [39]. Some authors have observed the differing contexts in the definitions of cybersecurity in the literature [40–44]. Schatz et al. [40] argued that the term is used broadly and sometimes can become confusing. Craigen et al. [41] argued that the definition should be domain neutral to accommodate the interdisciplinary nature of cybersecurity. On the other hand, Bay [45] argued that the broadness of the term is appropriate due to the multifaceted disciplines and challenges of cybersecurity. As such [40] provided a representative definition of cybersecurity to provide professionals with a substantive understanding of the term. The authors used exploratory text analytics to analyse the lexical and semantics of the term in authoritative and peer reviewed sources. A high word count was taken to correspond to a high significance of the word. Words such as “system”, “risk”, “use”, “process” and “protect” were identified as of high importance [40]. This process led to the construction of the definition of cybersecurity as follows:

“The approach and actions associated with security risk management processes followed by organisations and states to protect confidentiality, integrity and availability of data and assets used in the cyberspace. The concept includes guidelines, policies and collections of safeguards, technologies, tools, and training to provide the best protection for the state of the cyber environment and its users [40].”

Craigen et al. [41] constructed their definition by augmenting definitions in the literature with the views and opinions of multidisciplinary professionals in the cybersecurity field. Their definition was not different from the one in [40] as it utilised some of the terms that [40] identified as of high significance in defining cybersecurity. Galinec et al. [42] also studied cybersecurity strategy at the national

level. The authors defined cybersecurity as an umbrella term encompassing Information Technology (IT) security, (Operational Technology) OT security, and information security. The authors adopted a definition for cybersecurity that incorporates offensive security i.e., attacking the adversary's targets. Other related definitions of cybersecurity that are defined in [42] are stated below:

- (1) Information warfare – Applying psychological operations through propaganda and misinformation techniques, usually done to manipulate and persuade public opinion [42,46,47].
- (2) Cyberwarfare – The use of cybersecurity capabilities in a warfare context. This is usually carried out using asymmetric tactics and sometimes states sponsor underground criminal groups to achieve this objective [42,48,49].
- (3) Cyberterrorism – The use of cybersecurity capabilities for terrorism activities. In this instance a terrorist may not have to cross the physical borderlines into the target nation [42,50].
- (4) Cybercrime – The use of IT tools for criminal activities and it may not be related to cybersecurity [42,51]. The cyberspace mirrors the physical world in that crimes can be committed in it and through it.
- (5) Cyber defence – The provision of assurance in a cyber network by use of network defence mechanisms such as response to actions and critical infrastructure protection and information assurance [42,52,53].
- (6) Active Cyber Defence (ACD) – The United States (US) Department of Defence (DoD) has defined this new term ACD, to refer to the synchronized, real-time capability to discover, detect, analyse, and mitigate threats, and vulnerabilities [42,52,53].
- (7) Advanced Persistent Threat (APT) – The term originally was used to refer to cyber-attacks that were supported by the government of China [42,54]. But the term is now used broadly to refer to sophisticated and stealth programs that are custom designed by threat agents of high capability. These threat agents have the ability to infiltrate networks and lurk in the system for months or years [27,42,55,56]. This type of a threat usually covers all the phases in a cyber kill chain.

204 2.2 Cyber Threat Landscapes

205 NIST [57] constitutes risk into three parts. These are the likelihood of a potential
206 vulnerability, possibility of a threat exploiting the vulnerability, and impact of
207 successful exploitation. The cyber threat landscape is a collection of potential and
208 identified cyber threats in a particular domain or context [58–60]. This information
209 may include the vulnerable assets, threat risks, threat actors, geopolitics among
210 many factors to consider [58,59]. The cyber threat environment is made up of
211 internet service providers (ISPs), government organisations, private sectors, law
212 makers and military all forming the emerging cyber regime complex [34]. This threat
213 environment dynamically changes due to factors such as increased complexity of
214 technology, new products and sophistication of attacks [58,59]. External factors
215 such as global pandemics also contribute to the threat environment [58,59].
216 Understanding the threat landscape is important as it helps to plan the cyber
217 defences and mitigations to threats [61]. Cyber threat landscapes have been
218 investigated by different organisations throughout the Coronavirus pandemic
219 [56,61,62].

220 The European Agency for Cybersecurity identified nine prime cybersecurity threat
221 categories [61]. These are ransomware, malware, email related threats,
222 cryptojacking, threats against data, threats against availability and integrity,
223 misinformation – disinformation, non-malicious threats, and supply chain attacks
224 (See Table 1) [61]. The threat actors identified by [61] were predominantly state
225 sponsored actors, cybercrime actors, hacker for hire actors and hacktivists. In
226 addition to the threats identified in [61], Advanced Persistent Threat (APT) was also
227 identified as a threat that should be on the watch-out for [56]. The potential role of
228 attackers using Artificial Intelligence (AI) and machine learning in carrying out
229 attacks has also been highlighted [56]. Other trends in the year 2021 included
230 attacks targeting a popular Java library called Log4j and an increase in Linux based
231 malware [62]. Attackers also intensified their aggression and sophistication in
232 ransomware attacks [62]. Exploits targeting Microsoft Exchange Server were also
233 experienced by many organisations [62]. Finally, attacks targeting remote access
234 flaws in baby monitors also intensified [62]. Table 1 summarises the threat
235 categories discussed here.

Threat	Description
Ransomware [6,56,61]	Ransomware is a type of malicious code that encrypts the victim's data or device [61–64]. The attacker does not decrypt the data until the victim pays the attacker usually through cryptocurrencies [61–64].
Malware [6,56,61]	Malware is categorised as software that performs an unintended effect on a computer that compromises the confidentiality, integrity and availability of a system [61,65,66].
Email related [6,56,61]	These are threats that use emails to compromise the user's psyche and habits [6,61]. These usually take the form of coercive and intimidating messages. The messages are meant to lure and persuade the user to taking action that can be harmful to them. Successful email attacks can lead to theft of information, installation of malware and financial losses.
Threats against data [56,61]	This threat includes stealing data and leaking it online. Data leaks occur as a result of cyber-attacks, insider job and unintentional exposures [61,62].

Threats against availability and integrity [56,61]	These are attacks that target the availability and integrity of data such as denial of service and web attacks [61].
Misinformation – disinformation [56,61]	This group of threats involves the propagation of fake news and propaganda. It is also used in hybrid attacks to coerce and persuade victims [61,67].
Cryptojacking [56,61]	This type of threat is when bad actors use a victim's computing resources to mine cryptocurrencies without the knowledge of the victim [61,68].
Non-malicious threats [6,61]	These threats result from human and system errors and do not result from malicious intent [61]. System errors and misconfigurations are some of the most recurrent cyber threats [61,69].
Supply chain attacks [56,61]	This attack targets supplier vulnerabilities. It takes advantage of the trust people have on their suppliers. The attack targets both the supplier and customer and its effects can be cascaded to more than two targets in cases where there are multiple suppliers and customers along the chain [61,70].

Advanced Persistent Threats (APT) [56]	APT refers to a highly sophisticated type of attack on a target that persists for long periods possibly months and years. This attack has the aim of gathering information on the target and possibly causing financial harm and other damages [55,56].
--	---

Other works have also investigated the cybersecurity threat landscape in other contexts. Carter [71] investigated the forces influencing the cyber threat landscape for financial institutions. The study considered the changing environment of tools used by criminals and new technologies in financial institutions. Attacks in this sector include bank card fraud, point of sale fraud, crypto-ransomware, phishing attacks, mobile banking malware, business email compromise, insider threats and banking application attacks [71–73]. With financial institutions making larger investments in cybersecurity programs, attackers are also going for the institutions' core networks. Developing markets with low levels of cybersecurity awareness and cyber defences such as Asia, Latin America and Africa have also provided cyber-criminals with growing opportunities [71]. Attackers have also been reported to be using multiple attack vectors. An example is using multiple methods of Distributed Denial of Service (DDoS) and ransomware. Carter [71] also observed a growing trend whereby state actors are also developing offensive cyber capabilities targeted at financial institutions.

Pour et al. [74] also investigated the potential of internet-wide attacks based on Internet of Things (IoT) devices by characterising internet scale probing techniques. The authors proposed a near real-time threat alert system based on a dimensionality reduction technique and greedy search algorithm. The characterisation of the alerts was based on the industry or sector hosting the IoT device, IoT manufacturer and IoT device type [74]. The data in their study was from a globally routed /8 network telescope (passive data) as well as port scanning data from the Shodan network (active data) [74]. The study revealed more than 120 000 vulnerable IoT devices including those operating in critical sectors.

Shad [75] investigated the cybersecurity threat landscape for Pakistan based on the principle of securitization. This characterisation involved representing the cybersecurity issue as an existential threat and requiring urgency and extraordinary measures [76,77]. The three modalities of securitization in the cyber domain are hyper securitization, everyday security practices, and technification [77]. Shad [75] concluded that Pakistan's reliance on the internet for governance and service delivery is only met by poor cybersecurity preparedness. Domestic and regional hostility such as the cyber skirmishes between Pakistan and India also pose a cyber threat [75]. This is so especially considering India's cyber offence policy. Hence the need for coordination between agencies, increasing awareness and taking advantage of the skilled human capital in the country [75].

Pieterse [78] also investigated the cybersecurity threat landscape for South Africa looking at incidents from 2010 to 2020. The threats were characterised based on the incident type, affected sector, perpetrator type, and motivation of attacker. South Africa does not have data on threats publicly available from government institutions [37,78,79]. As such the study relied on media sources reporting on the occurrences of cybersecurity incidents. The results of the study showed a growing trend in the number of reported incidents over the ten year period.

Jabbour et al. [80] discussed the threat component of risk in information systems by reviewing traditional threat models. The study introduced characterization of the threat along ten dimensions. The authors used an analysis of the Stuxnet [81] threat to illustrate their thought process. According to [80] a viable cyber threat is one that has three components which are capability (the skills and time of a threat agent to create adverse action against a target), access (remote, physical, or access-less), and intent which is assumed is present. Jabbour et al. [80] cautioned against attributing the same ideologies, cultures, and doctrines that we have to the adversary (mirror-imaging). The reason is that today's warfare has a wide spectrum from "asymmetric warfare to peer nation-state skirmishes. Chabinsky [82] also shared the same sentiment stating that the intents and capabilities of the enemies should not be underestimated. Therefore it is important that we are not limited in imaginations of the potential threat.

2.2.1 Summary

It has been shown in this section that there are various methods used for assessing the cybersecurity threat landscape. The choice of method used usually depends on the goal, resources and data available to the investigator [83]. For example, [78] relied on media sources to characterise the threat landscape for South Africa. This dissertation also had similar challenges whereby there was no publicly available empirical data on threats from government sources in Botswana. Hence to validate the findings of this study, multiple sources of data were used. Kshetri [84] recommended that future conceptual and empirical work should focus on comparing economy sectors facing cyber-attacks in African countries with those overseas [84]. Examining political, economic, and institutional determinants of cybersecurity is another important area to be explored [84]. Other approaches to data gathering in threat landscaping involves the use of Open Source Intelligence (OSINT) [61].

2.3 National Cybersecurity Strategy

The concept of a strategy finds its genesis in the military [85]. In the military a strategy is used to deploy military resources tactically with the goal of gaining victory against the enemy troops. Upon contact with the enemy, the strategy is implemented to adaptively employ military resources and means. Reconfigurations are adaptively used to optimise successful operation. A strategy uses the best possible way of reaching the desired goal considering the available resources [86]. In the organizational/business realm the military resources are the organizational resources. The business environment within which the organization operates can be represented by the enemy in the battlefield. A strategy then can be thought of as a roadmap for a plan. It sets out how an organization would position and employ its resources to meet its objectives [85]. In other words, strategy is the ways, means and ends [33]. As such strategy specifies tactics for countering competitors or responding to changes in the business environment.

Schulman et al., [33] conducted a study on the United States (US) national technology strategy development process. The authors observed that a purposeful design of strategy development balances the trade-off between decision making

agility and stakeholder participation across the lifecycle [33,87]. At the same time the multiple intersecting and sometimes conflicting sub-processes which are internal, external, technical, and political have to be reconciled [33]. According to [33], common elements of any strategy model include self-assessment of existing tools, authorities, and their gaps; leadership alignment to strategic vision; assembly of the right talents to evaluate priorities and trade-offs; credible information to support analysis of trends, challenges, and opportunities; and a clear delegation of responsibilities for strategic elements.

The main objectives of a National Cybersecurity Strategy (NCS) are maintaining secure, resilient, and trusted electronic operating environment, promoting economic and social prosperity, promoting trust, business and economic growth, addressing risk of ICT and strengthening resilience of infrastructures [27]. The fundamental elements of an NCS are oriented towards legal, organisational, technological matters, cybersecurity professionals' development, public awareness as well as research and development (R&D) [27]. Establishment of a Computer Security Incident Response Teams (CSIRT), is one of the most common effective strategies against cyber threats [88]. However there are differences in how countries define priorities and quantification of threats [27,88]. Countries also demonstrate varying levels of the perception of cyber threats and security [88]. Differences are also observed in the perception of critical infrastructure.

The US is the best in global rankings in terms of its cybersecurity preparedness and programs [32]. The US was the first in the world to setup such a CSIRT in 1988 i.e., the Computer Emergency Response Team Coordination Centre (CERT/CC) [34] [89]. CSIRT teams are differentiated based on the level of skillsets and the funding that they comprise [34]. A CSIRT is responsible for assisting other organizations to mitigate cyber threats [90]. Bradshaw [34] categorised CSIRT teams into national, private, and technical or academic CSIRT.

National CSIRTs carry out the state's cyber defence policy, while private CSIRTs usually carry out a company or group of companies' cybersecurity responses [34] [90]. Technical/academic CSIRTs serve a non-governmental organisation such as a university and the Africa CERT is an example [34]. The Forum of Incident Response and Security Teams (FIRST) has a global scope with its membership

including over 600 CSIRTs around the world [91]. However representation from Africa is limited [34]. A CERT's scope of work includes reactive services, proactive services, artefact handling services and security quality management services [34] [90]. Considering the resources available to a nation, a national CSIRT's budget should meet needs of its constituents [90]. Additionally it should have skillsets that match its responsibilities [90].

As observed by [92], implementing a CSIRT team has its challenges. Poor information sharing and cooperation have been identified as some of the challenges faced by CSIRTs [92]. Some CSIRT teams lack a self-assessment mechanism. Other challenges include neglect of strategic objectives while focusing on technical capabilities for business continuation [92]. Bradshaw [34] identified a number of issues that may be the reason for the complexities that are in the way of cooperation efforts. These include commercialisation of cybersecurity and commodification of vulnerabilities such as zero-day exploits. States are also recognising the internet as a new domain to exert power and control (geopolitical power through state developed malware) [34]. As such state actors are hoarding knowledge. CSIRT teams also consist of diverse members with distinct and sometimes divergent laws, interests, and cultures. The legal issues preventing organisations and CSIRT teams from sharing data include liability for financial loss, reputational damage, privacy laws and jurisdiction issues such as data localisation laws [34]. Some countries also do not have trade secret laws for protecting the sharer's intellectual property rights [34]. [92] also observed that some CSIRT members do not want their employees spending time on collaborative efforts. This they consider as taking their time away from organizational work.

The national cybersecurity strategy (NCS) is an important plan for enabling and protecting the digital economy for a nation [27]. The focus of cybersecurity should be on critical infrastructure protection [70,93,94], national defence capabilities [95] and combating cybercrime [95]. Teoh et al. [27] analysed the correlation between a nation's cybersecurity strategy and the success of the digital economy [27]. The study found out that an NCS is not a pre-requisite for operationalising the digital economy. However an NCS is essential for the sustainability of the digital economy [27]. Hence it is essential to balance the need for a digital economy with the need

for cybersecurity. Teoh [27] observed that a strong private sector and industry is the reason for a thriving digital economy during the absence of an NCS. This was particularly observed for Singapore, Finland, and Switzerland.

To secure a nation's cyber assets, it is necessary to rollout a well-articulated strategy with SMART objectives (Specific, Measurable, Attainable, Results oriented, and Time specific) [27,96]. The objectives should cover the activities of cybersecurity such as stakeholder engagement, capacity building, governance, cyber defence and cybercrime [95]. The "what", "who" and "how" of cyber threats address the threat tools, threat agents as well as the attack vector, respectively [27]. Teoh [27] observed that the major cyber related risks include cyber espionage, hacktivism, and organised crime in cyberspace as well as cyberterrorism. Additionally, APT which is performed by well-resourced threat agents of high capabilities is also mentioned as a major risk to governments. Another threat is state and state sponsored attacks.

Israel has one of the most advanced digital systems in the world with extensive investments in technological innovations [97]. It is not surprising that its national cybersecurity strategy (NCS) is considered one of the best that even the US is impressed [13]. The Israeli 2017 NCS was built on three interrelated chapters being Concept of Operation, Capacity Building and Structure. Concept of operation (CONOP) is made up of a three-layer framework comprising of market robustness, systemic resilience, and defence [13,98]. Market robustness is the ability of the organization to repel and contain potential threats in the national cyber domain. The activities of this layer are aimed at reducing the nation's cyber threat levels [98]. The state's activities include the adoption of technological procedures such as awareness campaigns, guiding organizations and education [13].

Systemic resilience deals with the reaction to threats that have materialised [98]. This involves the state's ability to prevent the ripple effect of such threats spreading nationwide to other organisations [13]. The Israeli government has a national Cyber Events Response Team (IL-CERT) for responding to threats either independently or jointly with the impacted organisations. The IL-CERT's actions include threat detection, threat isolation, mitigation, threat alerts and denying its reoccurrence [13,98]. Defence layer is the exclusive responsibility of the Israeli government and

it includes proactive and offensive cybersecurity responses (cybernetic and kinetic) through law enforcement agencies [13,97]. The Israel Defence Force (IDF) is mainly responsible for executing the offensive and defensive campaigns in times of emergencies. It is also the main integrator of different security agencies during these times [13,97].

Capacity building chapter includes Research & Development (R&D) efforts, and cyber human capital development in all stages of education [13]. In addition to that, the Israeli government has invested hundreds of millions of dollars to companies and universities [13]. Other efforts include marketing and promoting exporting of Israeli cyber products. The structure chapter of the strategy outlines the organisational structure of the Israeli national cyber organ. Israeli National Cyber Directorate (INCD) is the highest authority that has capabilities to defend the national cyberspace[13,97]. This authority is also responsible for facilitation of international cooperation and the development of legal framework for cyber activities. The INCD has two arms under it which are the National Cyber Security Authority and the National Cyber Bureau. The National Cyber Bureau is responsible for strategic policy planning in terms of capacity building. The National Cyber Security Authority is responsible for national level implementation and regulation of the NCS. Israel has also succeeded where most countries are struggling. This is through managing to produce cybersecurity professionals who possess both the technical and the strategic cybersecurity expertise [13]. Israeli experts adopted a perpetrator indifferent approach by assuming that protection of the specific cyber assets is more important than dealing with the perpetrators [13].

2.3.1 Summary

Coordinated responses to cyber incidents have come a long way in the US since the 1988 incident of the Morris Worm. This incident initiated the first ever CERT team to be setup by the Defense Advanced Research Projects Agency (DARPA) [34]. Since then national cybersecurity strategies have been adopted worldwide. CSIRTs still remain one of the widely accepted and best national response to cyber threats. However, operationalisation of CSIRT teams in some nations is slowed by internal factors such as team dynamics, shortage of resources and skillsets. Cooperation efforts are also weakened by a lack of trust and commitment between

stakeholders. Despite the differences in the characterisation of threats and responsibilities of a CSIRT, national cybersecurity matters are consistently concerned with legal, cooperation, organisational, technological, R&D, professionals training and public awareness [27,32,61].

While the resources of a national CSIRT are dependent on the state's economy, smaller economies can learn from the example of Israel [13,97]. A key lesson being that organisations are the first line of defence in a national cybersecurity strategy. As such organizations should be facilitated by government to respond to cyber incidents [13]. In addition to that, it is better to invest more in cybersecurity programmes as opposed to chasing cybercriminals since the latter are difficult to bring to justice. This reinforces the statement by [34] that information sharing between governments, military, private and international stakeholders is a pivotal matter in securing a nation's cyberspace.

2.4 African Cybersecurity Responses

Africa has experienced tremendous ICT developments and the mobile penetration is high [99–103]. African countries have deployed Information Communication Technologies (ICTs) to compensate for the inequalities and challenges that are faced by their governments [99]. This has come at a cost since the same opportunity has also created an attractive environment for threat agents [104,105]. African governments are aware of the threats, and the need for public-private-partnerships, as well as the need for a multi-stakeholder model for responding to cybersecurity threats [99]. As such countries such as Botswana, Swaziland, Namibia, and Zambia have established legislative frameworks, and some are in the process of it [84,99,106,107].

The Southern African Development Community (SADC) has also assisted some member states in the legislative drafting process. This was done through the Computer Crime and Cyber Crime Model Laws and these are part of the Harmonisation of ICT Policies in Sub-Saharan Africa (HIIPSA) project [107]. Other continental cybersecurity instruments include the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) [108,109]. As of March 2022, only thirteen states out of fifty-five had ratified the Malabo

482 Convention [110]. Currently, twenty-six countries in Africa are members of the
483 Africa CERT team including Botswana [111]. Other nations are still in the
484 development process of setting up CSIRTs [99]. CSIRTs are important for
485 transnational cybersecurity efforts between states to address the borderless issues
486 of cybersecurity. Pillay [99] also concluded that there is a need for empirical data in
487 cybersecurity in the continent.

488 Sutherland [79] observed that African states have established telecoms regulatory
489 authorities but most have not been successful at setting up data privacy authorities.
490 Data privacy authorities are responsible for overseeing the collection, use and
491 storage of data. Coleman [112] observed that big technology companies sometimes
492 take advantage of loopholes in the law to violate data privacy. In some states the
493 data protection authorities are provided for in law but not yet operational [79]. The
494 implementation of cybersecurity strategies and centres for the collection of data on
495 attacks and defences is still being introduced slowly [79]. Additionally, African states
496 have introduced lawful surveillance and interception technologies without the
497 necessary oversight for such surveillance [79]. These inadequacies mean that the
498 rights to dignity and privacy are poorly observed and very often left to the
499 benevolence of those in state power.

500 Policies and structures for telecommunications regulation developed in the United
501 States (US) have been adopted as best practice by the European Union (EU) [79].
502 Consequently, African countries without thought for cultures, privacy laws and
503 politics have also adopted them in Africa. This adoption was due to the commercial
504 lobbying by telecoms manufacturers, seeking economies of scale for their products
505 [79]. However, these companies saw data protection as counterproductive and
506 expensive. Hence they lobbied the US Trade representative to argue against the
507 localization of personal data [79]. This was done knowing that such data would be
508 less protected once transferred overseas. Politically African governments vary with
509 the monarchies, authoritarian rule, and sometimes shaky democracies of countries
510 like Botswana and South Africa [79]. Hence there should be different approaches
511 and innovations for liberalisation of telecom markets, data protection and use of
512 surveillance technology. African states are more interested in their surveillance
513 capabilities than securing the cyberspace [79,113]. Examples of these are the

procurement of spying equipment such as the International Mobile Subscriber Identity (IMSI) catcher, and the collection of customer data from telecom operators [79]. On the other hand CERTs are under-resourced and lack incident registers [79,114,115].

Kshetri [84] conducted a study on cybercrime and cybersecurity in Africa. In the study, the author stated that Africa has become the source and target for cyberattacks [116]. Losses due to cyberattacks in Africa amounted to \$3.5 billion in 2017 [84]. Vulnerable systems and poor cybersecurity practices have been identified as the cause for the increasing cyberattacks in the continent. Another issue was the low priority placed on cybersecurity and many organizations invest very little of their budget towards cybersecurity. Kshetri [84] agreed with Sutherland [79], noting a lack of cybersecurity expertise as well as insufficient legal provisions to combat cybercrime in Africa. Some of the African states that were mentioned in the study that have suffered the impacts of poor cybersecurity included Kenya, Nigeria, Zimbabwe, Lybia and Cameroon. Some of the initiatives aimed at mitigating cyber threats in Africa include cooperation efforts, organizational efforts, technical efforts and laws to deal with cybercrimes and data protection [32].

In 2018 Botswana, alongside Namibia, Zimbabwe and Mozambique, did not prioritise cybersecurity in their national budgets [117]. However, Botswana has improved as cybersecurity now features in the national budget and parliamentary discussions [118]. Renaud [117] stated that South Africa is the hardest hit by cyberattacks in Southern Africa, citing the global WannaCry malware attack of 2017 as an example. Although the South African NCS was announced in 2012, it has not been clear how private individuals will be protected. This is because attacks will turn to individuals when big organisations become more resilient [117]. As such a supportive system should be put in place where government and the individuals play a role as in the case of New York City. At New York City, the government provides guidelines and a list of government sanctioned security software [117]. Currently governments treat cybersecurity risk as a “solo risk” where the harm is to an individual. However, cybersecurity risks are a society risk, where an attack can cascade through the entire community [117].

Adomako [106] assessed the cybersecurity effectiveness for west and east African countries based on qualitative and quantitative measures. For the qualitative approach Key Performance Indicators (KPIs) were identified and used to evaluate the effectiveness of the cybersecurity policies in those countries [106]. These KPIs included the existence of a CIRT, threat landscape identification, existence of cybercrime legislation, number of security professionals, security breach notification, conviction rates of cybercriminals, and accession to the Budapest convention [106]. For the quantitative approach statistical data related to cybersecurity incidents was used [106]. These statistical quantifiers included the cost of cybercrime before and after cybercrime legislation, impact of cybersecurity legislation and policies, and a security index was developed based on the KPIs. The study among other things observed that Africa has fewer cybersecurity professionals relative to its population. Secondly, African states tend to adopt laws and policies designed for countries with advanced responses to cybersecurity without regard to the African context [79]. In concluding the study found that implementation of cybersecurity legislation does not guarantee an improved mitigation against cyber-attacks. Therefore, in countries where legislation has been enacted it should be coupled with funding for cybersecurity initiatives as well as enforcement [106].

Cybercrimes that were reported in Zimbabwe included phishing, credit card fraud, identity theft, unauthorised access, hacking and telecommunications piracy [119]. Kabanda [119] carried out a study on the cybersecurity culture framework and its impact on Zimbabwean organisations [119]. "Cybersecurity culture is defined as the beliefs, assumptions, attitudes, values, perceptions and knowledge that people have pertaining to cybersecurity and how these manifest in their interaction with ICTs" [119]. A cybersecurity culture has to do with shared activities, attitudes, values, behaviours and norms that support cybersecurity [85,119,120]. A lack of a standardised cybersecurity culture framework in Zimbabwe is one of the issues that make it difficult to manage cyber risk. As mentioned in other studies, threat agents see humans as the weakest link in systems [34]. Therefore a strong cybersecurity culture has the potential to change the mindsets and behaviour of system human users to be better protected against cyber-attacks [119].

The recommendations by Kabanda [119] considered cybersecurity challenges in developing countries, as well as the requirements of a cybersecurity framework. The study identified the following building blocks of cybersecurity culture which are law enforcement officers, management, ICT professionals, acceptable practices, end users, and effective cooperation [119]. Kabanda [119] further identified five vision elements to focus on in developing Zimbabwe's cybersecurity culture framework. These were Talent Centricity (a culture that makes cybersecurity part of everyone's job and employing a Chief Information Security Officer for each organisation); Strategy and Innovation (placing cybersecurity at the heart of organisational strategy); Intelligence and Agility (Develop internal capabilities on threat knowledge and intelligence); Resilience and Scalability (rapid recovery from cyber-attacks while maintaining cybersecurity standards) [119].

Turianskyi [121] drew an analysis on the lessons that the African Union (AU) can learn from the European Union (EU). According to this study the AU has an institutional setup that is similar to the EU since it is loosely based on the EU model [121]. Differences exists between the EU and AU. These have to do with operational procedures and resources. The EU has a truly borderless single market as well as a single currency. EU initiatives and policies on cybersecurity date as far back as 1995 when the Data Protection Initiative was introduced, which is now replaced by the General Data Protection Regulation (GDPR) of 2018 and others [121]. The EU Cybersecurity Act will also establish a cybersecurity agency for the EU. On the other hand, the AU which has 55 member states compared to the 28 members of the EU, also has a policy on cybersecurity. However, the main difference here between the AU and EU is the influence that these organisations have over their member states. The AU on the one hand has less authoritative rule over its constituents compared to the EU. For instance, the 2014 Convention on Cybersecurity and Personal Data Protection, which is part of Agenda 2063, has been ratified by few of its member states [110,116]. The same applies for the Budapest Convention as African countries are slow to ratify it [122]. The EU on the other hand required its member states to adopt the GDPR within 2 years.

607 2.4.1 South Africa's National Cybersecurity Policy

608 A key factor in achieving coordinated action among cyber related entities in
609 response to cyber threats is the existence of a well-defined organizational structure
610 [123]. The International Telecommunications Union (ITU) advocates for legal
611 measures and a national cybersecurity framework to promote a cybersecurity
612 culture [124]. Gcaza and von Solms [85] argued that the South African government
613 has successfully implemented strategies for connecting communities to the internet
614 through initiatives such as free internet. However, South Africa ranked 3rd in the
615 world for cyber related crimes [85]. Implementation of cybersecurity still lags in
616 South Africa. The authors in [85] hold the position that a cybersecurity culture
617 strategy should be rolled out to promote and support the implementation of
618 cybersecurity in South Africa. In [85] the strategy development approach followed
619 five steps: Strategy Direction, Environmental Assessment, Strategy Formulation,
620 Strategy Implementation, and Strategy Control. The authors [85] did not develop a
621 comprehensive plan for strategy implementation but prioritized the following
622 programs: cybersecurity culture body, cybersecurity research agenda, stakeholder
623 engagement and partnerships establishment. For strategy control it was suggested
624 that the body responsible for the strategy should define benchmarks for the
625 proposed actions.

626 Some of the bad actors in South Africa's cyberspace include foreign states
627 attacking critical infrastructure and hacktivists [78,125]. Other threats include
628 ransomware, identity theft, malware, email spam, denial of service and phishing
629 attacks [125,126]. Implementation of smart cities and the deployment of IoT devices
630 is increasing the attack surface area [125]. South Africa has already recorded the
631 highest instances of cybercrimes estimated at ZAR 5.8 billion [125]. Hence the
632 South African government is under pressure to operationalise the National
633 Cybersecurity Policy Framework (NCPF). The Information regulator is not fully
634 operational, and the cyber warfare strategy has not yet been finalised due to poor
635 inter-ministerial coordination [125].

636 Other issues are weak oversight structures (e.g., parliament struggles to analyse
637 cyber related legislation hence the limited oversight), as well as counterproductive
638 secrecy [125,127]. Reporting of cybercrime incidents was made mandatory in 2018.

However the public is still sceptical about the capability of the South African Police Services to respond to such incidents. Hence government needs to be more accountable, strengthen its security structures and acknowledge its weaknesses to improve its credibility [125]. Private firms are also not forthcoming in reporting data breaches due to the potential financial losses that they may incur. An important factor of a cybersecurity strategy is the ability of the military to maintain resilience of critical infrastructure and still be able to launch offensive security measures [125]. However, the cyberwarfare strategy is not yet fully operational [125]. There is also a need to assess the effectiveness of the policies adopted from western countries in state and municipal South Africa.

Van Niekirk [37] analysed the cyber-incidents in South Africa. The study identified six types of cyber impacts due to cyber-attacks and these were data exposure, denial of service (DoS), financial, website defacement, data corruption, and system penetration [125,126]. Some of the data exposure attacks were categorised as APT and were attributed to China and Russia, respectively. The attacker group Anonymous also attacked the South African Police Service in 2013 releasing approximately 16,000 details of whistle-blowers and victims. This was in response to killings of Marikana Mine workers protestors by the police. Other data exposure incidents were due to flaws in systems. Financial attacks were carried out using phishing, insider attacks and use of key loggers. The Anonymous group also executed several DoS attacks on the African National Congress Party and state broadcaster. Web defacement attacks were targeted at South African universities and some companies.

2.4.2 SADC Computer Crime and Cyber Crime Model Laws

Bande [107] investigated the legislation of three Southern African Countries (Botswana, Malawi, Tanzania). Bande [107] sort to find out whether the three states harmonised their cybercrime laws with international conventions such as the Budapest; as well as maintaining diversity to meet domestic needs. To facilitate cooperation among countries domestic law must be harmonised with international conventions to eliminate cybercrime safe havens. Additionally, harmonisation of data protection laws will ensure protection when data is processed in a foreign country [128]. Hence SADC adopted the SADC Model Law on Cybercrime in 2012

to facilitate member states in the harmonization of domestic cybercrime laws [107]. However, Ferreira [128] argued that the Model Law has not been successful in harmonising the cyber law in SADC. Ferreira [128] noted that most laws in the SADC region are based on the outdated EU Directive which has been replaced by the GDPR. However, Mauritius and South Africa have more advanced laws which reflect some of the newer elements of the GDPR. While the Model Law has not been all together successful there is still opportunity for harmonisation of SADC laws. This is because most of the laws have elements of either the EU Directive or the GDPR [129].

Jurisdictional issues require a harmonised legal ground between multiple cooperating states [107,128]. Bande [107] describes the Budapest Convention [106] as the closest instrument to a global treaty on cybercrime. This is because although adopted under the Council of Europe, it was prepared together with non-European countries; and non-European states are invited to accede to it. According to Bande [107], the legislations of Botswana, Mauritius, South Africa, among others in SADC; as well as the SADC Model Law on Computer Crime and Cybercrime, were developed based on the Budapest guidelines. Bande [107] further states that, if SADC member states were to harmonise their laws with the Budapest convention, it would be opening its doors to cooperation with more than 73% of the world [107].

Antagonists of the Budapest Convention include Russia and China and other countries who support them [107,130]. Concerns are around issues of sovereignty over the Convention's article 32. This article creates a provision for trans-border access to data stored in a foreign state without authorization from state authorities [107,130,131]. In other instances, the Convention has been criticised for having been overtaken by technology. However, Bande [107] argues that the convention provides a minimum harmonisation model for other countries to base their cyber laws on. What is therefore needed is a diversification process at the national level – the so called “glocal” approach where countries are expected to merge global requirements with local needs [107]. The study concluded that indeed the three SADC states have cybercrime legislation that adheres to the Budapest Convention. The countries also extended the offenses found in the Budapest Convention, but this was only to broaden them as opposed to addressing new threats that were not

identified by the convention [107]. However, the study showed that there were instances where the Malawian legislation did violate guidelines by including technology specific terms in its legislation. It was recommended that Malawi should work more closely with Botswana and Mozambique to eliminate such discrepancies [107].

2.4.3 Summary

African states have setup institutions for dealing with cyber threats. However the efforts are not adequate enough to thwart cybercrimes. As a result, the ICT society in Africa is ahead of its cybersecurity. Some authors such as [79,125] have identified a lack of political will as the reason for a slow implementation of cybersecurity in Africa. However, the involvement of the president and his cabinet in implementation of a technology strategy is important for successful strategy execution [33]. As such involvement of the executive arm of government in cybersecurity implementation can positively turn things around for African cybersecurity. Other authors have also observed that African leaders are slow to ratify regional and international conventions such as the Budapest and Malabo conventions, respectively [121]. Ratifying these treaties will improve and promote coordination among member states. At the SADC regional level, countries are developing their cybersecurity laws based on the SADC Model Law, which is a regional localisation of the Budapest. Yet still, while some African countries are enacting cybersecurity related laws, there is low investment in cybersecurity programmes. Another issue pertaining to African countries identified in the literature is the need for a national cybersecurity culture strategy [85,119] which help change attitudes and habits towards cybersecurity. Finally, [117] noted that while it is important to promote cybersecurity at organizational level, African countries should also develop programmes that will assist their citizens to deal with cybersecurity at the individual level.

3. BOTSWANA CYBER LANDSCAPE

3.1 Economy

Botswana has a population of about 2.3 million people with and a growing GDP [1,2,31]. In 2020 the telecommunications regulatory authority of Botswana reported an impressive 187% mobile phone penetration and 101% mobile internet penetration [132]. In 2019 the country had 40,000 broadband subscriptions [1]. All the three mobile telephony service providers (Mascom, Orange Botswana and Botswana Telecommunications Corporation) have services for mobile money which are “MyZaka”, “Orange Money” and “Smega”, respectively. Another player in the mobile money service is Botswana Post with its Poso Money service [132].

Botswana is rapidly becoming the world’s developmental success story due to the discovery of diamonds and other minerals, good governance, a small population and prudent economic management [31]. Since independence, Botswana has enjoyed peaceful democratic elections in a multi-party democratic fashion [31] [133]. Recently the growth rate has slowed down due to diamond market volatility and the competition from synthetic diamonds. Other factors also include reduced Southern Africa Customs Union transfers and fiscal expansion [31]. As such income inequalities and unemployment remain high [31,134]. The ongoing Coronavirus pandemic has made matters worse as the restrictions imposed by the pandemic have impacted key production and export sectors of Botswana which are diamond (and mining), tourism and agricultural industries [31].

3.2 Peace and Security in Southern Africa

Peace and security cannot exist in one country in isolation [3]. Therefore, when investigating the threat landscape for Botswana it is important to investigate the peace and security of countries in the SADC region to get a clear picture of the threat. Since establishment of the AU in 2002, the number of wars in the SADC region has fallen [3]. However there has been some political instabilities in Zimbabwe, Lesotho, Madagascar [3]. More recently an armed group called al-Shabab linked to the ISIS has been terrorising Mozambique, killing thousands, and

displacing hundreds of thousands more [63]. Al-Shabab means the youth and it is not linked to the group with the same name in Somalia [4].

The US's military campaigns and its allies continue to have success against the extremists group ISIS. However, there are growing concerns over the ISIS propaganda that is being pushed through the internet and social media [135]. ISIS uses these internet and social media campaigns to direct and inspire its militant jihadi wannabes globally [135]. Interviews from ISIS defectors have revealed that if the group is defeated in open warfare, their plan is to cut their beard and blend with normal civilians to launch guerrilla style attacks. ISIS basically uses appropriated Islamist narrative and media to pull its recruits [136]. However, the group has been observed to attract young people in their 20s with little or no Islamic experience [137]. According to [136], for ISIS radicalisation to take place there has to be a pre-existing condition that is represented by a distress such as identity crisis or grievances [136]. It is possible for the youth in Botswana to fall for the ISIS Caliphate to join its terrorists' group through online campaigns. This is due to factors such as unemployment and idleness, which has been worsened by the pandemic. Other factors include an impressive mobile penetration, and free internet in libraries, schools, and public places. The authors in [135] observed that foreign recruits sometimes flow through countries such as Turkey posing as tourists, to Syria where they join ISIS. Such recruits may later declare themselves dead and return to their countries without their original passports. They would continue to live there undetected where further attacks may be launched [135]. It is not far-fetched that with the ongoing war in Mozambique, such a threat may exist in Botswana as well as the threat of home-grown terrorists.

3.3 Chinese Threat

In 2018 it was in the news that the AU headquarters were under espionage attack by the Chinese government [38]. However, African officials and China strongly denied the accusations [138]. After another reported attack in 2020 the AU spokesperson did not respond to an inquiry on the suspected hacking activity by the Chinese hacker group Bronze President [139]. China also denied the claims. The AU building which was built by the state-owned China State Construction Engineering Corporation, was installed with Huawei servers, which were daily

uploading content to servers based in Shanghai, China [38]. A sweep of the AU building also uncovered eavesdropping equipment which enabled China to study the personalities, habits, financial situation, and preferences of African leaders. This data may be used to facilitate recruitment of intelligence assets. It is also possible for China to obtain embarrassing information on African leaders and use blackmail to gain their support. Beijing has built and renovated more than 186 government buildings, as well as more than 14 sensitive government intra-network communications in Africa [38]. These buildings include presidential residences, foreign affairs buildings, parliaments, parliamentary residences, military, and police installations. This has given it surveillance capabilities more than anywhere else and this companies are legally obligated to help the China collect intelligence. Additionally, the Chinese government has also donated computers to at least 35 African states. Information gathered by the Chinese government may be used to exert influence on the continent, recruit intelligence assets which will give Chinese companies a competitive advantage in the ongoing trade war [38]. The economic risk here is that African states negotiate with Chinese banks and government. As such China may eavesdrop on African leaders' negotiation strategies, competitors' bids and other relevant information. The reliance of African states on China has made African states strategic allies to China, as they have helped China to win leadership of many international organisations [38].

Huawei also poses a threat to African states since the telecoms giant has built more than 70% of the 4G telecom networks in Africa, including military and police installations [38]. Plans are also underway to roll out 5G networks based on Huawei technology. The US House of Representatives has openly declared the Chinese telecom giants Huawei and ZTE as cyber threats to national telecoms infrastructure [140]. With developed states such as the US, Germany and Japan fearing that they cannot adequately protect against the Huawei threat, it is unlikely that African countries can [38]. Due to economic enmeshment and inducement of African leaders, African states may have accepted the risk posed by China and its companies [38]. In Botswana there are at least two government buildings that were built by the Chinese government, and these include Botswana High Court and Court of Appeal, and Botswana Police Service Forensic Science Laboratory [38]. Botswana has also engaged Huawei to install over 500 cameras for its Safe City

Project in Gaborone and Francistown. The project will be used to fight crime by keeping streets and buildings safe and counter terrorism [141].

3.4 Serianu Limited Report

Serianu Limited [8] conducted a survey on the cybersecurity for Botswana. The report covered cybersecurity trends, cyber intelligence, industry risk ranking and cybersecurity skills gap analysis. Some threats which are unique to African countries listed on the report include mobile money compromise and SIM swap [8]. The cyber risks in Botswana identified by the report include malware and cybersecurity skills gap. In particular crypto mining and banking malwares were found to be common in Botswana. The sectors which were mostly impacted by the crypto mining malware include manufacturing, educational and financial institutions [8]. Other examples of cryptocurrency attacks include the global WannaCry ransomware attack that required victims to pay the ransom in Bitcoin cryptocurrency. Cryptocurrency attacks have not deterred people in Botswana from using the currency [142]. As the Bank of Botswana Governor also pointed out, cryptocurrencies are also used for criminal activity cover-ups, money laundering, pyramid schemes and other unlicensed ventures [142]. The governor also stated that while some continue to invest in cryptocurrency investments, they should not expect any protection from the central bank beyond public policy interest [142]. Other vulnerabilities identified included third-party exposure through outsourcing, and employees' personal devices allowed through inadequately configured Bring Your Own Device (BYOD) policies. Other exploits targeted individuals based on their role in the organisation, e.g., employees who had access to sensitive documents and those who authorised payments were targeted by business email compromise. Employees who have credentials to critical infrastructure were targeted using keyloggers [8]. In general attackers targeted organisations that dealt with money transactions and financial institutions. The report also identified a big cybersecurity skills mismatch within the Botswana ICT society. This was coupled by the need for women representation in the cybersecurity industry. Hence the need for cybersecurity professionals training [8].

853 3.5 National Development Plan 11 (NDP 11)

854 Botswana is well connected by fibre optic cables internally and international
855 connectivity is provided through WACS, SEACOM and EASSY undersea cables.
856 These same opportunities present cybersecurity threats that should be dealt with.
857 The national cybersecurity strategy was developed during the NDP number 10
858 period (April 2009 to March 2016) [143]. The NDP number 11 period (April 2017 to
859 March 2023) envisions to achieve implementation of the strategy to see the delivery
860 of the strategic milestones of the NCS [144]. This means that provision has been
861 made for the implementation of the NCS in the NDP 11. The NDP 11 document
862 mentions that legislation to arrest cyber threats will be put in place during its time
863 period. As evidence of that, the Botswana Cybercrime and Computer Related
864 Crimes act of 2007, which was already regarded by some (e.g., [107]) as
865 procedurally and substantively comprehensive, was repealed and re-enacted in
866 2018. However, beyond revamping the legislation, the NDP 11 does not explicitly
867 identify other initiatives or programmes that will be achieved during its time period.
868 The plan does however identify the national cybersecurity strategy as the
869 foundational roadmap for addressing national cyberspace challenges [144].

870 3.6 Botswana NCS

871 The Botswana NCS was developed because of the Readiness Assessment Report
872 developed by the ITU in conjunction with IMPACT – International Multilateral
873 Partnership Against Cyber Threats – (ITU/IMPACT). The strategy identifies six
874 sectors which make up Botswana’s critical infrastructure which are
875 communications, governance, utility provision, healthcare, financial and transport
876 sectors [35]. During the corona virus-imposed restrictions on movement, “Mines”,
877 “Security”, “Supplies” and “Funeral” services were listed on the Government of
878 Botswana website under essential services that were allowed unrestricted
879 movement [145]. Other essential services on the website were mappable to the six
880 critical sectors identified in the NCS. Deployment of ICT in these critical sectors has
881 made the cyber threat a contingency that can potentially impact the economy and
882 slow down processes or potentially cause damages.

The recurrent theme of the Botswana NCS is that of inclusiveness and coordination of the partners involved in assuring a secure cyberspace [35]. These partners include government, private sector, regional and international organisations, and foreign governments. The involvement of international players is not surprising because the Botswana cyberspace is not an island that is closed from the worldwide. It is rather a subset of it that intersects with other domains from all the different countries of the world. Another anchoring theme of the Botswana NCS is resilience although little has been communicated on this requirement [35]. A safe internet is one other anchor of the Botswana NCS. Botswana NCS also identified public education and cyber awareness as one of the areas that are still behind in development [35].

Therefore, the strategy was a response to the weaknesses in the cybersecurity posture of the country which included lack of cybersecurity experts in the country [8]. Botswana also did not have a coordinated framework for the various stakeholders to engage on cybersecurity issues [35]. Hence the strategy. Through the strategy, the principles of open and free internet, data protection and integrity are promoted without hindering on the human rights. The strategy touched on the key areas of cybersecurity and its planned implementation covers all the stakeholders. The Botswana government still has more to do to achieve the strategic milestones as a lot of them have not been implemented for many years. The NCS should also be subjected to review considering the changes in the landscape that have been brought about by factors such as the coronavirus pandemic [32,61]. According to Dawson [146], cybersecurity is constantly evolving and as such the cybersecurity framework should be continually updated, essentially making it a living document.

3.7 Botswana Communications Regulatory Authority (BOCRA)

The Botswana Communications Regulatory Authority (BOCRA) has a responsibility for cybersecurity as its role in setting up the national CIRT shall be discussed later in this chapter. BOCRA has listed on its website draft guidelines for email security [147] and website security [148]. Based on the guideline, mail servers are second to web servers in terms of high frequency of attacks. The email security guideline is intended to provide best practice recommendations for organizations operating on

915 public and private networks. Table 2 describes the threats as outlined in the
 916 guidelines.

917 *Table 2: Cyber-attacks and their characterisation*

Cyber Threat	Characterisation	Common Source	Countermeasures
Malware	There are many different types of malware which include malicious mobile code [66], ransomware, Trojan, backdoor, rootkit, fake antivirus, adware, spyware and file infector virus [65].	Websites (e.g. adult content sites) [65] Email [65] Pop-up windows [65] Open wifi [65] Pirated software [65]	Organizational policy statements; Awareness programs for users and IT professionals; Vulnerability and threat mitigation efforts; Defensive Architecture consideration; Security configuration checklists; Patch management; Antivirus software; Intrusion prevention system; Firewalls; Sandboxing; Browser Separation; Virtualisation [65,66].

Social Engineering	Social engineering involves manipulating the victim into disclosing information that exposes them or that can be used to gain access to secure information and locations [149]. Examples include tailgating, impersonation, phishing emails and Trojan horse attacks.	Typically uses delivery based methods such as email and USB keys but can also use phone calls and site visits [150].	Cybersecurity training and awareness, physical security e.g. biometrics and cameras, Social engineering attack drills [149,150].
Denial of Service (DoS) or Distributed Denial of Service (DDoS)	A DoS or DDoS occurs when one or more infected systems launch a flooding attack on one or more targets in order to overload their resources [151]. The result of a DoS is that legitimate users are denied access to services, devices or other network resources [152].	Compromised devices, systems and servers [153].	Traffic analyser, Antivirus software, disaster recovery plan, DoS protection service [152].
Man in the middle	In a MITM attack a third party intercepts the communication channel	Phishing emails, Router spoofing, Malicious	Use encryption to digitally sign data,

(MITM) attacks	between two end points [154]. Examples are ARP poisoning and DNS spoofing [155].	employees, Malware infections [156].	Transport Layer Security 1.3 [157].
SQL Injection	This attack exploits web based applications [158]. An attacker uses the input variables on a web application to trick the application into executing the attacker's code on the database [159].	Poor coding practices e.g. Use of older (Application Programming Interfaces) APIs, non-validated SQL statements [159].	Parameterized queries, stored procedures, input validation [158,159].
Cross site scripting (XSS)	XSS allows an attacker to execute a malicious script onto pages viewed by the user [160]. This type of attack also takes advantage of browser vulnerabilities.	Outdated browsers [160], Poor security practices [161].	Validate inputs and outputs, eliminate dangerous insertion points [161].

918 Threats that were highlighted by the guideline include malware, social engineering,
919 spam and phishing, human factor (unintentional), denial of service (email bomb),
920 and man in the middle attacks [147,148]. The documents does not suggest that
921 these attacks have been reported in Botswana networks. However it is an
922 awareness campaign against web and email attacks. Website attacks that were
923 highlighted in the document included SQL injection, cross site scripting and other
924 web attacks. The countermeasures for those attacks included strong password
925 policy, multifactor authentication, longer encryption key algorithms, frequently
926 update keys and other security good practices [147,148]. Organisational measures
927 included implementing an organizational security policy, change management, risk

928 management, security training and awareness, contingency planning, and
929 certification and accreditation.

930 3.8 Botswana Computer Incident Response Team

931 Information on the ITU website shows that the ITU/IMPACT alliance conducted a
932 CIRT readiness assessment and capacity building programme for Botswana in
933 2012 [162]. The 2012 assessment recommended that Botswana setup a CIRT as
934 soon as possible, which will be able to identify threats, respond and manage them.
935 This would consequently improve the cybersecurity posture of Botswana. Based on
936 information presented on the Botswana Computer Incident Response Team (Bw-
937 CIRT) official website [163], the CIRT is the first (and the only one) in the country.
938 It was setup in 2019 by BOCRA through the supervision of the Ministry of Transport
939 and Communications (MTC). From the information provided on the website, the Bw-
940 CIRT is a department of the communications regulator (BOCRA) and it is funded
941 through its budget [163]. It is however ironical that the first CERT team in the world
942 was setup after seven days of recommendation by DARPA in the US [34]. In
943 Botswana it took seven years after the initial recommendation by ITU/IMPACT to
944 setup the same. This is against the fact that the Botswana NCS recommended
945 giving first priority to setting up the Bw-CIRT [35]. Bradshaw [34] states that the
946 threat-related information that are collected by CERT teams include internet
947 protocol (IP) addresses, email addresses [34]. These are used to identify and
948 remove addresses and domains known for distributing malware and executing
949 attacks such as phishing against the CERT's constituents. CERTs also work with
950 law enforcement and government to bring down cybercriminals [34].

951 The Bw-CIRT website is said to collect information on cyber incidents from
952 government departments, Internet Service Providers (ISPs) and other relevant
953 entities. The Bw-CIRT aims to be a trusted point of contact for cyber related
954 incidents, improve cybersecurity awareness, and cooperate with national and
955 international CIRTs. Bw-CIRT is also affiliated to the Africa CERT [111]. Services
956 listed on the CIRT website include cybersecurity awareness and capacity building,
957 cyber threat intelligence, information sharing, and incident management [163].
958 However, there is no report/review available on the website regarding the activities
959 of the CIRT. On the date of access [163], the website had four general worldwide

warnings listed under “Alerts and Warnings”. More vulnerabilities and latest worldwide hacks can be seen from the “Newsletter” page of the Bw-CIRT page. Additionally, no information relating to vulnerabilities or incidents on the Botswana’s cyberspace was available on the website. Although the Corona virus has changed the cybersecurity threat landscape, there was no information or report related to the impact of the pandemic and the mitigations introduced on the CIRT website. A list of upcoming cyber awareness events is however listed on the website.

3.8.1 South Africa Cybersecurity Hub

South Africa’s national CSIRT (The Cybersecurity Hub) website [164] is very similar to that of Botswana and both are affiliated to the Africa CERT [111]. The cybersecurity Hub also has a list of internationally known recent vulnerabilities. However, unlike Botswana the Cybersecurity Hub also displays cyber-attacks that have hit South Africa. Cyber awareness resources displayed on the CSIRT website are cyberbullying, and phishing. “Cyber tips & advice” provides cybersecurity tips and advisory. Finally, the website provides a list of upcoming cyber awareness campaigns in the “Events” page.

3.8.2 UK National Cyber Security Centre (NCSC)

The NCSC is the authoritative voice of information security in the UK [165]. Compared to Botswana (and South Africa) cybersecurity activities, the UK is ages ahead. The NCSC website has a wealth of reports on cyber threats information, intelligence, and cybersecurity strategies. While Botswana’s CIRT provides generalised information on cybersecurity, the NCSC on the other hand provides an account of the actual cybersecurity programmes and activities that are being executed by the UK government. Under the “Advice and Guidance” section of the website, the trends include Video conferencing, Cyber Aware, Coronavirus, Passwords, 5G and Phishing. A quick overview of these links shows that all these topics are addressing current threats that are faced by the UK. For example, the video conferencing link is addressing the pertinent issues of data protection and privacy issues since holding meetings online has become a norm due to the coronavirus pandemic [6,165].

An interesting factor again is the structuring of data on the NCSC website. For example, the NCSC not only provides weekly and annual reports on threats, but it also produces customised reports that target cybersecurity professionals, individuals and families, large organisations, public sector, self-employed & sole traders, and small & medium sized organisations. It can therefore be comfortably said that the NCSC approach supports the UK community at all levels of society. The NCSC 2020 report [6] downloadable from the NCSC website covered seven chapters which are: (1) Coronavirus – Responding to the pandemic, (2) Defending democracy, (3) Building a resilient nation, (4) Proactive engagement, (5) Defending the digital homeland 24/7, (6) Driving cyber skills and innovation, and (7) International influence. All these chapters are made up of practical cybersecurity operations that the UK government executed in the year 2020. The NCSC’s work reaches far and wide, from protecting and supporting individuals, essential services providers, and the critical network infrastructure, supporting and protecting the military, mitigating potential supply chain vulnerabilities, as well as developing international standard technology. On the issue of partnerships on cybersecurity, the UK collaborates with its allies on bilateral levels and at organisations such as NATO (North Atlantic Treaty Organization). NATO has a membership of 28 European countries and two North American Countries. Other alliances include “the Five Eyes” – the USA, UK, Canada, Australia, and New Zealand.

3.9 Cybercrime Legislation

Cybercrime law must be technology neutral to cater for the evolving technological advancement, provide checks and balances to law enforcement powers to protect and the rule of law. It must also be compatible with laws of other countries to satisfy the requirement for dual criminality [166]. According to [1], the rule of law is entrenched in Botswana and the independence of the judiciary is highly valued. However, the author also noted that there are some cases where the government has ignored some court orders. Botswana criminalised the criminal activities that are executed on the cyberspace in its Cybercrime and Computer Related Crimes Act (Bw-Cybercrime Act) of 2007 [167]. Crimes in the Bw-Cybercrime Act were already included in the penal code, however without specificity to the electronic online environment [167].

1022 Other legislation that is related to cybercrime includes The Electronic Record
1023 Evidence Bill [168], Communications Regulatory Authority Act No. 19 of 2012,
1024 Electronic Communications and Transactions Act no.14 of 2014 and Electronic
1025 Records (Evidence) Act no. 13 of 2014, and the Data Protection Act of 2018. In
1026 2018 an act to repeal and re-enact, with amendments the Cybercrime and
1027 Computer Related Crimes was passed into law. There are twenty offences specified
1028 by the 2018 Bw-Cybercrime Act. These offenses address the three major types of
1029 cyber threats which are denial of e-services, data integrity breach and confidentiality
1030 breach. In addition to that the act protects individuals from human rights abuses
1031 that are protected by the penal code as already stated in [167].

1032 The Bw-Cybercrime Act also defines the jurisdiction of the law. However, as already
1033 pointed out by [13,168], cyber breaches can be perpetuated from anywhere in the
1034 world. This is because bad actors are skilled at masking their identity. In addition to
1035 that, sovereign states hold varying views on internet laws and freedoms [121,168].
1036 As such sometimes even when these criminals are found it becomes difficult to
1037 persecute or extradite them. Considering this, as much as it is important to have
1038 good cybercrime laws for maintaining law and order, it is as much important to
1039 resource cybersecurity responses for defence, resilience, and offensive operations.

1040 On the international scene, Botswana is not a party to the Budapest Convention.
1041 However, the Bw-Cybercrime Act covers both substantive law and procedural law
1042 that corresponds to the Budapest Convention [169]. Additionally, the Electronic
1043 (Evidence) Records Act of 2014 addresses the admissibility of electronic evidence
1044 in the courts of law. It is interesting though to observe that although Botswana laws
1045 correspond to the Budapest Convention, it is not a signatory to the same. However,
1046 according to [166], the Budapest Convention is best considered as a whole in order
1047 to benefit fully from its guidelines. The Council of Europe reported that Botswana
1048 was a part of international capacity building programmes and conferences in the
1049 issue of cybercrime [169]. Continentally, Botswana has also not signed nor ratified
1050 the African Union Convention on Cybersecurity and Personal Data Protection.

1051 In summing up Botswana is one of the countries in Africa that have provisions for
1052 substantive and procedural laws vis-à-vis cybercrime and computer related crimes.
1053 Its laws correspond to the Budapest Convention even though it is not a signatory of

the convention. Botswana will benefit more from signing the convention because in addition to the good guidelines that are provided by it, it also serves as a framework for international cooperation. Nonetheless the state has been actively involved in cybercrime capacity building programmes which is commendable. Botswana will also do well by implementing regulations of the Bw-Cybercrime Act to enforce the law. However, law enforcement should be adequately resourced so that cyber criminals do not defeat the ends of the law. This can happen due to incapacity of law enforcement agencies to carry out investigations, and failure to collect electronic evidence for admission in the courts of law.

3.10 Analysis of Botswana Cybersecurity Rankings

Based on ITU [32] rankings Botswana is number 12 in the Africa region. In terms of legal measures Botswana has shown relative strength [32]. This is supported by other studies in the literature [107,167]. Generally, states with developed countries status scored higher on the ITU rankings [32]. This is understandable since the cybersecurity budget is limited by the size of an economy. Hence developing nations have to prioritize other developmental issues such as job creation and income disparity reduction [34,90]. However, countries categorised as Least Developed Countries such as Tanzania, Rwanda and Benin were outliers as these countries scored really high in the ITU rankings [32]. Tanzania ranked number 2 in the Africa region with an overall score of 90.58 after Mauritius [32]. Mauritius scored 96.89, while South Africa ranked number eight with a score of 78.46. In global rankings the US is number one followed by the UK and Saudi Arabia. Generally African countries have strengths in different cybersecurity measures. As such the region can benefit more from increased cooperation as there is potential for them to learn from each other.

3.11 Summary

In summary Botswana continues to expand its ICT society, which is something that is inevitable considering the global changes such as the global Corona pandemic. However, these ICT developments are not met by an equal investment in cybersecurity. The national CIRT team still must do more to achieve its mandate. The Corona pandemic has provided threat agents with lucrative opportunities to

exploit people. However, there is no evidence of local reports addressing the cybersecurity concerns that are heightened by the pandemic on the Bw-CIRT website. As a result, the cyber society of Botswana is ahead of its cybersecurity. Based on information on their respective websites, the Botswana and South Africa CSIRTs are still at a developmental stage compared to the UK. Botswana and South Africa should work together to learn from developed CSIRTs such as the UK. In terms of its legislative framework, Botswana has installed cybersecurity related legislation that is both substantive and procedural. However, some observers such as [1] (and [125] in the case of South Africa) have observed that sometimes these laws and the penal code are abused by those in state power to oppress and muzzle those who oppose state leaders.

4. METHODS

The methods used in this study follow an exploratory research design. Both qualitative and quantitative approaches were employed in this study. Exploratory data analytics, text analysis, questionnaire and literature review were the methods used. R is the tool that was used for statistical and data analysis. Microsoft Excel and the Notepad applications were also used for manually editing and preparation of the datasets. An HP 250 G7 Notebook computer with an i5 Intel processor, and 8GB RAM was used for performing the analysis. The following sections describe the methods in detail.

4.1 Data Collection

Data triangulation is used in this study and the data collected came from the following sources:

- UK cybersecurity incidents dataset
- Questionnaire
- Official documents and online content

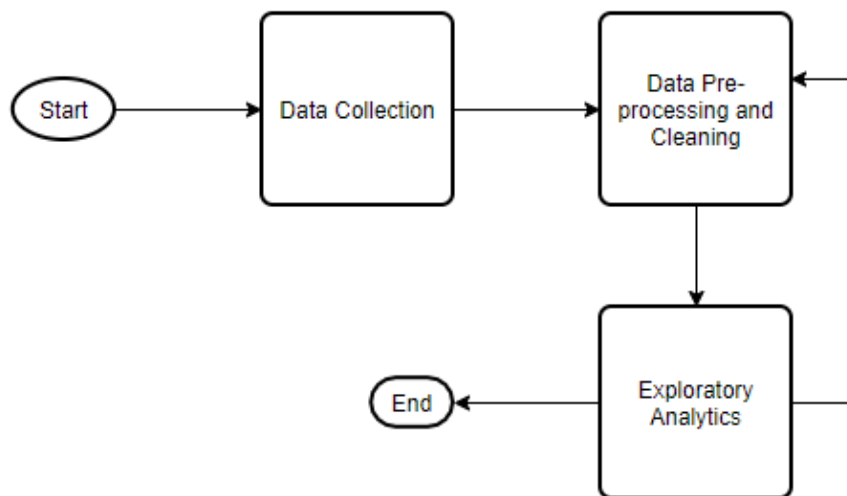
A dataset on cybersecurity incidents was obtained from the UK's Information Commissioner's Office (ICO). The ICO is an independent authority in the UK set up to uphold information rights in the public interest, promote openness by public

1113 organisations and data privacy for individuals [170]. The UK has legislation on
1114 public information access rights, and data privacy protection that makes it possible
1115 to collect data on cybersecurity incidents and make it public. Since Botswana does
1116 not have such a dataset, the UK dataset was used to identify the current
1117 cybersecurity threat trends. These threats were then used as a baseline for
1118 investigating the threats on the Botswana cyberspace.

1119 A questionnaire was designed based on the findings of the UK dataset analysis.
1120 Both open and closed ended questions were used in the survey which was
1121 delivered using the Google Forms platform. The threats identified in the UK dataset
1122 analysis were used as possible answers to the closed ended question on threats
1123 registered by the organisations. Options were also made available for participants
1124 to give answers to open ended questions. The same approach was also used when
1125 designing questions on cybersecurity strategies. Some common strategies were
1126 provided as answers to the question on strategies implemented by the organisation,
1127 and open-ended questions were also used to give the participants the opportunity
1128 to provide answers in their own words.

1129 Legislation on cybercrime from Botswana, South Africa and the UK was also
1130 textually analysed to make comparisons between them. The R package for the
1131 Quantitative Analysis of Textual Data (quanteda) [171] was used to quantitatively
1132 compare the legislations. Word clouds and frequency charts were produced. Online
1133 content from the news, speeches by government and industry players were also
1134 analysed using the quanteda package.

1135 4.2 Data Analysis



1136

1137 *Figure 1: Exploratory Data Analysis*

1138 The data analytics approach used in this study is summarized in figure 1. First step
1139 in the approach is data collection. Data collection was carried out aligned to the
1140 objectives of this study as already described in section 4.1. Data was cleaned both
1141 manually on Microsoft Excel and using R tools. Exploratory data analytics was
1142 carried out on the dataset to produce charts that were used to analyse trends. Text
1143 analysis was done as described in section 4.1.

1144 4.3 Dataset pre-processing and cleaning

1145 The ICO dataset contained both cybersecurity incidents and non-cybersecurity
1146 incidents. The non-cybersecurity incidences were ignored and removed because
1147 they fell beyond the scope of this work. Both R and Microsoft Excel were used for
1148 data preparation and cleaning. R packages like tidyverse and ggplot2 were used
1149 for cleaning the data and for producing charts, respectively. The following steps
1150 were taken for data preparation and cleaning:

- 1151 1. Deleting columns with non-cyber instances (they were beyond the scope of
1152 the research).
- 1153 2. Deleting other irrelevant data columns.
- 1154 3. Rearranging the columns for easy analysis.
- 1155 4. Removing NA values.

1156 4.4 Web and Document Scraping

1157 Tools that were used for web scraping included a SelectorGadget Google Chrome
1158 extension that was added to the web browser to make analysis of webpages easier.
1159 SelectorGadget is used to make CSS (Cascading Style Sheet) selector generation
1160 and discovery easy on complex websites. R packages used for scraping included
1161 rvest and xml2. The read_html function which takes in a webpage URL (Unified
1162 Resource Locator) was used to return an XML (Extensible Markup Language)
1163 document of the webpage. The SelectorGadget makes it easier to identify and
1164 select specific elements from the webpage to form the text corpus for analysis. A
1165 dataframe was made from the extracted web elements to form a dataset.

1166 Text analysis was easily performed on the corpus. The text mining package tm was
1167 used together with quanteda to clean-up the data and perform some text
1168 processing. Using the tm_map function of the tm package, punctuation, numbers,
1169 stop words and white spaces were removed from the corpus. Parallelism that is
1170 provided by tm_parLapply_engine function was used to speed up processing on
1171 the large text corpora. This enabled all eight cores of the processor to be used, and
1172 text processing was done instantly. Specifically, building the term document matrix
1173 was greatly improved using parallelisation. The corpus was analysed for frequency
1174 of words and visualised using word clouds and bar plots. Co-occurrence analysis
1175 was also performed to find the relationship in word terms.

1176 Document scraping followed a similar procedure using R's text mining package tm
1177 and quanteda. The pdftools library was used for importing the files into R and
1178 minimal corpus cleaning was done in order to preserve the text for analysis. Both
1179 traditional (manual) reading heuristics and R's heuristics were used to analyse the
1180 corpora.

5. RESULTS

5.1 UK Dataset Analysis

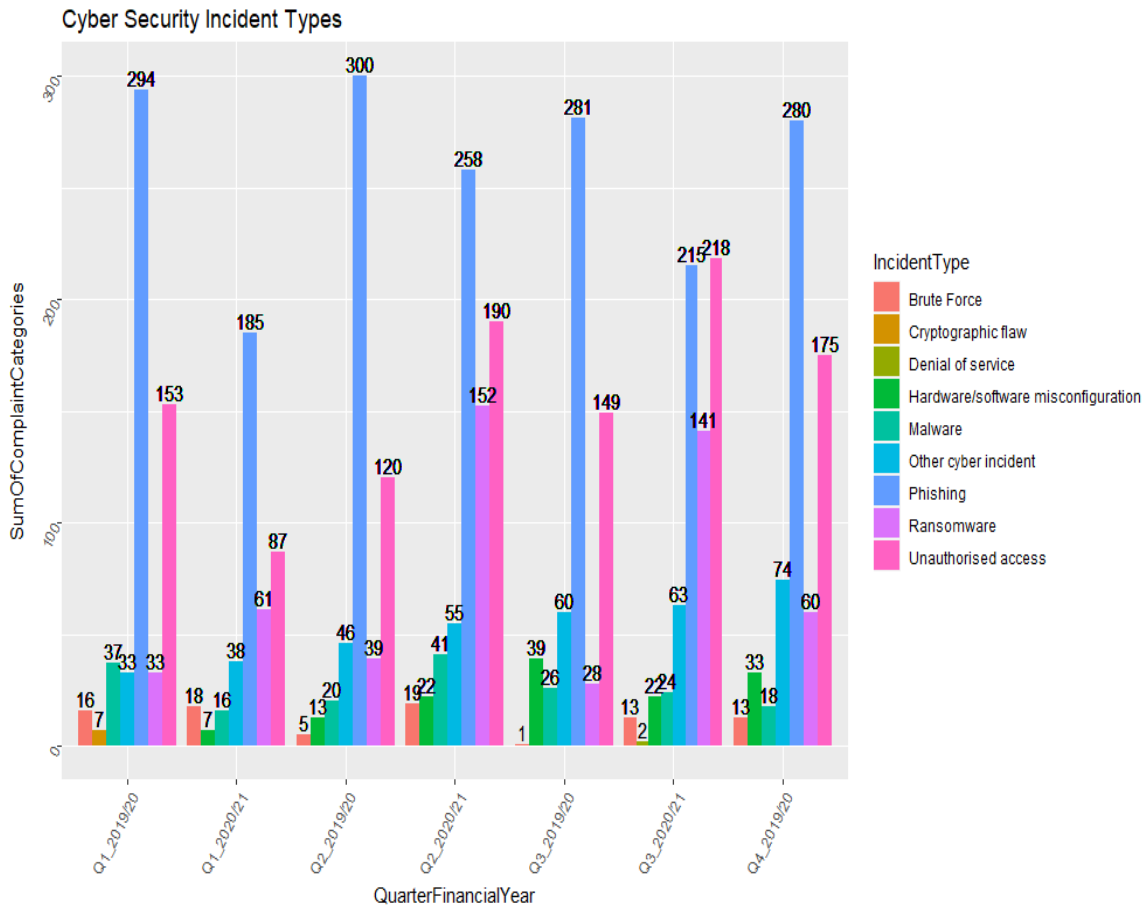


Figure 2: Grouped Bar Chart Showing Quarterly Cyber Incidences

Figure 2 shows the quarterly sums of cybersecurity related complaints in the UK dataset. The data is divided into seven quarters showing the cyber incidents that were reported during each quarter. Phishing was the highest recorded cyber incident for all the quarters. However, during Q3_2019/20 unauthorised access recorded more than phishing. Phishing consistently had the highest record for incidents throughout the quarters followed by unauthorised access. Phishing is usually carried out as an untargeted type of attack where an attacker indiscriminately targets as many devices, systems, and users as possible [34]. However, this is not to say that phishing attacks are never targeted (hence spear phishing). Phishing usually requires a victim to send sensitive information by responding to an email. Social engineering tactics such as phishing are being used

1195 more frequently because attackers consider people as the weak link in cyber
1196 systems [34].

1197 According to a Check Point [36] 2020 cybersecurity report, phishing is the top attack
1198 vector. It involves the use of emails, SMS texting attacks, messaging on social
1199 media, and gaming platforms. Emails are on top of the list as the number 1 attack
1200 vector. The use of Software-as-a-Service (SaaS) based email has spiked email
1201 phishing attacks [36]. Attackers can obtain a victim's email credentials and study
1202 their activity for two weeks and then craft a message to lure them into giving up
1203 personal information or money [36]. According to [36] phishing is expected to
1204 increase in sophistication luring unsuspecting victims to click on malicious links.
1205 Other phishing attacks lure victims into installing malware into their devices.
1206 According to [36], in 2019 mobile banking malware increased by 50% compared to
1207 2018. This is because the mobile banking malware is easy to develop, and it works
1208 by searching for banking app in the infected device and displays a fake overlay.
1209 Once the user enters their credentials they are sent directly to the attacker. The
1210 malware developers usually sell the malware to anyone who is willing to pay for it
1211 [36].

1212 The 2020 annual review by the UK's National Cyber Security Centre (NCSC)
1213 observed that phishing attacks were exploiting people's worries over the corona
1214 virus [6] [61]. Various attacks were identified selling bogus Personal Protective
1215 Equipment (PPE) and even vaccines, and bogus medical charities seeking
1216 donations [6] [61]. The NCSC [6] blamed the Russian cyber actors known as APT29
1217 for spear-phishing. Russian actors were also blamed for custom malware that was
1218 used to steal valuable intellectual property related to coronavirus vaccine
1219 development [61]. Phishing attacks were also seen to be combined with malware
1220 attacks whereby clicking a link installed malware or led to loss of data [6] [61]. The
1221 NCSC responded by providing the UK with guidance on how to respond to phishing
1222 attacks, as well as launching a Suspicious Email Reporting Service (SERS). The
1223 SERS led to a significant identification of previously unknown suspicious domains
1224 and their removal [6].

1225 On the other hand, brute force was the least recorded cyber incidence type for the
1226 year 2020/21 (figure 2). Figure 3 is a code snippet showing the results after running

the MAX and MIN functions on the dataset. The functions returned 300 phishing incidents for the MAX function, and 1 brute force incident for the MIN function. According to information on the UK's NCSC website [172], the US and the UK agencies partnered to expose a global brute force campaign against hundreds of governments and private organisations (mostly in the US and Europe) blamed on the Russian military intelligence, the GRU (General Staff Main Intelligence Directorate) [6] [61].

The advisory by the US and UK duo recommends rolling out Multi Factor Authentication (MFA) to protect against these attacks. Other defences recommended by the National Security Agency (NSA) [173] include timeout and lockout features, mandatory complex passwords, implementation of a Zero Trust Model that uses additional attributes, analytics for detecting anomalous access, denying unusual anonymised accesses from commercial virtual private networks (VPN's) and The Onion Router (TOR) [173]. More recently the NCSC warned about pervasive style of hacking around the world on Microsoft Exchange Server by Chinese state backed actors [174]. The attack had the capacity to perform large scale acquisition of personally identifiable information and intellectual property. The NCSC [172] also warned that Microsoft has also identified password spraying and brute force activity which is suspected to be by another APT group called NOBELIUM.

```
> max(table_cs$SumOfComplaintCategories)
[1] 300
> min(table_cs$SumOfComplaintCategories)
[1] 1
```

Figure 3: Code Snippet for max and min values

Figure 4 is a stacked bar chart showing cyber incidents in different sectors of the UK economy. The per sector analysis also revealed that phishing was the top vector of attack across all sectors. This was followed by unauthorised access. Twenty-two sectors in total of the UK economy were analysed in the dataset. "General business" sector recorded the most cyber incidents followed by "Retail and manufacturing". There was an occurrence also of reports which were not assigned to any specific sector, this unassigned sector recorded the least number of cyber incidents.

Perhaps this indicates that the hardest hit sectors need more cybersecurity support. This sort of information is important for CSIRT teams as it helps them to better support their constituents.

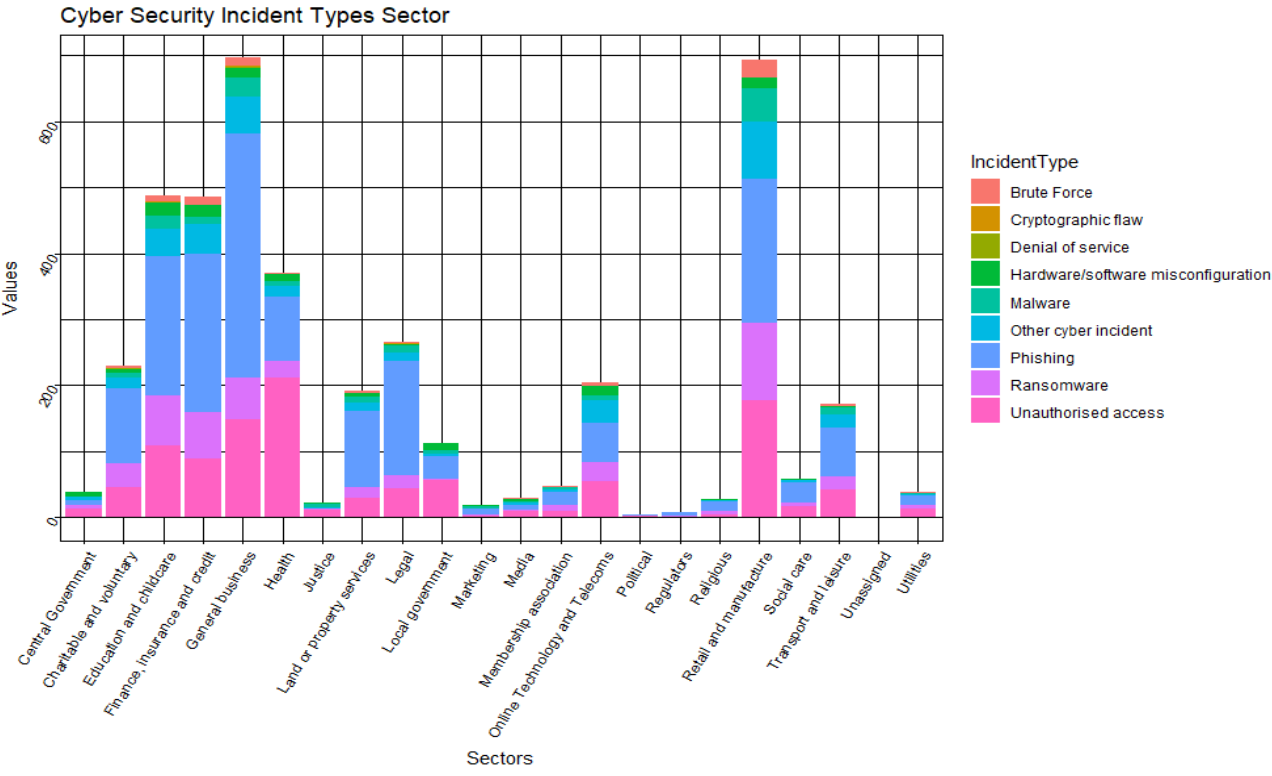


Figure 4: Stacked chart for cyber incidents per sector

Figure 5 shows the code snippet showing maximum and minimum number of cyber incidents per sector. The maximum record was 123 instances for phishing (in the general business sector), and the minimum was for the unassigned sector which only recorded 1 incident of unauthorised access. It can still be observed that even per sector, phishing still stands out. The “general business”, “land or property services” “retail and manufacturing”, “finance, insurance, and credit”, “education and childcare”, “legal”, “online technology and telecoms” and “health” also reported high cyber-attack incidents.

```
> max(table_cs$values)
[1] 123
> min(table_cs$values)
[1] 1
```

Figure 5: Code Snippet for max and min values per sector

Figure 6 is a bar chart showing frequency for the different cyber incidents. Phishing had the highest frequency followed by unauthorised access, and denial of service had the lowest frequency.

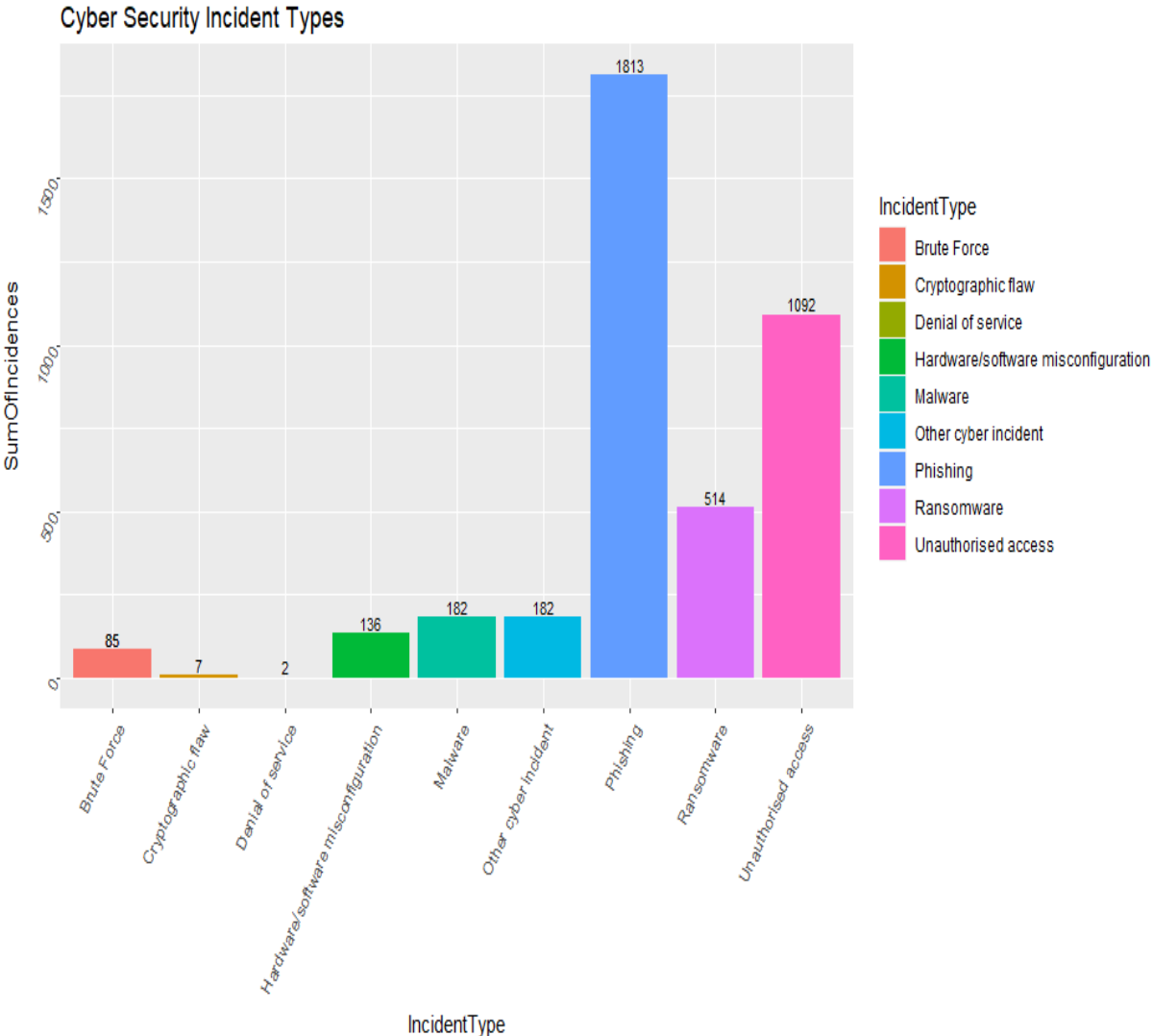


Figure 6: Bar graph showing frequency of cybersecurity incidences.

In figure 6, ransomware had the third highest record for cyberattack incidents. The Check Point [36] 2020 report stated that sophisticated and targeted ransomware escalated in 2019. These attacks can shutdown businesses, hospitals, and governments. Ransomware attacks impact was so devastating that the Federal Bureau of Intelligence (FBI) softened its stance on paying ransom stating that businesses should evaluate their options to protect their stakeholders, customers, and employees [36]. This prompts that organisations should adopt prevention strategies in addition to detection and mitigation strategies [36]. The UK's NCSC

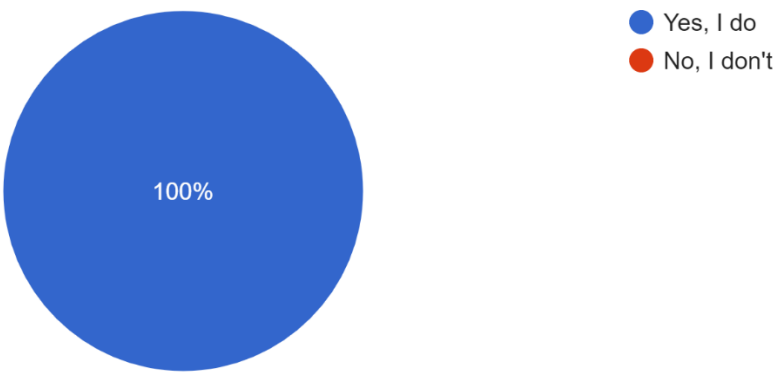
also reported increased ransomware numbers as well as increased sophistication, and aggression [6]. Since threat actors lurk in the systems for weeks studying the target's behaviour and patterns before installing ransomware, sometimes victims find out that their cloud backup is also compromised [6] [36]. Ransomware actors sometimes continue to extort victims after they have paid the ransom by further threatening to expose sensitive data in their hands. Table 3 summarises the recommended countermeasures by the NCSC on the specified attacks.

Table 3: Cyber-attacks and mitigations

Cyber-attacks	Mitigations
Phishing	Suspicious email reporting service [6], Phishing email response guidelines
Ransomware	Security in-depth [6], Backup data (cloud, and of-line storage)
Malware	Security in depth [6]
Brute force	Multifactor authentication, password complexity, login attempts timeout, Zero Trust Model, Prevent unknown anonymised access from VPNs [173]

1291 5.2 Botswana Questionnaire Results

Do you freely consent to participate in this study?
31 responses

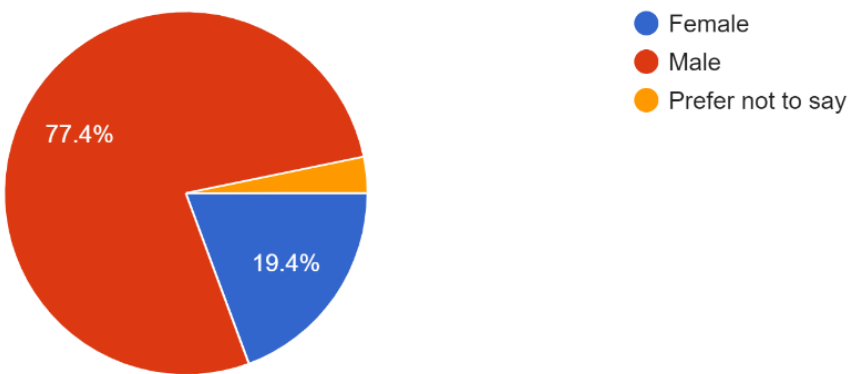


1292

1293 *Figure 7: Number of participants in the study*

1294 An investigation on the cybersecurity threats and strategies in Botswana was
1295 carried out, and 31 people participated (figure 7) in the questionnaire which was
1296 delivered using Google Forms. The participants came from 20 companies in 10
1297 sectors of the economy.

What is your gender
31 responses



1298

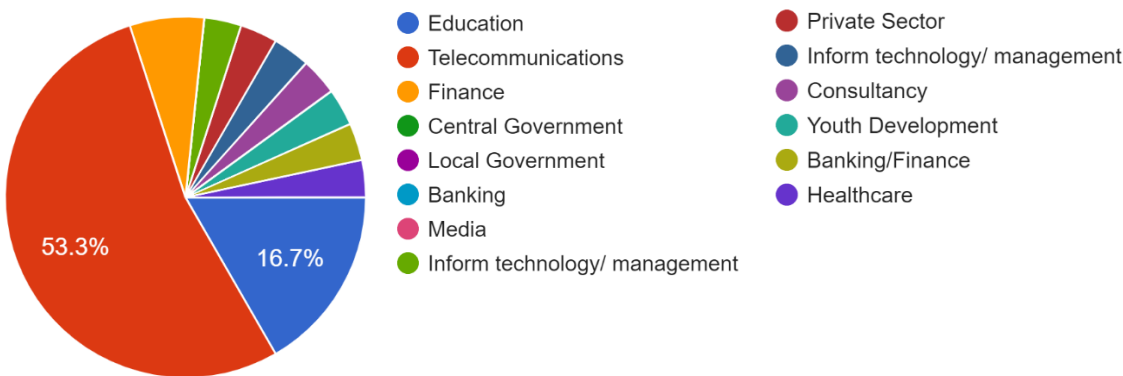
1299 *Figure 8: Pie chart showing gender of participants*

1300 Of the 31 participants, 77.4% (24) were male, 19.4% (6) were females, and the
1301 remaining 3.2% (1) did not disclose their gender (figure 8). It is concerning that
1302 women were not well represented in the study. However, [8] indicated that there is

1303 a shortage of women in the cybersecurity sector in Botswana, and more needs to
1304 be done to address this need.

Which sector best describes your organisation?

30 responses

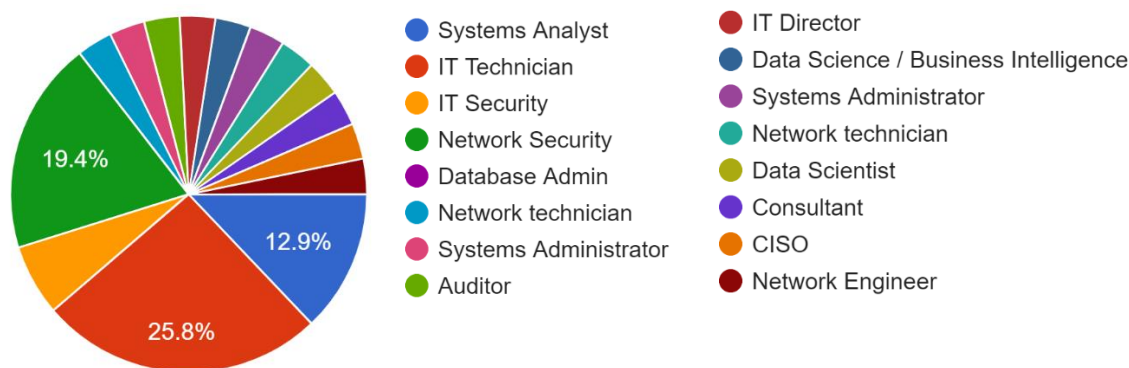


1305 *Figure 9: Percentage of participants by sector*

1306 Figure 9 is a pie chart showing the participants of the study according to their sector.
1307 53.3% (16) of the participants were from the Telecommunications sector, 16.7% (5)
1308 from Education, and 6.7% (2) were from the Finance sector. The remaining sectors
1309 which each had a representation of 3.3% (1) were Healthcare, Banking/Finance,
1310 Youth Development (non-governmental), Consultancy, Information Technology
1311 Management, Software Development, and Private Sector.

What is closest to your job role

31 responses



1312 *Figure 10: Job roles of interviewees*

Figure 10 above shows the different job roles of the study participants. 25.8% (8) of the participants were IT Technicians, 19.4% (6) hold Network Security roles, 12.9% (4) work as System Analysts, 6.5% (2) hold IT Security roles. The remaining participants each had a share of 3.2% i.e., 1 person and they identified as Auditor, Software Engineer, Software Developer, IT Director, Data Science/Business Intelligence, Systems Administrator, Network Technician, Data Scientist, Consultant, CISO, and Network Engineer respectively. The participants were also from different academic backgrounds in information technology and cybersecurity as shown in figure 11. 71% (22) had bachelor's degrees as their highest qualification, 16.1% (5) had master's degree, 6.5% (2) had diplomas, 3.2% (1) had an honours degree, 3.2% (1) had certificate. An interesting observation also is that none of the participants had qualifications at the doctoral level. Of the 31 participants, 23 had industry certifications and 15 had cybersecurity related industry certifications.

What is your highest qualification?

31 responses

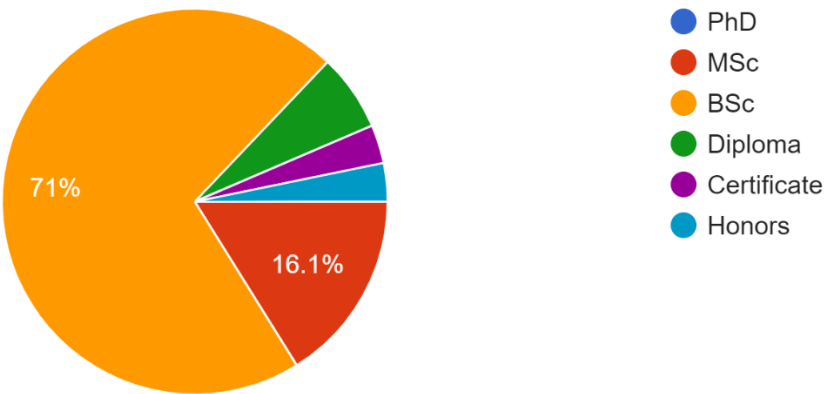


Figure 11: Participants by qualification

Based on figure 12, the survey participants from Botswana indicated that malware (67.7%) was the most frequent cybersecurity incident in their organisations followed by phishing (58.1%), unauthorised access (48.8%), denial of service (41.9%) and ransomware (38.7%), respectively. Other cyber breaches were due to hardware and software misconfigurations (29%), brute force (16.1%), and cryptographic flaws (3.2%) respectively. Insider threat accounted for 19.4% of attacks and one

participant identified web crawlers and bots as the type of malware that affected their organisation. Finally, one participant declined to be specific about cyber threats experienced by their organisation, citing fears that a non-disclosure agreement will be breached. These fears are sometimes caused by fear of losing customers and financial liability. However, such fears may be a challenge to a national multi-stakeholder response to cyber threats. A national CIRT is usually mandated to collect such information, and usually has mechanisms (legislatively and in terms of processes) in place to address such concerns. Therefore, it is promising that collection of data on threats by the Botswana CIRT and publicising the resulting dataset will improve cybersecurity research efforts in Botswana. Research efforts will also not be limited, and in that regard more cybersecurity solutions may be developed by the industry and academia.

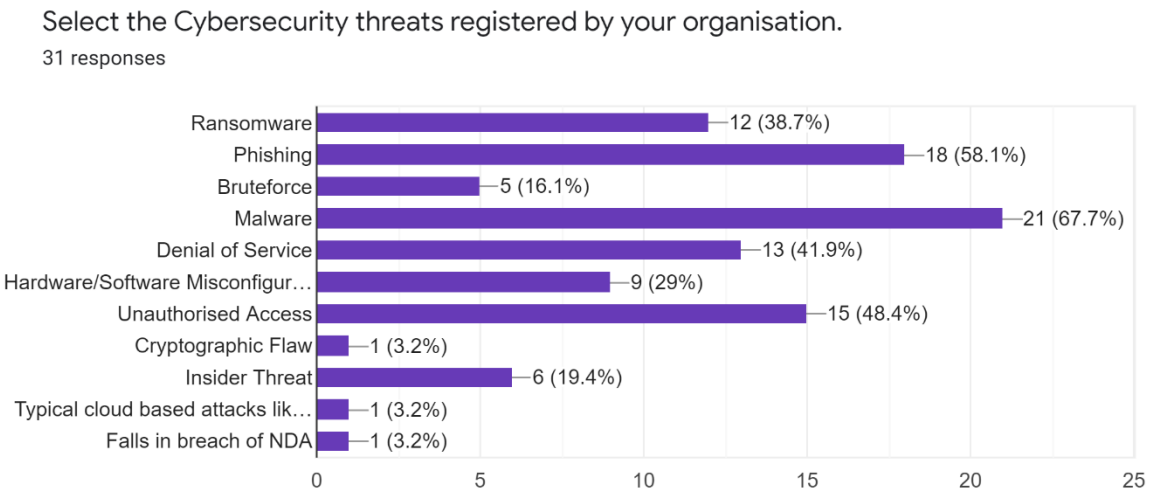
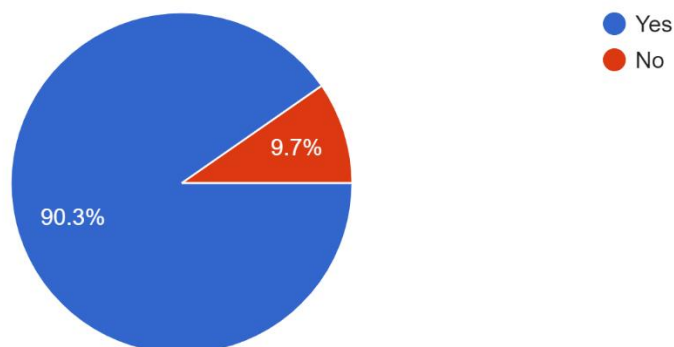


Figure 12: Cybersecurity attacks in Botswana

Compared to the UK threats (figure 6) which had phishing as the top vector of attack, the results from Botswana (figure 12) are not too far apart as phishing still comes second in the Botswana survey. Unauthorised access and ransomware also appear with relatively higher numbers similar to the UK dataset.

Are systems (software and hardware) in your organisation regularly updated?

31 responses



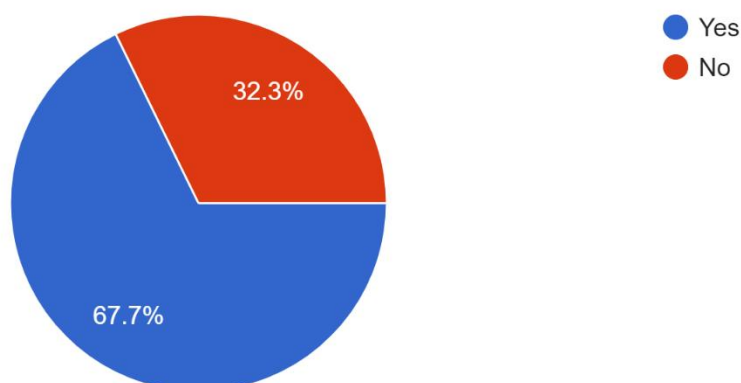
1353

1354 *Figure 13: Percentage of organisations that regularly update systems*

1355 On the question of system updates (figure 13), 90.3% (28) participants indicated
1356 that systems in their organizations are regularly updated, while 9.7% (3) indicated
1357 that their systems are not regularly updated. The organisations that do not update
1358 systems regularly are at a higher risk of attacks that target vendor vulnerabilities.

Does your organisation have a Bring Your Own Device (BYOD) Policy?

31 responses



1359

1360 *Figure 14: Percentage of organisations that have BYOD policy*

1361 In figure 14, 67.7% (21) participants indicated that their organizations have a BYOD
1362 policy and 32.3% (10) indicated that they do not. The organisations that do not have
1363 a BYOD policy in place should move swiftly to put in place controls for employees'
1364 personal devices that they use to connect on the work network. This is especially
1365 important considering stay at home restrictions introduced by the pandemic have
1366 made remote work the new normal of work. Increasingly more employees are using

their devices both at home and at work for carrying out organisational duties. Most of the time users' devices are not configured with the best controls to protect them and the organisation. Measures should also be put in place to secure the VPNs that users use to connect to the corporate networks, as well as measures for preventing connections from unrecognised VPNs.

Does your organisation have a cyber incident reporting mechanism in place?
30 responses

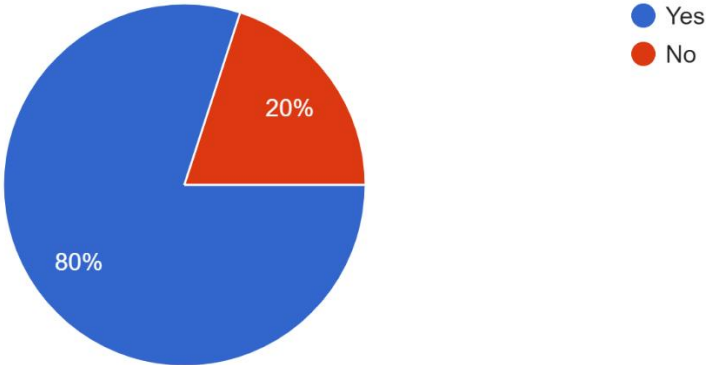


Figure 15: Percentage of organisation with cyber incident reporting mechanism

Figure 15, 80% (24) of the participants indicated that they have a cyber incident reporting mechanism compared to the 20% who do not. Such a reporting mechanism is important as it helps the organisation to identify threats and to respond to them with agility. A lack of a reporting mechanism may mean that responding to threats is not organised and more threats go undetected.

Does your organisation run backups on important data?
31 responses

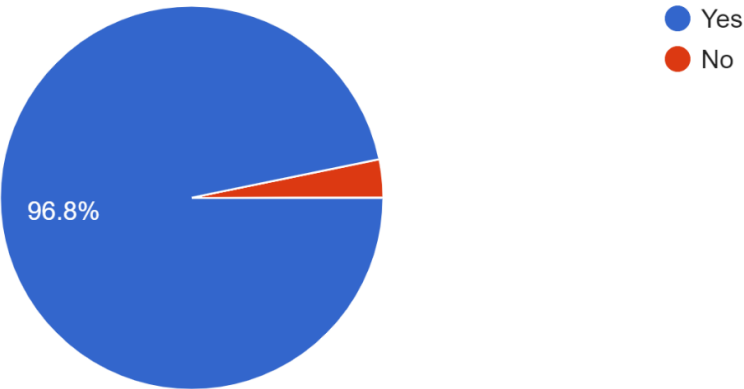


Figure 16: Percentage of organisations that run backups on important data

In figure 16, almost all the participants (30 out of the 31) responded that their organisations run backups on important data, while one indicated that their organisation does not run backups on important data. Running backups on data is important as it helps protect organisations against attacks such as ransomware. It is also important to rely on multiple layers of backup storage such as tape and cloud storage. This is because attackers sometimes compromise online backups when they carry out an attack.

Does your organisation have a password complexity policy?

31 responses

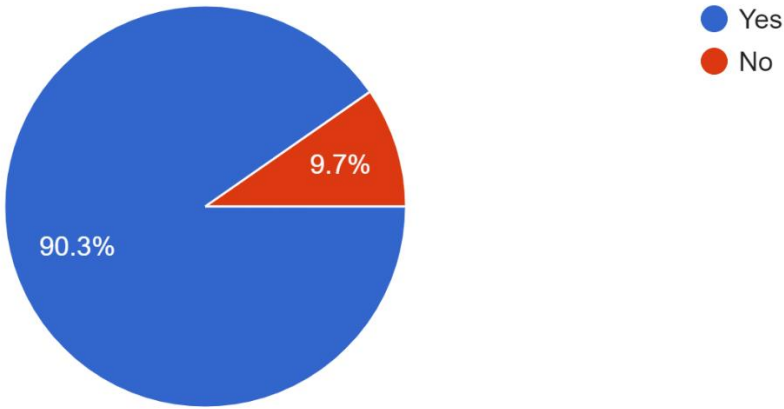
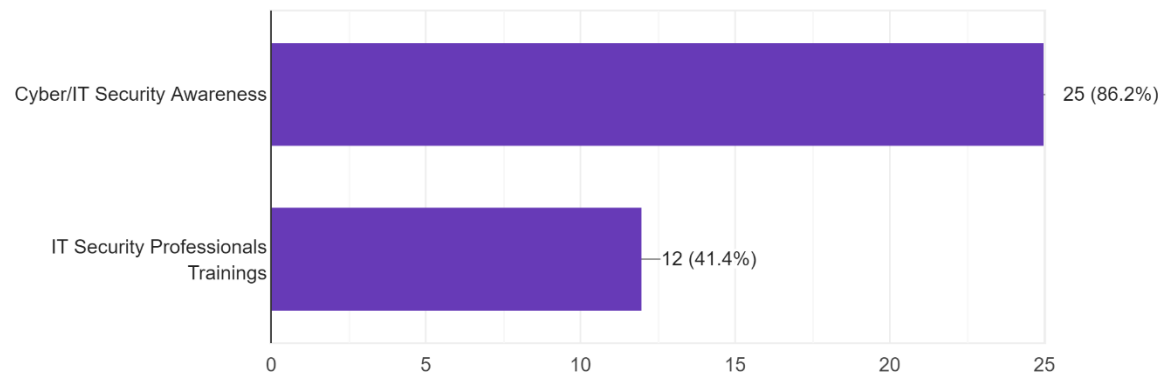


Figure 17: Percentage of organisations that have password complexity policy

Out of the 31 participants of the study, 3 indicated that their organisations do not have a password complexity policy (figure 17). This is a standard policy and an important one since people are considered the weakest link by attackers. A password complexity policy makes it harder for threat actors to launch successful brute force and social engineering attacks on a system.

Which of the following does your organisation provide?

29 responses



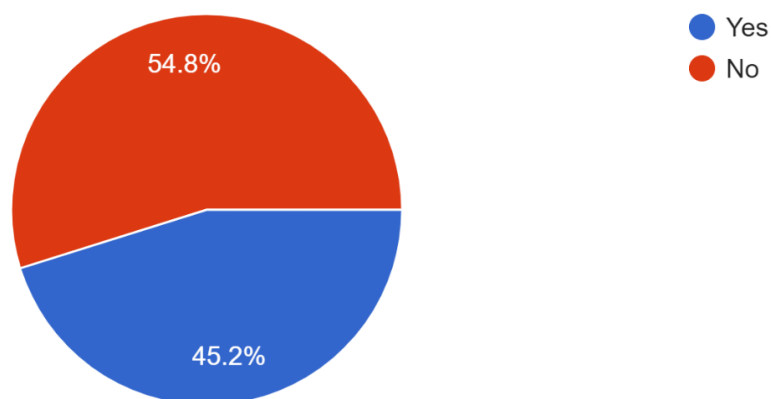
1395

1396 *Figure 18: Percentage of organisations that provide cybersecurity trainings*

1397 Figure 18 shows that only 29 participants responded to this question. 86.2% of the
1398 study participants who responded indicated that their organisations provide cyber/IT
1399 awareness campaigns. While this is good for promoting a good cybersecurity
1400 culture, it is concerning that the remaining 14.8% organisations do not have
1401 cybersecurity awareness initiatives in their organisations. As for IT/cybersecurity
1402 professionals training, only 41.4% responded that their organisations provide or
1403 cater for such trainings. It is also concerning that 59.6% of the participants indicated
1404 that their organisations do not provide their staff with professional cybersecurity
1405 training. These trainings are important to equip employees with the necessary skills
1406 to protect themselves and their organisations.

Does your organisation use security in-depth strategy?

31 responses



1407

1408 *Figure 19: Percentage of organisations that use security in depth strategy*

1409 More than half of the participants (17) indicated that their organisation do not use
1410 security in-depth strategy i.e., applying many layers of security to protect their
1411 systems. The remaining 14 participants indicated that indeed their organisations
1412 use security in-depth strategy. Participants who stated that they use a security in
1413 depth strategy were required to answer a follow up question to specify the layers of
1414 security that they apply. The responses however did not capture how security in-
1415 depth is being applied as most participants only gave one security strategy and
1416 some strategies were at a high-level concept. One participant however indicated
1417 that their organisation is compliant with the NIST cybersecurity framework. A
1418 participant in the Software Development industry stated that they use secure coding
1419 practices i.e., security by design and they implement several layers of security on
1420 top of the application such as HTTPS, SSL, backup and recovery, secure hosting,
1421 and complex passwords. Other strategies stated by other participants included the
1422 following:

- 1423 • Regular cybersecurity awareness trainings
- 1424 • Network security training and updating systems
- 1425 • Using multiple firewalls and system audit
- 1426 • Use of antivirus and firewall
- 1427 • Domain security, use of Public Key Infrastructure (PKI) tokens, Remote
1428 Authentication Dial In User Service (RADIUS) for VPN connections
- 1429 • Third party penetration testing
- 1430 • Patch management

1431 In summary, it is necessary for organisations in Botswana to invest in the
1432 cybersecurity of their organisations, by recruiting and continually develop talent in
1433 this area. More effort should also be dedicated towards detecting and identifying
1434 threats in the organisation. While organisations are applying one cybersecurity
1435 strategy or the other, it is important for the organisations to adopt strategies such
1436 as security in depth, thereby reducing the likelihood of a successful attack. This is
1437 important because threat actors use multiple vectors of attack. The national CIRT
1438 will play a big role in closing gaps in less resourced organisations by providing
1439 information on threats and their mitigations, support and advisory in Botswana.

1440 5.3 Online Discussions and Cybersecurity News in Botswana

1441 Analysis of online news and reports was carried out in this study. Web sources that
1442 were selected were limited to reports based on industry professionals, and
1443 government officials. The following section provides brief summaries of the
1444 webpages that were scrapped as well as results from the text analysis.

1445 5.3.1 Sunday Standard

1446 Based on a 2017 report by the Sunday Standard, Botswana ranked 8th in Africa
1447 among ten of Africa’s biggest sources of cyber-attacks [175]. According to the
1448 report, “Botswana is per capita the continent’s biggest source of cyber-attacks” with
1449 just a population of 2.2 million. These conclusions were based on a report by the
1450 African Union Commission and Symantec [7]. A report by Check Point [36] also
1451 found Botswana as the most attacked country out of a list of 117 nations. The report
1452 mentioned different ransomwares (Locky and Cryptowall) and malwares (Conficker,
1453 Sality) that were ravaging organisations across the world. Figure 20 shows a word
1454 cloud visualising frequency of words from the web article, and it can be seen that
1455 the word “attacks” had the highest frequency indicating the emphasis of the article.
1456 The term “malware” can also be seen in the word cloud.



1457
1458 *Figure 20: Sunday Standard report word cloud*

1459 5.3.2 Remarks by the Minister of Transport and Communications – Botswana

1460 A Facebook post on the Ministry of Transport and Communications page showed
1461 remarks that were made by Minister Thulaganyo Segokgo at a Virtual Cybersecurity
1462 Symposium, that was hosted by the Botswana International University of Science
1463 and Technology (BIUST) [176]. In his remarks the Minister mentioned that the
1464 Smart Botswana Strategy aims to promote digitalization of public services. Some of

the government digital projects identified by the Minister include development of National Biometric Identity Card, integration of government ministries systems, online visa applications, and e-learning. The Minister also observed the impact of the Coronavirus pandemic on the ICT landscape citing contact tracing application and other government initiatives. However, the downside, he observed, has also been increased cyber-attacks. In his speech, the minister also commended efforts by both private and public tertiary institutions for raising awareness in cybersecurity issues. Among other things the Minister touched on the issue of capacity building and the need for a multi-stakeholder cybersecurity response. In figure 21, the term “cybersecurity” had a high occurrence in the text corpus. An association was observed between industry, public, and BIUST showing the emphasis the minister placed on partnerships and collaboration. Other associations are between academia, research and cybersecurity indicating the priorities that the minister placed on role academia has to play in cybersecurity initiatives.



Figure 21: A word cloud on the Minister's remarks

5.3.3 Rhodes University Latest News

A master’s in Journalism & Media Studies student, reporting on the 2021 Highway Africa Virtual Conference stated that cyber-attacks against journalists around the world are increasing exponentially [177]. This is because journalist carry out work that challenges those in positions of power including state power. One of the participants of the conference argued that journalists should be equipped with hacking skills to be able to protect themselves from cyber-attacks. A participant from Botswana identified deep fake videos as one of the attacks that are faced by journalists. The Botswana participant further advised that basic journalism skills such as fact checking can protect them from such attacks that lead to fake news.

Figure 22 shows that the author of the article made associations between journalists and cyberattacks. Another association can be seen between cyber-attacks and the occurrence of fake news.



Figure 22: Word cloud on the report from the Rhodes University website

5.3.4 BizTech Africa

A 2019 post on the BizTech website cited that Botswana needs to produce 1000 cyber professionals annually to combat cyber threats [178]. This is compared to the current figure of 20 – 30 new professionals who join the market each year. The report cited that banks are not keen on reporting cybersecurity incidences for fear of losing customers. Another reason mentioned by the report for silence on cyber-attacks by organisations is that some attacks are carried out by insiders and organisations feel embarrassed to report about that. Figure 23 shows the frequency analysis of the BizTech article and “cyber”, “security” and “cybercrime” are some of the high occurrence words in the text.

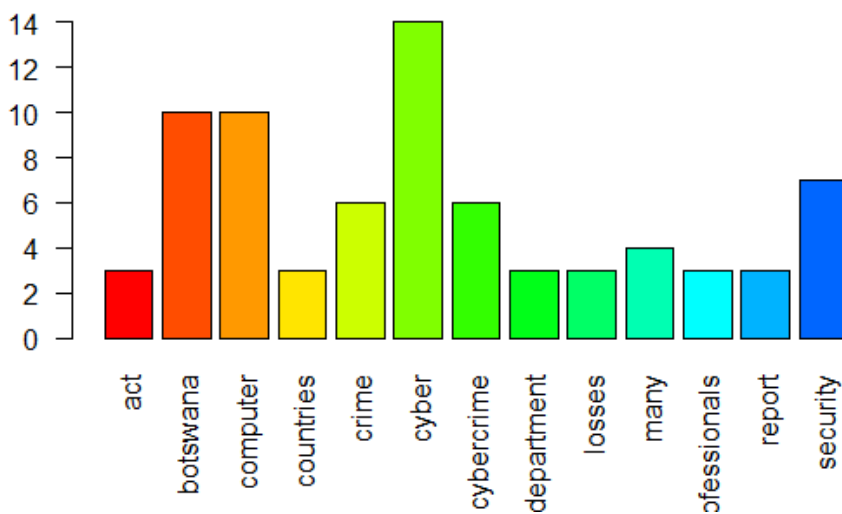


Figure 23: Frequency chart for the BizTech article

5.3.5 ASC Services Botswana Website

ASC Botswana predicted that the technological changes brought by Corona pandemic such as remote work are here to stay [179]. Hackers are already taking advantage of the weak security measures in home networks and systems, and these are being compromised to access organisations. The post identified ransomware as a dominating threat in the world of IT security. Cybercriminals are also using COVID19 themed phishing tactics to lure victims. ASC identified modernisation of data protection as a critical factor for ensuring business continuity and countering ransomware. ASC recommends cloud volumes backup to protect against unauthorised encryptions on data. Other recommended solutions include software-defined solutions and using an Air Gap (tape storage) to make backup inaccessible. The advantage of these solutions is that they make data invisible to ransomware. Figure 24 shows that the ASC article associated ransomware protection to data protection using backup solutions. The term “data” had a high frequency, and it can be concluded that the article focused on ransomware attacks that target data.



Figure 24: ASC Services Botswana website word cloud

5.3.6 Botswana Guardian Website

A 2019 report by the Botswana Guardian reporter indicated that Botswana cybersecurity stakeholders were expected to meet in January 2019 to discuss progress on cybersecurity initiatives as well as the NCS [180]. According to the reporter Botswana Police Service (BPS) registered 143 cybercrime cases during the period of 2015 – 2018. In addition to that the report added that BPS is faced by a challenge of a shortage of digital forensic examiners which inhibits prosecution of

criminals. Based on the report, by 2018 80% of the 30 certified practicing digital forensic examiners were employed by law enforcement agencies in Botswana. Figure 25 visualises the frequency of words in the article in a word cloud. The term “cyber” had the highest frequency and was associated to words like government and crime indicating the emphasis of the article on cybercrime.



Figure 25: Botswana Guardian article word cloud

5.3.7 The Patriot on Sunday

The Patriot on Sunday ran a story on the 5th Annual African Cyber Conference. Commenting on the issue, the managing director of African Cyber Security – ACS (a Botswana cybersecurity company) said the conference is a good platform for raising awareness on issue of cybersecurity [181]. He further identified a lack of cybersecurity professionals and lack of cybersecurity integration in local institutions as some of the major issues in Botswana. An official from Serianu (another cyber security company in Botswana) also commented that the cybersecurity in Botswana is weak and highlighted that a lot of damage happened since the election season. Figure 26 shows the frequency of words in the text corpus and “cyber”, “cybercrime”, “crime” and “security” had high frequencies indicating the focus of the article.

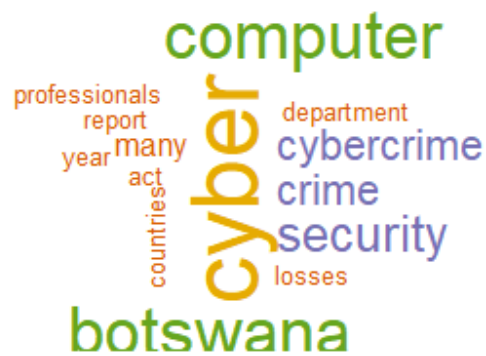


Figure 26: The Patriot on Sunday article's word cloud

5.3.8 Mmegi Website

A 2016 Mmegi reporter interviewed the Director of Public Prosecution (DPP) at the Internet, Cyber Security, and Information Systems (ICSIS) conference [182]. The DPP mentioned that cybercrime is a serious threat in Botswana and gave the example of an incidence in which ICT was used to execute a money heist on the Central Medical Stores. For the solution part, the DPP talked of building technical capacity in ICT and establishment of legal framework. Figure 27 shows frequency of the terms in the article and the words “cyber” and “crime” had the highest frequency indicating the article’s focus.

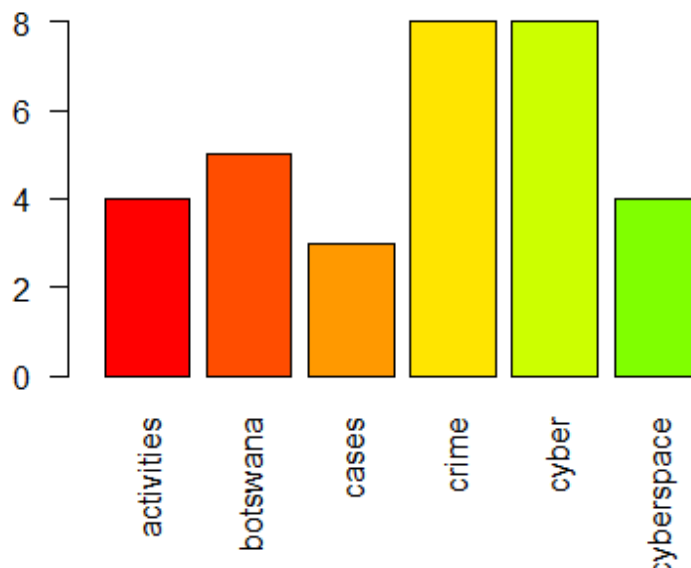


Figure 27: Bar chart for the Mmegi interview with the DPP

1565 5.3.9 Mmegi Website

1566 Still in 2016, Mmegi ran another story on cyber bullying and interviewed the
1567 telecoms regulator for Botswana (BOCRA) deputy director of corporate
1568 communications [183]. On his part the deputy director stated that BOCRA always
1569 undertakes initiatives to raise awareness on the safe use of the internet. According
1570 to the report the regulator has some annual activities educating the public on cyber
1571 bullying. The word cloud for the article is depicted in figure 28, and the article's
1572 focus is on cyberbullying as it had high frequency.



1573

1574 *Figure 28: Mmegi interview with BOCRA word cloud*

1575 5.3.10 Committee of Supply Speech (2021/2022)



1576

1577 *Figure 29: Minister's speech on the Committee of Supply*

1578 The Minister of Transport and Communications delivered a message on the
1579 Committee of Supply and touched on the important issue of cybersecurity [118].

The word cloud in figure 29 is made from the part of the speech on cybersecurity, and “strategy” and “cybersecurity” were some of the high frequency terms. The minister also used the term “ministry” frequently to assume responsibility by his ministry for cybersecurity initiatives. This speech was important as it laid foundation for discussions on the issue from both the ruling and opposition parties. In his speech the minister mentioned key cybersecurity strategies that the Ministry was engaged in. These included cybersecurity professionals’ recruitment and training, and delivery of the Digital Forensics Laboratory. The Minister also spoke of the CIRT team in the future tense perhaps expressing plans that are underway or in the future as can be seen in the kwic output in figure 30. The minister also mentioned that his ministry is collaborating with third parties such as EU Cyber-4-Dev and E-Botho to develop the cybersecurity laws and cybersecurity professionals’ training respectively.

```
Keyword-in-context with 6 matches.
[text10, 178]      remains rudimentary levels just e-Education | will | working responsible Ministries support realising
[text10, 263] key stakeholders kick-start implementation Ministry | will | work key stakeholders working committees
[text10, 419] infrastructure safeguard customers online COMM-CIRT | will | responsible advising responding cyber security
[text10, 493]      Incident Response Team BW- CIRT | will | coordinate response cyber security issues
[text10, 515]      areas enacting cybersecurity laws BW-CIRT | will | coordinate sectoral CIRTs National Cybersecurity
[text10, 543]      established COMM-CIRT BW-CIRT sectors economy | will | also establish sectoral CIRTs Currently
```

Figure 30: Kwic output for “will” as a keyword

While commenting on the minster’s speech, a member of parliament from the opposition highlighted that cybercrimes on social media, such as the use of fake accounts for impersonating others on Facebook, and cyberbullying are rampant [118]. The Member of Parliament further stated that the police have not been successful at stopping these criminals. Although these discussions are still at an early stage at parliamentary meetings, it is promising that these will take an advanced form in the future and more will be done in this area. It may also seem necessary in the future to capacitate members of parliament on cybersecurity.

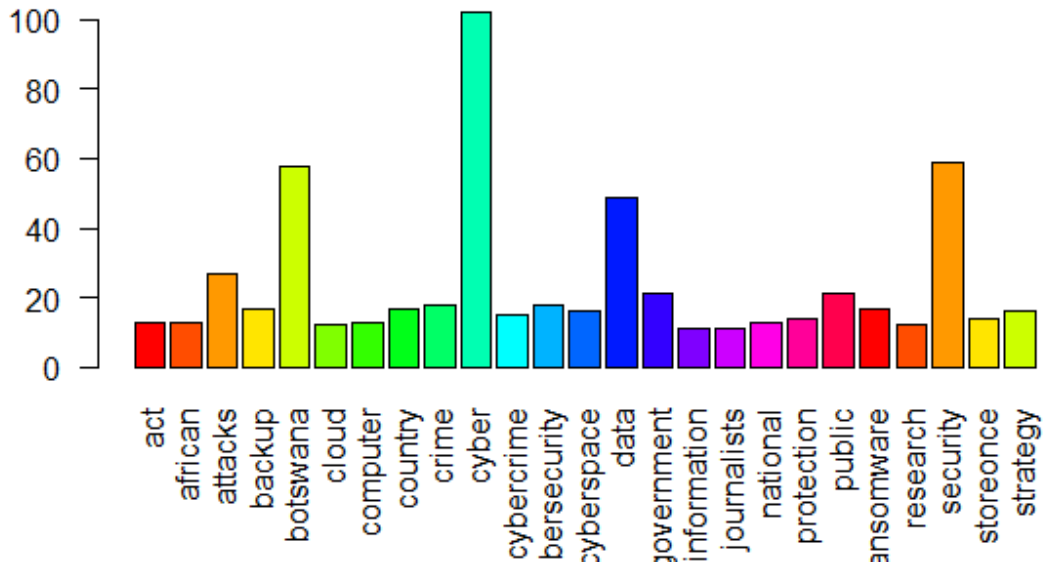


Figure 31: Frequency analysis of the combined corpora of all webpages

A frequency analysis (frequency set at >10) on the merged text corpora of all the scraped webpages is shown in figure 31. The term “cyber” had a high occurrence in the whole corpora of scraped webpages. Other terms of high frequency included “data”, “Botswana” and “security”. It can be seen from the frequency analysis that most commentators in Botswana associate cybersecurity to data. Therefore, cybersecurity discussions in Botswana are concerned mostly with data protection. There is however no mention of critical infrastructure cybersecurity in the articles. A further inspection of the document term matrix revealed that the term “malware” had a frequency of 5 (hence not showing on figure 31) on the whole corpora compared to ransomware which had a frequency of 20 occurrences on the whole corpora. Using the frequency metric, compared to the ICO dataset (figure 6), ransomware still has a more occurrence than malware even for the UK.

A close examination of the corpus for the term awareness using the kwic function (kwic stands for keyword in context) of the quanteda library is shown in figure 32. Analysis of the console output in figure 32 and the words which appeared together with awareness include “raising awareness”, “stimulating awareness”, “cyber security awareness”, “public awareness initiatives”, “promote cyber awareness” and “promoting cyber security awareness”.

```

[text1, 25] week is set to be a good platform for raising awareness |
[text8, 14] to indicate that ACS on its concerted efforts of stimulating awareness |
[text15, 13] said although Botswana is not much effective in cyber security awareness |
[text58, 25] It was also aimed at the public, to raise awareness |
[text74, 38] because the month is recognised internationally as the cyber security Awareness |
[text82, 924] Cyber, among others. we have seen other public awareness |
[text82, 1071] enhance cyber capacity and capability 3. To promote cybersecurity awareness |
[text82, 1174] local and international partners have already started with promoting cyber awareness |
[text82, 1246] building capacity and capability as well as promoting cyber security awareness |
[text82, 1351] two strategic objectives on building capacity and promoting cyber security awareness |

or interest on the important emerging issue of Cyber Security
on cyber security and its associated effects, they have
, it is crucial to appreciate that the country enacted
and build capacity among them to safeguard against cyber threats
month.
initiatives from civil society such as eBotho and their anti-cyber
4. To foster cyber security research and development 5
and building capacity. Following the approval of the strategy
among members of the public. A report by one
. I trust all of you here will be cyber
> |

```

Figure 32: Console output for keyword in corpus function using the term "awareness"

Table 4 shows a summary of the threats and mitigations identified from the web sources. The attacks identified in table 4 are also covered in table 1 and as such those mitigations also apply here.

Table 4: Cyber Threats and Mitigations from Online Posts

Threats	Mitigations
Ransomware	Cloud and offline backup [179]
Malware	Cybersecurity awareness [183]
Cyber bullying	Cybersecurity awareness [183]
Lack of cybersecurity professionals	Professional's training [54,55]
Cyber-attacks (and deep fakes) on journalists	Hacking skills training, cybersecurity awareness, traditional fact checking to protect against deep fakes [177].

1630 5.4 Analysis of Cybercrime Acts

1631 Since Botswana has enacted laws to deal with cybercrime, the cybercrime act for
1632 Botswana was analysed for similarity with similar acts in South Africa and the UK.
1633 High frequency words were identified in the corpora and analysed. Additionally,
1634 frequent terms were analysed for context using the kwic function.

1635 5.4.1 Botswana Cybercrime and Computer Related Crimes Act of 2018



1636

1637 *Figure 33: Word cloud produced from Botswana Cybercrime Act*

1638 On frequency analysis of the Botswana cybercrime act corpus the terms
1639 “computer”, “data”, “person” and “system” had higher frequencies, respectively. The
1640 maximum number of words on the word cloud in figure 33 was set at 50.

	feature	frequency	rank
1	computer	151	1
2	data	77	2
3	person	75	3
4	system	70	4
5	exceeding	46	5
6	offence	36	6
7	act	36	6
8	access	33	8
9	imprisonment	26	9
10	term	26	9
11	liable	24	11
12	fine	24	11
13	years	24	11
14	service	23	14
15	information	23	14
16	programme	21	16
17	part	19	17
18	communication	18	18
19	order	18	18
20	commits	18	18
21	unauthorised	15	21
22	material	15	21
23	botswana	14	23
24	child	14	23
25	includes	13	25
26	police	12	26
27	director-general	12	26
28	officer	12	26
29	pornography	11	29
30	commissioner	11	29

> |

Figure 34: Frequency ranking of terms for Botswana Cybercrime Act

Figure 34 shows the top 30 most frequent features in the corpus. The first top 3 features i.e., “computer”, “data”, “person” are further analysed for frequency with other terms, and for context using the kwic function to see whether frequency of a term means importance of a term.

Keyword in Context Analysis for the Feature “Computer”

Markers	Jobs	
access to a	computer	or computer system
a computer or	computer	system
access to a	computer	service
interference with a	computer	or computer system
a computer or	computer	system
Damage to a	computer	or computer system
a computer or	computer	system

Figure 35: kwic output for using “computer” as keyword

Figure 35 is the kwic output for the feature “computer”. The Botswana Cybercrime Act uses the phrase “computer or computer system” extensively in the text hence the visualised kwic output’s word cloud in figure 36 shows that the terms “system” and “computer” are clear outliers so to speak. The definition provided by the Cybercrime Act for “computer or computer system” is such that it includes

1655 electronic, magnetic, or optical device or a network of related such devices. By this
1656 definition, a computer can become an object used to commit a cybercrime as well
1657 as a target of a cybercrime. As such both the terms “computer” and “computer
1658 system” have been used extensively in the text in reference to offences that can be
1659 carried out against a “computer or computer system”.



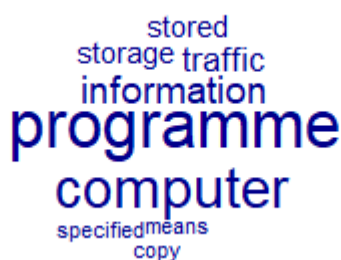
1660

1661 *Figure 36: Kwic output's word cloud for "computer"*

1662 *Keyword in Context Analysis for the Feature "data"*

1663 A kwic function was run on the corpus using “data” as the keyword and the
1664 frequency analysis of the output was visualised using a word cloud (figure 37).
1665 Figure 37 shows that the term “data” occurs together with the term “programme”,
1666 followed by “computer” and information, respectively. The terms “data” and
1667 “programme” appear together as they relate to data stored in a computer. Since
1668 sometimes it becomes easier to analyse text that you know something about, the
1669 Botswana Cybercrime Act was read through. An interesting observation made was
1670 that the Cybercrime Act's definition of “data” includes any “programme suitable to
1671 cause a computer or computer system to perform a function”. A separate definition
1672 is also provided for programme describing the term “as a set of instructions... which
1673 is capable of causing a computer or computer system to achieve a particular task”.
1674 The definitions of the terms “data” and “programme” are provided in the context that
1675 they exist in a computer or computer system either “stored” or in “transit”. These
1676 terms (“data” and “programme”) can either be the object of a crime or subject of a
1677 crime, and when a crime involves either a programme or data it is also related to a
1678 computer or computer system. Hence the term “data” appears around “computer”
1679 frequently. Information is another term found around data. Perhaps this is not
1680 surprising since the Cybercrime Act defines “data as any representation of
1681 information”. Therefore, when they appear together the term “information” is used

1682 to give context in meaning to the term “data” since the act provides two contexts for
1683 the meaning of “data” i.e., information or data; and programme.



1684

1685 *Figure 37: Kwic output for the term "data"*

1686 *Keyword in Context Analysis for the Feature "Person"*

1687 The term person has the third highest frequency in the corpus. A kwic analysis of
1688 the term “person” is visualised in a word cloud, figure 38. Using traditional reading
1689 heuristics, the term appears across the text where it is used in relation to a
1690 perpetrator who has committed offences punishable under the Cybercrime Act.
1691 Figure 38 shows that the terms “computer” and “programme” have higher
1692 frequencies looking at words that appear around the feature “person”. As already
1693 discussed, the term “programme” appears together with “data” most of the time in
1694 the corpus in the phrase “data or programme”. As such when increasing the
1695 distance around the keyword (“person”), data also comes out in the kwic output.
1696 Applying both R and traditional reading heuristics the feature “person” is associated
1697 to a cybercrime by “any means” which contravenes the provisions of the Cybercrime
1698 Act. Additionally, the features “programmes”, “data” and “computer” can be used to
1699 carry out a crime or as the subject of a crime, as already discussed. Hence the high
1700 frequency of these two features around the feature “person” which is punishable for
1701 crimes under the Cybercrime Act. Other terms are “traffic”, “information”, “storage”,
1702 and “stored” as relates to data and computer systems. Moving out from the centre
1703 of the word cloud in figure 38 the features in the outside (the less frequent features
1704 in figure 38) are “provide”, “access”, “possession”, “copy”, “preserved”, and these
1705 relate to the actions that may relate to a person according to this law. Finally, the
1706 term person is also used in reference to law enforcement agents in relation to
1707 procedural powers e.g., as relates to the preservation of evidence. The term

1708 preserved is used in reference to the preservation of data as evidence by law
1709 enforcement.



1710

1711 *Figure 38: Kwic output for the term "person"*

1712 5.4.2 South Africa Cybercrime Act of 2020

1713 South Africa's cybercrime act of 2020 was analysed using frequency of terms and
1714 the following results were discovered as shown in the word cloud (maximum
1715 number of words was set at 50) in figure 39.



1716

1717 *Figure 39: Word cloud visualising terms frequency in South Africa's Cybercrime Act*

1718 The first three high frequency words were further analysed to see the context in
1719 which they were used. Figure 40 shows the frequency rankings of the features from
1720 the corpus.

	feature	frequency	rank
1	data	208	1
2	person	156	2
3	offence	128	3
4	contemplated	100	4
5	computer	95	5
6	terms	95	5
7	communications	90	7
8	must	86	8
9	service	85	9
10	police	82	10
11	act	81	11
12	electronic	81	11
13	part	77	13
14	direction	74	14
15	court	67	15
16	information	65	16
17	referred	65	16
18	official	61	18
19	application	55	19
20	warrant	55	19
21	search	48	21
22	evidence	46	22
23	republic	44	23
24	provider	44	23
25	designated	40	25
26	message	38	26
27	order	38	26
28	preservation	37	28
29	foreign	36	29
30	manner	36	29

Figure 40: Frequency rankings of words

The feature “data” had the highest frequency ranking in the corpus followed by “person” and “offence”, and these terms were analysed for context using the keyword in context function (kwic) function.

Keyword in Context Analysis for the Feature “Data”

On analysis of the kwic output in figure 41 (the first 10 results) it was discovered that the term “data” was used in relation to some action which is criminalised by the act. The following activities in relation to the term data have been criminalised by South Africa’s Cybercrime Act:

- The disclosure of data messages which are harmful
- Unlawful interception of data
- Unlawful interference with data or computer program
- Unlawful interference with a computer data storage medium or computer system
- Data messages which incite damage to property or violence

- 1737 • Data messages which threatens person with damage to property or violence
- 1738 • Disclosure of data messages of intimate image (real or simulated)

1739

criminalise the disclosure of	data	messages which are harmful
. Unlawful interception of	data	
. Unlawful interference with	data	or computer program
interference with a computer	data	storage medium or computer
9.	Data	message which incites damage
10.	Data	message which threatens persons
11. Disclosure of	data	message of intimate image
. Expedited preservation of	data	direction 15
18. Disclosure of	data	direction and search for
and using publicly available	data	or receiving data from

1740 *Figure 41: Kwic analysis using the term "data"*

1741 Other uses of the term “data” also appeared in contexts that address procedural
 1742 law such as directing law enforcement on the expedited preservation of data, and
 1743 the use of publicly available data. Examples are shown below:

- 1744 • Expedited preservation of data or receiving data from person who is in
 1745 possession of data.
 - 1746 ○ Section 45 (a) and (b) of South Africa’s Cybercrime Act here
 1747 recognises the geographical reach of cybercrimes by catering for the
 1748 receival, obtaining or use of “publicly and non-publicly available data
 1749 regardless of where it is located” by the police.

1750 Feature frequency visualisation of the terms that appear together with “data” is
 1751 shown in figure 42. It is clear from the figure that “computer” appeared the most
 1752 times with “data”. Other co-occurrence features include “message”, “direction”,
 1753 “storage” “traffic” just to mention a few. Therefore, when applying natural reading
 1754 heuristics, the use of the term “data” is mostly related to “computer data” either
 1755 stored or in transit as it can be seen appearing with “storage” and “traffic”. The other
 1756 use of the term is associated with the procedure for obtaining and securing data by
 1757 law enforcement.



1758

1759 *Figure 42: Visualisation of kwic output using the term "data"*

1760 *Keyword in Context Analysis for the Feature "Person"*



1761

1762 *Figure 43: Visualisation of kwic output using "person" as keyword*

1763 A kwic analysis of the feature "person" (figure 43) shows a number of words with
 1764 high frequency that appear close to the term "person". Appearance of the term
 1765 "person" in figure 43 is due to how the function works. Kwic cast a net around a
 1766 keyword based on the specified distance or window size, and it happens to be that
 1767 the term person was frequently appearing in close proximity to itself in the corpus.
 1768 Both the features' "data" and "unlawfully" had a high frequency of occurrence
 1769 around the term "person". Other high frequency terms include "intentionally",
 1770 "electronic", "contemplated" and "communications". A dive into the corpus using the
 1771 kwic function shows that the "term" person is used once too many times to refer to
 1772 a person as the perpetrator of an unlawful act. The feature "unlawfully" is also found

around the term “person” specifying the commission of an unlawful activity that is chargeable by the Cybercrime Act. “Intentionally” also appears around the feature “person”. Interestingly the phrase “unlawfully and intentionally” occurs 19 times out of the 22 appearances of the term “unlawful”, requiring that an unlawful action has to be intentional for it to constitute a crime under the Cybercrime Act.

Keyword in Context Analysis for the Feature “Offence”



Figure 44: Visualisation of the kwc output using "offence" as the keyword

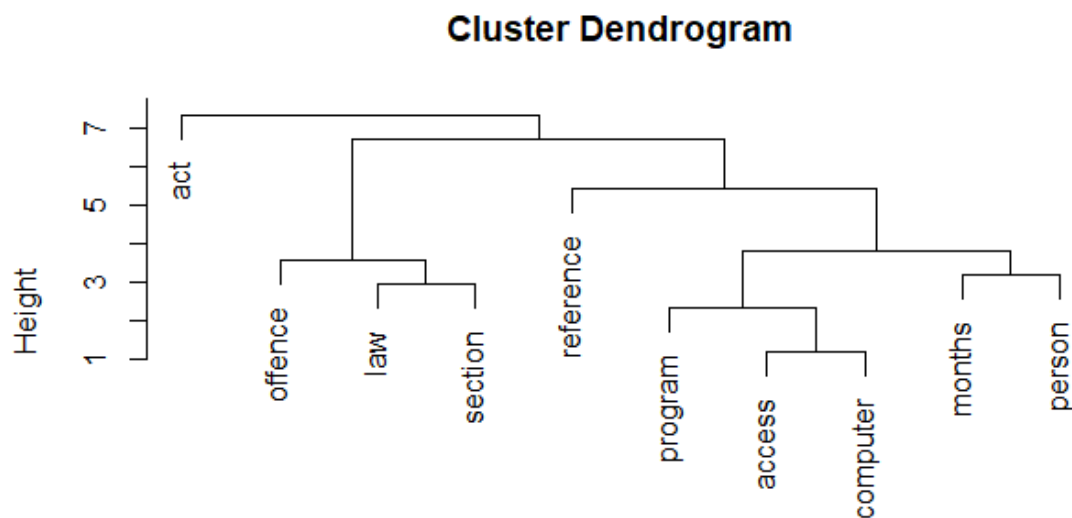
The frequency of words that appear around the feature “offence” is visualised in figure 44. “Guilty” comes out on top followed by the term “terms”. Other frequent terms include “similar”, “proven” and “referred”. An interesting observation using the kwc function is the frequent occurrence of the phrase “guilty of an offence”. The term “guilty”, it appears is closely related to the term “offence”, where the phrase “guilty of an offence” relates to a crime (or unlawful activity) committed by a person which is punishable under the Cybercrime Act. Another frequent term is “terms”, when analysed in context, this term is used to reference other sections of South Africa’s Cybercrime Act and sections in other acts and constitution of South Africa. “Terms” is also used to reference orders of a court or authority in a foreign state. The term “similar” also co-occurs with the term “data” 10 times as the phrase “similar data”. The phrases “similar data or devices” and “similar data and devices” are used to accommodate other methods and devices used for authentication, other than those specified by the Cybercrime Act.

1795 5.4.3 United Kingdom Computer Misuse Act of 1990



Figure 45(a): UK Computer Misuse Act Word Cloud Figure 45(b): UK Computer Misuse Act Word Cloud

1796 The UK's Computer Misuse Act of 1990 was also analysed alongside the Botswana
 1797 and South African cybercrime acts. The word cloud in figure 45(a) visualises the
 1798 frequency of features in the corpus. Both "Offence" and "reference" had the highest
 1799 frequency rankings followed by "act". "Person" also comes fourth on the frequency
 1800 rankings. The features "England", "Northern", "Ireland", and "Wales" appear
 1801 frequently on the corpus. This is because this act applies to these territories
 1802 (England, Northern Ireland, Ireland, and Wales), as well as in Scotland. However,
 1803 the act is applied differently in these territories. The term "reference" is used in
 1804 relation to interpretation of the Computer Misuse Act, other UK laws and is also
 1805 used to refer to territories that the act applies to and how it is applied there. The
 1806 term "offence" and its plural form "offences" appears throughout the text spelling
 1807 out the offences that are punishable under this act. Another high frequency terms
 1808 used in the act is "act" and is used in reference to an unauthorised act committed
 1809 by a person. Figure 45(b) is a visual representation without the words "England",
 1810 "Northern Ireland", "Wales" and "Scotland". However, figure 45(b) does not reveal
 1811 any patterns that are hidden in figure 45(a). A further analysis was carried out using
 1812 a dendrogram shown in figure 46.



d
hclust (*, "ward.D2")

Figure 46: Cluster analysis of the UK Computer Misuse Act

The dendrogram in figure 46 shows how the words in UK Computer Misuse Act are clustered. Since “act” appears frequently throughout the text, its chunk can be seen higher and separate from all the other chunks in figure 46. The term “act” is used to provide a reference to other acts as well as referring or providing interpretation for the use of certain terms and phrases. The clade that connects “act” to “offence”, “law”, and “section” associates “act” to these terms. “Act” as connected to “offence” depicts the use of the term to refer to some unauthorised or unlawful act. When connected to “law” and “section”, “act” is used in relation to the laws in the UK and external law. Applying traditional reading heuristics, the term “section” is mostly used in reference to UK law and the use of “law” was most consistent with external laws.

There are three clusters to the right of the “reference” cluster in figure. The first one contains the terms “program”; and the second one contains the terms “access” and “computer”; and the last one contains the terms “months” and “person”. The dendrogram shows that the terms “computer” and “access” are closer to each other with respect to “program”. All these terms (“computer”, “access”, “program”) are used in relation to an act that is used to provide unauthorised access to a computer

or program with intent. The features “months” and “person” are clustered together. “Months” is used in the text in reference to a sentence that a “person” can be given.

5.4.4 Comparison of the Acts

It was observed in this study that the UK cybercrime law did not follow a similar style of writing to Botswana and South Africa. For example, while the Botswana and South African Cybercrime Acts provide extensive definition of technology terms, the UK took a different approach entirely, with limited technology or computer jargon. The words “computer”, “access”, “program” were the most important technology terms in the UK law. In the Botswana law for example, the terms “computer”, and “computer systems” were used extensively when the term computer alone would have sufficed as in the UK law. Section 17(2) of the Computer Misuse Act of the UK provides interpretation for what it means to secure “access to any program or data held in a computer”, with subsequent interpretations given in the subsections that follow. The interpretation provided in section 17(2) made it possible for the authors of the law to use less technology jargon. This can be seen in figure 45(a) and 45(b) that technology terms were not the most frequent. It was observed that the UK Computer Misuse Act is focused on computer offences which are committed through, or their committal is facilitated by unauthorised access to computer material. While the Botswana and South African acts relied heavily on the use of technology related terms (shown by frequency of technology terms such as computer and data in figure 34 and figure 40), they also criminalise computer offences which are committed through, or their committal is facilitated by unauthorised access to computer material.

It has been demonstrated quantitatively that both the Botswana and South African Cybercrime Acts are similar in their use of words, the style of writing, as well as offences. For both acts, the terms “data” and “person” had high frequencies, as well as “computer” and “offence”. It was also observed through traditional reading heuristics that the acts in Botswana and South Africa are closely related. However, on analysing the document further it was also observed that the act in South Africa has some interesting chapters that are not available in Botswana. Chapter 8 – Reporting Obligations and Capacity Building – of the Cybercrime Act of South Africa, which obligates electronic communications service providers to report cyber

1864 offences under this act; and the responsible ministers to develop capacity to detect,
1865 prevent and investigate cybercrimes.

1866 It was also observed from the three countries that unauthorised access, itself being
1867 an offence, is also needed to commit further offences. As such this is the first
1868 offence that is criminalised by the acts from all the countries. While both the
1869 Botswana and South African acts criminalise cybercrimes, it is worth observing that
1870 the UK act used less electronic communications jargon. Perhaps the UK approach
1871 is the more futuristic way of writing cybercrime related laws as it is technology
1872 neutral. As can be seen from the UK Computer Misuse Act of 1990, being
1873 technology neutral makes the law clear, precise and to the point, hence taking away
1874 the headache of understanding technology jargon so that those who enforce the
1875 law can do so expeditiously.

6. CONCLUSIONS

1876 In this dissertation, the cyber threat landscape for Botswana was investigated. Data
1877 collected using a UK dataset, questionnaire, online news and posts was analysed
1878 using R. The results showed that the most common attacks are phishing, malware,
1879 ransomware, unauthorised access, and DoS. It was also discovered that the UK
1880 has an advance CIRT compared to Botswana which puts it at a good position to
1881 protect its constituents. Through the questionnaire and online content analysis, it
1882 was found out that the cyber-attacks in Botswana are similar to those in the UK.
1883 The online content and questionnaire results analysis showed that Botswana
1884 organisations rely mostly on cyber awareness and little capacity building. There are
1885 still organisations that do not implement strategies such as security in depth, BYOD,
1886 and password complexity. This places these organisations at risk of having their
1887 cyber systems compromised. A multi-stakeholder approach led by government can
1888 help protect vulnerable organisations by benefiting from knowledge shared by the
1889 wider community.

1890 This dissertation demonstrated through a dataset analysis the kind of insights that
1891 can be gained from a cybersecurity incidents register. Analysis of the UK's dataset
1892 revealed that phishing is the number one attack vector. Additionally, the NCSC
1893 found out that online scammers are taking advantage of people's fears over the

coronavirus. Other attacks identified by this study include ransomware and malware. APT attacks are also on the watch out for since the NCSC has picked up some global brute force activity under its radars. The increased crime and terrorism activity on the internet requires that Botswana moves to protect its sovereignty on the cyberspace considering the ongoing war in Mozambique and the pandemic.

Botswana has taken measures to improve its cybercrime legislation as one of its cybersecurity strategies. As such the cybercrime act of Botswana was also analysed alongside similar legislation from South Africa and the UK. The cybercrime act of Botswana was found to be comparable to that of South Africa and even that of the UK. However, there is concern over the overuse of technology related terms. Botswana therefore should continue working closely with regional bodies and states such as South Africa, Mauritius and Tanzania to improve its laws on cybercrime. However, without the right talents in law enforcement, government and private organisations, the best cyber legislation in the world cannot deter even a script kiddie. This is because cybersecurity professionals are to the law what the police are to traditional crimes. In addition to training cybersecurity professionals, government and organisations should invest in procuring the hardware and software necessary for cyber operations. Botswana should also learn from and increase collaboration with states that are already advanced in cybersecurity such as the UK and the US so that she can benefit from the advances made there.

6.1 Recommendations

This study recommends that the cybersecurity stakeholders in Botswana should prioritise training cybersecurity professionals and equipping the people with the skills to protect themselves online. National frameworks on cybersecurity education and culture should also be developed to guide such initiatives. The national CIRT team should also introduce an incentivisation mechanism for organisations to register cyber incidents. The dataset should thereafter be publicised as well as provide localised and timely cybersecurity incidents warnings, support, and advice.

1922 6.2 Future Work

1923 Future work will focus on developing frameworks for cybersecurity education and
1924 culture in Botswana. These areas are not yet developed and as such there is a gap
1925 here. Another area to consider for future work is investigating the cybersecurity of
1926 critical infrastructure in Botswana. From the literature conducted and web scraping
1927 results, cybersecurity discussions in the country have not reached the level of
1928 discussing critical infrastructure cybersecurity. However, authors such as Dawson
1929 [146], have observed that cyberattacks on critical infrastructure cause damages that
1930 are propagated beyond cyber assets, causing kinetic effect, damaging properties,
1931 industries and even lives. Other considerations for future work include the need for
1932 Artificial Intelligence (AI) and applications into the growing industries such as
1933 Industry 4.0. While AI is being used in manufacturing, it has come out clear that it
1934 introduces some cybersecurity risk and this fall in three areas which are people,
1935 process, and technology [184]. The aspect that researchers have not investigated
1936 is how to equip those responsible for AI systems to defend themselves from cyber-
1937 attacks [184]. Research also needs to investigate the AI development processes
1938 and security needs to be designed into all levels of the development lifecycle [184].
1939 The final consideration for risk is technology, and cyber supply chain vulnerabilities
1940 is an important area considering that some nations are already using AI for
1941 asymmetric warfare [184] [185]. While Botswana imports most of its electronics
1942 from countries such as South Africa, China, UK, US, Germany, India, Russia, etc
1943 [186], it is important for cybersecurity research to be carried out in this area,
1944 considering the threat posed by software that may be installed by third parties to re-
1945 route data for espionage activities [13,82].

References

- 1 B. Tutwane, "The State of Internet Freedom in Botswana 2019," The collaboration on ICT Policy in East and Southern Africa (CIPESA), 2020.
- 2 T. Nyoni and L. Muchingami, "Modeling and forecasting Botswana's Growth Domestic Product (GDP) per capita," in *Munich Personal RePEc Archive*, 2019.
- 3 D. NAGAR and M. PATERSON, "Peace and Security; SOUTH AFRICA IN SOUTHERN AFRICA," Centre for Conflict Resolution, 2013.
- 4 BBC, "Mozambique insurgency: Rwanda leads the fightback," BBC, 6 August 2021. [Online]. Available: <https://www.bbc.com/news/world-africa-58079510>. [Accessed 28 August 2021].
- 5 E. Morier-Genoud, "The jihadi insurgency in Mozambique: origins, nature and beginning," *Journal of Eastern African Studies*, vol. 14, no. 3, pp. 396-412, 2020.
- 6 National Cyber Security Centre , "Annual Review 2020, Making the UK the safest place to live and work online," 2020.
- 7 African Union Commission, Symantec, "Cyber Crime & Cyber Security Trends in Africa," 2016.
- 8 Serianu Limited, "Africa Cybersecurity Report - Botswana," Serianu Limited, Gaborone, 2018.

- 9 W. Crumpler and J. A. Lewis, "The cybersecurity workforce gap," in *Center for Strategic and International Studies (CSIS)*, Washington, DC, USA, 2019.
- 10 S. Cobb, "Mind this gap: criminal hacking and the global cybersecurity skills shortage, a critical analysis," in *Virus Bulletin Conference*, 2016.
- 11 J. Oltsik, C. Alexander and &. C. CISM, "The life and times of cybersecurity professionals," in *ESG and ISSA: Research Report*, 2017.
- 12 D. N. Burrell, "An exploration of the cybersecurity workforce shortage," in *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2020.
- 13 D. Adamsky, "The Israeli Odyssey toward its National Cyber Security Strategy," *The Washington Quarterly*, vol. 40, no. 2, pp. 113-127, 2017.
- 14 B. Earle and G. A. Madek, "Transatlantic Cyber Forum—Cooperating on Borderless Cyber Security Challenges.," in *Redesigning Organizations*, Springer, Cham, 2020.
- 15 A. Arewa, "Borderless crimes and digital forensic: Nigerian perspectives," in *Journal of Financial Crime*, 2018.
- 16 J. Kurebwa and J. R. Tanhara, "Cybercrime as a Threat to Zimbabwe's Peace and Security," in *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications*, IGI Global, 2020.

- 17 D. Bunga, "Legal response to cybercrime in global and national dimensions," *PADJADJARAN JURNAL ILMU HUKUM (JOURNAL OF LAW)*, vol. 6, no. 1, pp. 69-89, 2019.
- 18 A. Ncube, "Cybercrime as a threat to the Southern African Development Community (SADC) maintenance of peace and security: The case of Zimbabwe," Doctoral dissertation, University of Zimbabwe, 2018.
- 19 S. R. Khan, "Implication of cyber warfare on the financial sector. An exploratory study," *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 1, pp. 31-38, 2018.
- 20 S. Saad, S. Bazan and C. Varin, "Asymmetric Cyber-warfare between Israel and Hezbollah: the Web as a new strategic battlefield".
- 21 M. Courtney, "States of cyber-warfare," *Engineering & Technology*, vol. 12, no. 3, pp. 22-25, 2017.
- 22 R. Solgi, H. Khodaverdi and Z. Poustinchi, "Modern Cyber warfare between the Islamic Republic of Iran and the United States (2010-20)," in *International Studies Journal (ISJ)*, 2022.
- 23 C. M. Williams, R. Chaturvedi and K. Chakravarthy, "Cybersecurity risks in a pandemic," *Journal of medical Internet research*, vol. 22, no. 9, 2020.
- 24 R. A. Ramadan, B. W. Aboshosha, J. S. Alshudukhi, A. J. Alzahrani, A. El-Sayed and M. M. & Dessouky, "Cybersecurity and Countermeasures at the Time of Pandemic," *Journal of Advanced Transportation*, 2021.

- 25 B. Pranggono and A. Arabo, "COVID-19 pandemic cybersecurity issues," *Internet Technology Letters*, vol. 4, no. 2, 2021.
- 26 C. M. Williams, R. Chartuverdi and K. Charkravarthy, "Cybersecurity Risks in a Pandemic," in *Journal of Medical Internet Research*, 2020.
- 27 C. S. Teoh and A. K. Mahmood, "National Cyber Security Strategies," in *IEEE*, 2017.
- 28 R. Gallagher and P. Burkhardt, "'Death Kitty' Ransomware Linked to South African Port Attack South African Port Attack," Bloomberg, 29 July 2021. [Online]. Available: <https://www.bloomberg.com/news/articles/2021-07-29/-death-kitty-ransomware-linked-to-attack-on-south-african-ports>. [Accessed 31 August 2021].
- 29 J. Chigada and R. Madzinga, "Cyberattacks and threats during COVID-19: A systematic literature review," *South African Journal of Information Management*, vol. 23, no. 1, pp. 1-11, 2021.
- 30 T. M. Mbelli and B. Dwolatzky, "Cyber security, a threat to cyber banking in South Africa: an approach to network and application security," in *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)*, 2016.
- 31 World Bank, "The World Bank in Botswana," World Bank, 1 April 2021. [Online]. Available: <https://www.worldbank.org/en/country/botswana/overview#1>. [Accessed 28 August 2021].

- 32 International Telecommunications Union, "Global Cybersecurity Index 2020," 2021.
- 33 L. D. Shulman and A. Riikonen, "Strategy Development," Center for a New American Security, 2021.
- 34 S. Bradshaw, "Global Commission on Internet Governance," Center for International Governance Innovation, 2017.
- 35 Ministry of Transport and Communications, "National Cybersecurity Strategy," Government of Botswana, 2016.
- 36 Check Point Software Technologies LTD, "Cyber Security Report," 2020.
- 37 B. Van Niekerk, "An analysis of cyber-incidents in South Africa," *The African Journal of Information and Communication (AJIC)*, vol. 20, pp. 113-132, 2017.
- 38 J. Meservey, "Government Buildings in Africa Are a Likely Vector for Chinese Spying," *BACKGROUNDER*, *The Heritage Foundation*, no. 3476, pp. 1-23, 2020.
- 39 National Institute of Standards and Technology, "NIST Computer Security Resource Center," NIST, [Online]. Available: <https://csrc.nist.gov/glossary/term/cybersecurity>. [Accessed 14 June 2022].
- 40 D. Schatz, R. Bashroush and J. Wall, "Towards a More Representative Definition of Cyber Security," *Journal of Digital Forensics, Security and Law*, vol. 12, no. 2, pp. 53-74, 2017.

- 41 D. Craigen, N. Diakun-Thibault and R. Purse, "Defining cybersecurity," *Technology Innovation Management Review*, vol. 4, no. 10, 2014.
- 42 D. Galinec, D. Moznik and B. Guberina, "Cybersecurity and cyber defence: national level strategic approach," *Automatika*, vol. 58, no. 3, pp. 273-286, 2017.
- 43 M. Bay, "What is Cybersecurity?," *French Journal for Media Research*, vol. 6, 2016.
- 44 K. Guerra and D. J. Kim, "Cybersecurity: A Definition across Europe and North America," *AMCIS 2020 Proceedings*, vol. 16, 2020.
- 45 B. M., "WHAT IS CYBERSECURITY? In search of an encompassing definition for the post-Snowden era," *French Journal For Media Research*, vol. 6, 2016.
- 46 G. A. Crawford, "Information Warfare: New Roles for Information Systems in Military Operations," in *Air University*.
- 47 N. Shallcross, "Social Media and Information Operations in the 21st Century," *Journal of Information Warfare*, vol. 16, no. 1, pp. 1-12, 2017.
- 48 C. Abdyraeva, "Cyber Warfare:," in *OIIP - Austrian Institute for International Affairs*, 2020.
- 49 R. Syed, A. K. Ahmed and M. Yasin, "Cyber Warfare," in *Sustainable Development Policy Institute*, 2019.

- 50 O. Sultan, "Tackling Disinformation, Online Terrorism, and Cyber Risks into the 2020s," *The Cyber Defense Review* , vol. 4, no. 1, pp. 43-60, 2019.
- 51 J. Lusthaus, "Cybercrime as a Local Phenomenon," in *Australian Strategic Policy Institute*, 2020.
- 52 B. Wanner and G. Solange, "Conceptualizing Active Cyber Defence in Cyber Operations: Quo Vadis, Switzerland?," *St Antony's International Review*, vol. 15, no. 1, pp. 58-82, 2019.
- 53 E. Mandt, "Integrating Cyber-Intelligence Analysis and Active Cyber-Defence Operations," *Journal of Information Warfare*, vol. 16, no. 1, pp. 31-48, 2017.
- 54 M. R. DeVore and L. Sangho, "APT(ADVANCED PERSISTENT THREAT)S AND INFLUENCE: CYBER WEAPONS AND THE CHANGING CALCULUS OF CONFLICT," *The Journal of East Asian Affairs*, vol. 31, no. 1, pp. 39-64, 2017.
- 55 I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han, R. Hegarty, K. Rabie and F. J. Aparicio-Navarro, "Detection of advanced persistent threat using machine-learning correlation analysis," *Future Generation Computer Systems*, vol. 89, 2018.
- 56 CERT-EU, "Threat Landscape Report," CERT-EU, 2021.
- 57 National Institute of Standards and Technology, "Guide for Conducting Risk Assessments: Information Security," NIST Special Publication 800-30 - rev1, September 2012.

- 58 The IT Law Wiki, "Threat landscape," The IT Law Wiki, [Online]. Available: https://itlaw.fandom.com/wiki/Threat_landscape. [Accessed 18 June 2022].
- 59 Kaspersky, "Threat landscape," [Online]. Available: <https://encyclopedia.kaspersky.com/glossary/threat-landscape/#:~:text=The%20threat%20landscape%20is%20the,time%20period%2C%20and%20so%20forth..> [Accessed 18 June 2022].
- 60 CISO Portal, "Cybersecurity Landscape: What Is The Definition?," 18 September 2021. [Online]. Available: <https://www.ciso-portal.com/cybersecurity-landscape-what-is-the-definition/>. [Accessed 18 June 2022].
- 61 ENISA Threat Landscape 2021, "ENISA Threat Landscape 2021," ENISA, 2021.
- 62 FORTINET, "Global Threat Landscape Report," FORTINET, 2022.
- 63 F. Mercaldo, V. Nardone, A. Santone and C. A. Visaggio, "Ransomware steals your phone. formal methods rescue it," in *International Conference on Formal Techniques for Distributed Objects, Components, and Systems*, Springer, Cham., 2016.
- 64 D. Kansagra, M. Kumhar and D. Jha, "Ransomware: a threat to cyber security," *CS Journals*, vol. 7, no. 1, 2016.
- 65 Europol, "Malware Basics," 2015.

- 66 S. Murugiah and S. Karen, "Guide to Malware Incident Prevention and Handling for Desktops and Laptops," NIST, 2013.
- 67 J. Posetti and A. Matthews, "A short guide to the history of 'fake news' and disinformation," *International Center for Journalists*, vol. 7, 2018.
- 68 S. Eskandari, A. Leoutsarakos, T. Mursch and J. Clark, "A First Look at Browser-Based Cryptojacking," in *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2018.
- 69 S. S. Alhashim and R. M. M. H., "Cybersecurity Threats in Line with Awareness in Saudi Arabia," in *International Conference on Information Technology (ICIT)*, 2021 .
- 70 ENISA, "ENISA Threat Landscape for Supply Chain Attacks," European Union Agency for Cybersecurity, 2021.
- 71 W. Carter, "Forces shaping the cyber threat landscape for financial institutions," in *SWIFT Institute Research Paper Series*, 2017.
- 72 S. Varga, J. Brynielsson and U. Franke, "Cyber-threat perception and risk management in the Swedish financial sector," *Computers & Security*, vol. 105, 2021.
- 73 P. Black, I. Gondal and L. Robert, "A survey of similarities in banking malware behaviours," *Computers & Security*, vol. 77, pp. 756-772, 2018.
- 74 M. S. Pour, E. Bou-Harb, K. Varma, N. Neshenko, D. A. Pados and C. K.-K. Raymond, "Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale

- IoT probing campaigns,” *Digital Investigation*, Vols. 28, Supplement, pp. S40-S49, 2019.
- 75 M. R. Shad, “Cyber threat landscape and readiness challenge of Pakistan,” *Strategic Studies*, vol. 39, no. 1, pp. 1-19, 2019.
- 76 B. Buzan and L. Hansen, “The Evolution of International Security Studies,” Cambridge University Press, (Cambridge, New York, 2009.
- 77 L. Hansen and H. Nissenbaum, “Digital Disaster, Cybersecurity and the Copenhagen School,” *International Studies Quarterly*, pp. 1163-1168, 2009.
- 78 H. Pieterse, “The cyber threat landscape in South Africa: A 10-year review,” *The African Journal of Information and Communication*, vol. 28, pp. 1-21, 2021.
- 79 E. Sutherland, “Digital privacy in Africa: cybersecurity, data protection & surveillance,” 2018.
- 80 K. Jabbour and E. Devendorf, “Cyber Threat Characterization,” *The Cyber Defense Review*, vol. 2, no. 3, pp. 79-94, 2017.
- 81 R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon,” *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49-51, 2011.
- 82 S. R. Chabinsky, “Cybersecurity strategy: A primer for policy makers and those on the front line,” *J. Nat'l Sec. L. & Pol'y*, vol. 4, no. 27, 2010.

- 83 L. O. Nweke and S. D. Wolthusen, "A Review of Asset-Centric Threat Modelling Approaches," (*IJACSA International Journal of Advanced Computer Science and Applications*, vol. 11, no. 2, pp. 1-6, 2020.
- 84 N. Kshetri, "Cybercrime and Cybersecurity in Africa," *Journal of Global Information Technology Management*, vol. 22q , no. 2, pp. 77-81, 2019.
- 85 N. Gcaza, "A Strategy for A Cybersecurity Culture: A South African Perspective," *EJISDC*, vol. 80, no. 6, pp. 1-17, 2017.
- 86 M. Mckeown, *The strategy book*, UK: Pearson , 2019.
- 87 C. Woody and R. Creel, "Lessons Learned in Building and Implementing an Effective Cybersecurity Strategy," in *Acquisition Research Program*, 2021.
- 88 N. Shafqat and A. Masood, "Comparative Analysis of Various National Cyber Security Strategies," *Journal of Computer Science IJCSIS*, vol. 14, no. 1, pp. 129-136, 2016.
- 89 B. Horne, "On computer security incident response teams," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 13-15, 2014.
- 90 M. Bada, S. Creese, M. Goldsmith, C. Mitchell and E. Phillips, "Computer Security Incident Response Teams (CSIRTs): An Overview," in *The Global Cyber Security Capacity Centre*, 2014.
- 91 Forum of Incident Response and Security Teams, "FIRST Teams," [Online]. Available: <https://www.first.org/members/teams/>. [Accessed 22 June 2022].

- 92 R. Van der Kleij, G. Kleinhuis and H. Young, "Computer security incident response team effectiveness: A needs assessment," *Frontiers in psychology*, vol. 8, 2017.
- 93 K. L. TER, "Singapore's cybersecurity strategy," *Computer Law & Security Review*, vol. 34, no. 4, pp. 924-927, 2018.
- 94 F. A. Lopez, D. Ruete and G. Gatica, "Critical Infrastructure and Cybersecurity in Chile: Guidelines for Consensus," *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, pp. 41-55, 2021.
- 95 R. Sabillon, V. Cavaller and J. Cano, "National Cyber Security Strategies: Global Trends in Cyberspace," *International Journal of Computer Science and Software Engineering (IJCSSE)*, vol. 5, no. 5, pp. 67-81, 2016.
- 96 O. Osho and A. D. Onoja, "National cyber security policy and strategy of Nigeria: a qualitative analysis," *International Journal of Cyber Criminology*, vol. 9, no. 1, 2015.
- 97 D. Housen-Couriel, "National Cyber Security Organisation: Israel," NATO Cooperative Cyber Defence Centre of Excellence, 2017.
- [98] E. Matania and L. Yoffe, "Some Things the Giant Could Learn from the Small," *The Cyber Defense Review*, vol. 7, no. 1, pp. 101-110, 2022.
- 99 K. Pillay, "Guest Editor's Introduction: AJIC Focus Section on Cybersecurity," *The African Journal of Information and Communication (AJIC)*, vol. 20, pp. 79-82, 2017.

- 100 O. & E. O. Adeola, "ICT, infrastructure, and tourism development in Africa," *Tourism Economics*, vol. 26, no. 1, pp. 97-114, 2020.
- 101 O. O. David and W. Grobler, "Information and communication technology penetration level as an impetus for economic growth and development in Africa," *Economic research-Ekonomska istraživanja*, vol. 33, no. 1, pp. 1394-1418, 2020.
- 102 A. J. Njoh, "The relationship between modern information and communications technologies (ICTs) and development in Africa," *Utilities Policy*, vol. 50, pp. 83-90, 2018.
- 103 S. Asongu and A. Boateng, "Introduction to special issue: mobile technologies and inclusive development in Africa," *Journal of African Business*, vol. 19, no. 3, pp. 297-301, 2018.
- 104 S. N. Mogoane and S. Kabanda, "Challenges in Information and Cybersecurity program offering at Higher Education Institutions," in *ICICIS*, 2019.
- 105 A. van der Spuy and K. Oolun, "Promoting cybersecurity through stronger collaboration in Africa," in *SSRN 3275125*, 2018.
- 106 K. Adomako, N. Mohamed, A. A. Garba and M. Saint, "Assessing Cybersecurity Policy Effectiveness in Africa via a Cybersecurity Liability Index".
- 107 Bande and L. C., "Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-

- Specific Specificities,” *International Journal of Cyber Criminology*, vol. 12, no. 1, pp. 9-26, 2018.
- 108 U. J. Orji, “The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?,” *Masaryk University Journal of Law and Technology*, vol. 12, no. 2, pp. 91-129, 2018.
- 109 K. E. N. OHENE AGYAPONG, “REPORT OF THE COMMITTEE ON COMMUNICATION ON THE AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION (MALABO CONVENTION),” 2018.
- 110 African Union, “AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION,” 25 March 2022. [Online]. Available: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf. [Accessed 22 June 2022].
- 111 Africa CERT, “African Teams,” [Online]. Available: <https://www.africacert.org/african-csirts/>. [Accessed 22 June 2022].
- 112 D. Coleman, “Digital colonialism: The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws,” *Mich. J. Race & L.*, vol. 24, no. 417, 2018.
- 113 O. Analytica, “Digital authoritarianism in Africa is evolving,” Emerald Expert Briefings, 2022.

- 114 E. Calandro and N. Berglund, "Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC case," in *GIGAnet annual symposium*, Berlin, 2019.
- 115 R. S. Fonseca and J. A. van Wyk, "Cybersecurity in South Africa: Status, governance, and prospects," in *Routledge Companion to Global Cyber-Security Strategy*, Routledge, 2021.
- 116 African Union, "African Union Convention on Cyber Security and Personal Data Protection," African Union, 18 July 2021. [Online]. Available: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection/>. [Accessed 18 July 2021].
- 117 K. Renaud, "It's time for governments to help their citizens deal with cybersecurity," *The Conversation*, 26 August 2018.
- 118 Parliament of Botswana, "SECOND MEETING OF THE FIFTH SESSION OF THE TELEVENTH PARLIAMENT," Parliament of Botswana, Gaborone, 2021.
- 119 G. Kabanda, "A Cybersecurity Culture Framework and Its Impact on Zimbabwean Organisations," *Asian Journal of Management, Engineering & Computer Sciences (AJMECS)*, vol. 3, no. 4, pp. 17-34, 2018.
- 120 B. GROYSBERG, J. LEE, J. PRICE and J. Y.-J. CHENG, "The Leader's Guide to Corporate Culture," *Harvard Business Review*, pp. 1-15, January-February 2018.
- 121 Y. Turianskyi, "Africa and Europe: Cyber Governance Lessons," South African Institute of International Affairs, 2020.

- 122 Council of Europe, "Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY," [Online]. Available: <https://www.coe.int/en/web/cybercrime/parties-observers>. [Accessed 22 June 2022].
- 123 M. J. Z. Barros and H. Lazarek, "Comparative Study of Cybersecurity Policy Among South Africa and Mozambique".
- 124 International Telecommunications Union , " Global Cybersecurity Index & Cyberwellness Profiles," ITU, Switzerland, 2015.
- 125 E. Sutherland, "Governance of Cybersecurity – The Case of South Africa," *The African Journal of Information and Communication (AJIC)*, vol. 20, pp. 83-112, 2017.
- 126 T. Ncubukezi, L. Mwansa and F. Rocaries, "A review of the current cyber hygiene in small and medium-sized businesses," in *2020 15th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2020.
- 127 E. Sutherland, "The governance of data protection in South Africa," in *SSRN* 3922218, 2021.
- 128 C. Ferreira, "Harmonisation of Data Protection Regimes in the Southern African Development Community: Considering the influence of the SADC Model Law on Data Protection and the European Union on data protection laws in SADC," Master's thesis, Faculty of Law, University of Cape Town, 2021.

- 129 G. Greenleaf and B. Cottier, "International and regional commitments in African data privacy laws: A comparative analysis," *Computer Law & Security Review*, vol. 44, 2022.
- 130 S. S. Costigan, "Sovereign or Global Internet? Russia and China Press for Cybercrime Treaty," *Connections: The Quarterly Journal*, vol. 20, no. 2, pp. 9-13, 2021.
- 131 G. Glasze, A. Cattaruzza, F. Douzet, F. Dammann, M. G. Bertran, C. Bômout and C. Zanin, "Contested Spatialities of Digital Sovereignty," in *Geopolitics*, 2022.
- 132 M. Mahalelo, "Mobile Money Data Collection In Botswana," Botswana Communications Regulatory Authority, Gaborone, 2020.
- 133 U. Onyeukwu, "DEMOCRACY AND DEVELOPMENT IN BOTSWANA," *BW Academic Journal*, vol. 1, no. 1, 2022.
- 134 K. Diraditsile, "The nexus between youth empowerment programmes and youth unemployment reduction in Africa: Evidence from Botswana," in *Development Southern Africa*, 2021.
- 135 A. Speckhard, A. Shajkovci and Y. A. S., "Defeating ISIS on the Battle Ground as well as in the Online Battle Space: Considerations of the "New Normal" and Available Online Weapons in the Struggle Ahead," *Journal of Strategic Security*, vol. 9, no. 4, pp. 1-10, 2016.
- 136 S. Mahood and R. Halim, "Islamist narratives in ISIS recruitment propaganda," *The Journal of International Communication*, pp. 15-35, 2016.

- 137 E. Torlis, "Investigating the influence of ISIS radicalisation on the recruitment process: a critical analysis," *Journal of Policing, Intelligence and Counter Terrorism* , pp. 129-146, 2019.
- 138 I. Carrozza, "China's African Union Diplomacy: Challenges and Prospects for the Future," *LSE Global South Unit Policy Brief Series*, no. 2, pp. 1-8, 2018.
- 139 Reuters, "Exclusive-Suspected Chinese hackers stole camera footage from African Union - memo," Reuters, 16 December 2020. [Online]. Available: <https://www.reuters.com/article/us-ethiopia-african-union-cyber-exclusiv-idINKBN28Q1DB>. [Accessed 1 September 2021].
- 140 C. McGuffin and P. Mitchell, "On domains: Cyber and the practice of warfare," *International Journal* , vol. 69, no. 3, pp. 394-412, 2014.
- 141 Xinhua Net, "Safe city project in Botswana's two major cities operational," Xinhua Net, 20 February 2020. [Online]. Available: http://www.xinhuanet.com/english/2020-02/20/c_138799621.htm. [Accessed 1 August 2021].
- 142 M. D. Pelaelo, "FINTECH, PAYMENTS AND FINANCIAL INCLUSION WORKSHOP - GABORONE," Bank of Botswana, Gaborone, 2018.
- 143 Ministry of Finance and Development Planning, "National Development Plan 10," Government of Botswana, Gaborone, 2009.
- 144 Ministry of Finance, "National Development Plan 11," Government of Botswana, 2017.

- 145 Government of Botswana, "Movement Permits," 2020. [Online]. Available: <https://www.gov.bw>. [Accessed 30 July 2021].
- 146 M. DAWSON, R. BACIUS, L. B. GOUVEIA and A. VASSILAKOS, "Understanding the challenge of cybersecurity in critical infrastructure sectors," *Land Forces Academy Review*, vol. XXVI, no. 1, 2021.
- 147 Botswana Communications Regulatory Authority, "Draft Guidelines on Electronic Mail (E-mail) Security," [Online]. Available: <http://www.bocra.co.bw>. [Accessed 24 June 2021].
- 148 Botswana Communications Regulatory Authority, "Website Application Security Guidelines Draft," 29 March 2021. [Online]. Available: <http://www.bocra.co.bw>. [Accessed 24 June 2021].
- 149 A. Jimoh, "Social Engineering Attacks," Illinois Institute of Technology, 2022.
- 150 Metasploit, "Best Practices for Social Engineering Attacks," [Online]. Available: https://www.rapid7.com/globalassets/external/docs/download/Metasploit_Best_Practices_for_Social_Engineering_Attacks.pdf. [Accessed 6 June 2022].
- 151 Allot, "DDoS Attack Handbook - Service Providers," 2018. [Online]. Available: <https://allot.com/docs/ddos-attack-handbook.pdf>. [Accessed 6 June 2022].
- 152 Cybersecurity & Infrastructure Security Agency, "Understanding Denial-of-Service Attacks," 10 November 2019. [Online]. Available: <https://www.cisa.gov/uscrt/ncas/tips/ST04-015>. [Accessed 16 June 2022].

- 153 NSFOCUS, "Distributed Denial of Service (DDoS) Attacks: An Economic Perspective," [Online]. Available: https://nsfocusglobal.com/wp-content/uploads/2017/01/Distributed_Denial_of_Service_Attacks__An_Economic_Perspective__Whitepaper.pdf. [Accessed 6 June 2022].
- 154 D. Javeed and U. Mohammed Badamasi, "Man in the Middle Attacks: Analysis, Motivation and Prevention," in *International Journal of Computer Networks and Communications Security*, 2022.
- 155 E. Yllia and J. Fejzaj, "Man in the Middle: Attack and Protection," in *CEUR Workshop Proceedings*, 2021.
- 156 Solid State Systems LLC, "How to Prevent Man in The Middle Attacks," [Online]. Available: <http://solidsystemsllc.com/prevent-man-in-the-middle-attacks/>. [Accessed 17 June 2022].
- 157 Internet Society, "Man In The Middle Attacks," 2020. [Online]. Available: <https://www.internetsociety.org/wp-content/uploads/2020/03/Man-in-the-Middle-Fact-Sheet.pdf>. [Accessed 16 June 2022].
- 158 N. Patel, F. Mohammed and S. Soni, "SQL Injection Attacks: Techniques and Protection Mechanisms," in *International Journal on Computer Science and Engineering (IJCSE)*, 2011.
- 159 S. Reetz, "SQL Injection," Center for Internet Security, 2017.
- 160 A. E. Mohamed, "Complete Cross-site Scripting Walkthrough," [Online]. Available: <https://www.exploit-db.com/docs/english/18895-complete-cross-site-scripting-walkthrough.pdf>. [Accessed 17 June 2022].

- 161 H. Gao, "Cross-Site Scripting The most prevalent web application risk," [Online]. Available: <https://owasp.org/www-pdf-archive//OWASPTop10XSSLongIsland.pdf>. [Accessed 17 June 2022].
- 162 International Telecommunication Union / International Multilateral Partnership Against Cyber Threats, "ITU Document," [Online]. Available: www.itu.int. [Accessed 20 June 2021].
- 163 Botswana Cyber Incident Response Team, "BWCIRT: Home," Botswana Communications and Regulatory Authority, [Online]. Available: www.cirt.org.bw. [Accessed 23 June 2021].
- 164 Republic of South Africa, "Official Website of the South African National CSIRT," Department of Telecommunications & Postal Services, [Online]. Available: <https://www.cybersecurityhub.gov.za>. [Accessed 20 July 2021].
- 165 National Cyber Security Centre , "What we do," 31 July 2021. [Online]. Available: <https://www.ncsc.gov.uk/about-ncsc/what-we-do>. [Accessed 31 July 2021].
- 166 Council of Europe, "The state of cybercrime legislation in Africa – an overview," 2015.
- 167 A. L. Molokomme, "The Botswana Experience with Cybercrime Legislation and other Measures," in *Octopus Conference on Cooperation Against Cybercrime*, Strasbourg, 2012.
- 168 T. A. Chimuka and L. Mashumba- Paki, "UNDERSTANDING CYBER SCAMS: AN ASSESSMENT OF THE CHALLENGES OF LAW

ENFORCEMENT IN BOTSWANA,” *Journal of Sustainable Development in Africa*, vol. 18, no. 2, pp. 115-126, 2016.

- 169 Council of Europe, “Capacity Building on Cybercrime,” Council of Europe, Bucharest, 2020.
- 170 Information Commissioner's Office, “About the ICO,” Information Commissioner's Office, [Online]. Available: <https://ico.org.uk/about-the-ico/>. [Accessed 1 September 2021].
- 171 B. Kenneth, K. Watanabe, H. Wang, P. Nulty, A. Obeng, S. Müller and A. Matsuo, “quanteda: An R package for the quantitative analysis of textual data,” *Journal of Open Source Software*, vol. 30, no. 3, p. 774, 2018.
- 172 National Cyber Security Centre, “NCSC joins US partners to expose global brute force campaign by Russian Intelligence Services,” 1 July 2021. [Online]. Available: <https://www.ncsc.gov.uk/news/global-brute-force-campaign-advisory>. [Accessed 24 July 2021].
- 173 National Security Agency , “Cybersecurity Advisory, Russian GRU Conducting Global Brute Force,” 2021.
- 174 National Cyber Security Center, “UK and allies hold Chinese state responsible for pervasive pattern of hacking,” National Cyber Security Center, 19 July 2021. [Online]. Available: <https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking>. [Accessed 1 September 2021].
- 175 Online Editor, “Botswana is the cyber crime capital of Africa,” Sunday Standard, 28 August 2017. [Online]. Available:

- <https://sundaystandard.info/botswana-is-the-cyber-capital-of-Africa>.
[Accessed 20 July 2021].
- 176 Ministry of Transport and Communications , “Ministry of Transport and Communications-Botswana Facebook Page,” Ministry of Transport and Communications, 2021. [Online]. Available: <https://m.facebook.com/>.
[Accessed 20 July 2021].
- 177 L. Mnyobe, “Latest News,” Rhodes University, 24 June 2021. [Online]. Available:
<https://www.ru.ac.za/latestnews/cybersecurityexpertswarnofcyberattackstargetedatjournalists.html>. [Accessed 19 July 2021].
- 178 J. Churu, “Cyber security professionals: Botswana's headache,” BizTech Africa, 7 October 2019. [Online]. Available:
<https://www.biztech africa.com/article/cyber-security-professionals-botswana-headache/15072/>. [Accessed 19 July 2021].
- 179 ACS Services Botswana, “Ransomware Attacks,” ACS Services Botswana, [Online]. Available: <https://acs.co.bw/2021/02/11/ransomware-attacks/>.
[Accessed 20 July 2021].
- 180 Botswana Guardian, “Cyber security stakeholders introspect,” Botswana Guardian, January 2019. [Online]. Available:
www.botswanaguardian.co.bw/news/item/3945-cyber-security-stakeholders-introspect.html. [Accessed 20 July 2021].
- 181 The Patriot on Sunday, “Botswana: 'Botswana Has Huge Cyber Security Skills Gap,” All Africa, 11 September 2019. [Online]. Available:
<https://allafrica.com/stories/201909111000.html>. [Accessed 19 July 2021].

- 182 K. Goitsemodimo, "Cyber crime activities real in Botswana - DPP Director," Mmegi, 20 May 2016. [Online]. Available: <https://www.mmegi.bw/index.php?aid-60139&dir=2016/may/20>. [Accessed 19 July 2021].
- 183 K. Goitsemodimo, "BOCRA intensifies awareness on cyber-bullying," Mmegi, 4 November 2016. [Online]. Available: <https://www.mmegi.bw/index.php?aid=64387&dir=2016/november/04>. [Accessed 19 July 2021].
- 184 M. Dawson, "CYBERSECURITY IMPACTS FOR ARTIFICIAL INTELLIGENCE USE WITHIN INDUSTRY 4.0," *BULETIN ȘTIINȚIFIC*, vol. 1, no. 51, pp. 24-31, 2021.
- 185 D. N. Burrell, N. Bhargava, O. Bradley-Swanson, M. Harmon, J. Wright, D. Springs and M. Dawson, "SUPPLY CHAIN AND LOGISTICS MANAGEMENT AND AN OPEN DOOR POLICY CONCERNING CYBER SECURITY INTRODUCTION," *International Journal of Management and Sustainability*, vol. 9, no. 1, pp. 1-10, 2020.
- 186 STATISTICS BOTSWANA, "INTERNATIONAL MERCHANDISE TRADE STATISTICS," STATISTICS BOTSWANA, Gaborone, 2020.