DOI: 10.15587/2523-4153.2022.259764

A REASSESSMENT OF PUBLIC AWARENESS AND LEGISLATIVE FRAMEWORK ON CYBERSECURITY IN SOUTH AFRICA

Sogo Angel Olofinbiyi

How to cite:
Olofinbiyi, S. A. A reassessment of public awareness and legislative framework on cybersecurity in South Africa. ScienceRise: Juridical Science, 2 (20), 34–42. doi: http://doi.org/10.15587/2523-4153.2022.259764

Cybersecurity has become a growing concern globally, following this era of unparalleled resources, power relations and technological evolution. Technological vulnerabilities have led to massive data breaches in recent years and research has highlighted potential uses of artificial intelligence to engineer more powerful cyber-attacks thus revealing new hardware weaknesses. Cyber-attacks pose a threat to critical infrastructure thereby compelling countries to intensify their national security testing for cross-border partnerships. South Africa, however, is lagging in terms of readiness and capacity building against various forms of cyber-attack. Currently, the country has the world's third-highest number of cybercrime victims. By the same token, there is evidence that the South African Banking Risk Information Centre (SABRIC) loses over R2.2bn annually to cyber-attacks. In October 2019, two seemingly separate syndicates of hackers threatened to close the finance and local government sectors at a time when South Africa was struggling to recover from its previous economic recession. Taking insights from the existing literature, the study demonstrates that the level of awareness of cybersecurity among the South African populace is very poor, while the legislations put in place have done little to alleviate the trends and shield the general population from cyberwarfare. With growing legislation focussing on cybersecurity, the study contends that there is also the need for diverse professional and academic institutes to deliver hands-on educative services to the society through research-led activities to ensure South Africa is resilient to the growing threats. Given the borderless nature of cybercrime, South Africa should start intensifying efforts to incorporate the Joint Cybercrime Action Taskforce (J-CAT) alongside the local laws and necessitate the establishment of police-oriented learning centres, where citizens can be educated on the dangers of cybercrime and its devastated impacts on national development. With the drive towards digital economy and advanced global technologies, there is the need for further consolidation of South Africa's cybersecurity system with a view to ensuring the safety and security of national infrastructure, society, and global economic relations from malicious online crime spree. Until these are done, the storm is not yet over

Keywords: *cyberbullying, cybercrime, cybersecurity, cyberwarfare, data breach and protection, legislative framework, public awareness*

1. Introduction

Research concerns on data security and privacy in contemporary global communities have been a provoking debate over the last few years [1, 2]. As countries, organizations and individuals continue to stride towards digital transformation, the challenges they encounter in the course of this progression are multi-faceted. Real transformation involves exploring new ways of doing business, while increasing efficiency, costs reduction and higher investment returns. While navigating these new frontiers cautiously, we should remain aware that digital networking, data specifications and distributions, which enhance a more digitalized means of livelihood, have equally become more abstract, which may, in turn, increase our vulnerability to internet risks [3]. Increasingly, our infrastructures are also frequently becoming complex and relying on external dependencies. As digital evolution continues, some legacy issues will vanish, some will remain, and some new challenges will become more visible to reality. Hence, "the explosion of global connectivity, increase in the number of internet-connected devices, and the large number of unregulated social media channels, such that generate untrusted contents, have given cybercriminals many opportunities to hack organizations" [4].

Attacks on the cyberspace are constantly evolving. However, attack numbers do not necessarily increase, but when new threats are introduced, complexity changes. Hence, while companies strive to keep up with updates and eliminate controls on a weekly and daily basis, the boom in the number of vulnerabilities will also help increase complexity. Some of these bugs have been in processor chips and therefore can shake the whole computer world. A number of these vulnerabilities have been discovered

and have been present for years in older software. Take, for instance, the GNU Bash vulnerability, discovered in 2014, also known as "*Shellshock*," which affects many versions of Unix, Linux and Mac OSX, continues to be one of today's most targeted vulnerabilities [5, 6].

Mischievous cyber-attacks and negligent cybersecurity protocols have again resulted in massive personal information breaches in 2018. The highest was in India, where Aadhaar, the government's Identification system, allegedly suffered multiple breaches that could compromise the records of about 1.1 billion registered people. About 50 million 'Facebook users' and 150 million 'MyFitnessPal application users' have been affected by personal data breaches elsewhere. The U.S. government said in July 2018 that hackers had gained access to the U.S. utility companies' control rooms. The possible vulnerability of strategic technical infrastructure has become a growing national security concern. One of the growing national security concerns revolves around the vulnerability of critical technological infrastructure. In 2019 GPRS, the second most frequently cited risk interconnection was the combination of cyber-attacks with the critical breakdown of information infrastructure [7].

Drawing insights on previous empirical inquiries from Pre and amid COVID-19 pandemic, studies revealed that the Republic of South Africa has, hitherto, not had a breathing space from cyber threats; and recent cyberattacks on South Africa have shown how vulnerable the country is to cybercriminals and ransomware assaults - all of which have posed monumental threats to people, the economy and infrastructure at large. Consequently, the forgoing introduction sets the pace for this inquiry by addressing the following questions. What is the extent of people's knowledge on the danger, affiliated with cybersecurity in South Africa? How has South Africa been protecting its cyberspace from criminals that prowl the internet? How effective is South Africa's legislative framework on cybersecurity?

2. Literature Review

New vulnerabilities have emerged in 2019, and some have been added by updates, initially designed to address previous vulnerabilities. The finance sector has been the most attacked since the last six years, accounting for 17 per cent of the cyber-attacks globally. The Global Threat Intelligence Report indicates that "Increased web and service-specific attacks result in the finance sector becoming the most attacked sector in EMEA [Europe, Middle East, and Africa]; and this accounts for 30 per cent of all attacks, outpacing Business and Professional Services". Increasing vulnerabilities over the past two years is a concern for organizations, as many of these vulnerabilities occur in common frameworks, services and software, and library computer codes, employed to help daily operations. Likewise, illicit *coin mining* was one of the most common attacks in 2018 – often accounting for more detections than any other combined malware. But other risks presented a global challenge to companies as internet attacks intensified, partially due to the number of vulnerabilities, found in popular applications [8].

In the same vein, Symantec Internet Security Threat Report shows that incidents of form jacking – "the use of malicious JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of eCommerce sites". Trended upwards in 2018, the report also demonstrates that 4,818 different websites were hacked each month in 2018 with form jacking software. For example, data, sold on underground markets from a single credit card, yielded up to $45, while 10 credit cards, stolen from compromised websites, could yield up to $2.2 million per month to cybercriminals. Hence cybercriminals' appeal for form jacking is clear. Similarly, crypto jacking – "where cybercriminals surreptitiously run coin miners on victims' devices without their knowledge and use their central processing unit (CPU) power to mine cryptocurrencies" – was rampant in the last quarter of 2017 and dominated the cybersecurity landscape in 2018 [9].

Emphasizing on the worst hit of cybercrime spree in contemporary global societies, the advent of quantum computers has made countries, companies and individuals more susceptible to cyberattacks. Although quantum computing is a new concept, 71 % of global organisations view them as a major security threat. Protecting oneself against the dangers of quantum computing has become imperative. Quantum computers, still in the early stages of development, may be able to process and solve massive computational problems that exceed current supercomputer capabilities. Theoretically, on quantum computers, mathematical problems that require days of calculation could be solved instantaneously. To quantum computers, huge algorithms are digestible with opening doors in several spaces like encryption, seismology, decryption, pharmaceuticals, physics, decryption, to mention but a few. The possibility of quantum computers being able to crack RSA cryptography (which is widely used for secure data transmission), is one field that is extremely exciting for those in the quantum computing realm. Nevertheless, the ability of quantum computers to break encrypted data, if in the wrong hands, is precisely what makes it so dangerous. These developments pose great risks to the National Security of nation-states. Thus, defending the availability, integrity, and confidentiality of people's data and companies against constant threats by cybercriminals who try to steal, use and/or access these data has become a practical necessity [10, 11].

Recently, the trend in COVID-19 upsurge has called for an increase in remote working across the world. Consequently, the devasting effects have been felt across various sectors of the global economy in various significant ways. The spread of COVID-19 has sent a shockwave through the financial sectors of

the world and poses substantial cyber risks to strategic sectors of the economy. The discontinuity of work and lockdowns in several countries has led to increased online activity as many people were compelled to resort to working from home. As a corollary, the financial sector of most global organizations has felt a huge blow since the virus has staged the global sphere. There has been evidence in the extant literature that the global systems have recurrently been attacked and millions of United States dollars have gone down the drain through persistent attacks by cybercriminals [12]. It was also established, that stock markets around the world and every segment of the global economy have been severely affected, while phishing, malware and ransomware (techniques of social engineering, adopted by cybercriminals) have dealt a great blow to financial service industries across the world [13]. Given the various incidents of cyberattacks and threats around the world, the South African banks have taken pre-emptive measures to embark on a frequent drive to educate their clientele concerning fake emails and phishing [14].

In a study, conducted by the Price Waterhouse Coopers, South Africa (PWC), cyberattacks and threats on financial institutions between February and April, 2020 were seen to increase by more than 238 % globally, at a time when the global economy was working tirelessly to fight the COVID-19 infections [15]. It was suggested, that the COVID-19 insurgency pioneered a perfect climate for cybercriminals to exploit their targets. Congruently, ransomware attacks experienced a nine-fold upsurge during the period, with phishing emails as the primary source of attacks, launched on the suitable target. From this standpoint, Chigada and Madzinga contend that cyberattacks and threats are remarkably growing in South Africa, because cybercriminals are intelligent individuals who have gained better knowledge of the legislative policies and procedures of financial institutions. The foregoing scholars unfold that, there was an upsurge in money laundering and terrorist financing, orchestrated through increased misuse of online financial services, as well as virtual assets, harnessed to move and conceal illicit funds; and this perhaps shows some level of cybercrime, perpetrated by government officials [16]

3. The Aim and Objectives of the Study

The aim of the study was to reassess public awareness and legislative framework on cybersecurity in South Africa. To achieve the aim of the study, the following specific objectives were examined.

1. To determine the extent of people's knowledge on the dangers, affiliated with cybersecurity in South Africa.

2. To examine what government has done to protect the South Africa's cyberspace from malicious online crimes.

3. To evaluate the effectiveness of South Africa's Legislative framework on cyber security.

4. Materials and Methods

A meta-analytical methodological approach, involving a systematic review of empirical data sources and relevant legal case notes on cybersecurity, was adopted to interrogate the phenomenon and discuss the findings within a socio-legal framework. Secondary data sources obtained from media reports, academic journals, as well as findings, presented by the Cybersecurity and Infrastructure Security Agency (CISA), South African Government Cybercrime Act 19 of 2020, the South African National Cybersecurity Policy Framework (SANCPF) et cetera. Through a conceptual and critical evaluation of the following scholarly materials, the study was able to offer some interesting insight on how the problems could be tackled through the development of more appropriate culturally acceptable socio-legal strategies. Overall, the design irrefutably provides a well-grounded research baseline for future empirical studies on cybersecurity and related crimes.

Analytical Definition of Key Concepts

To circumvent the vagueness of matters, arising from the subject of this discourse, this section provides a definition and clarification of key concepts, which predominate the cyber world. Makeri argues that since computer crime includes all types of crime, the knowledge, particularity, or use of computer technology must be highlighted in any definition. Hence, he notes that 'cyber-space' refers to the internet boundless space and interdependent network of components of information technology that underpin many of today's existing communications technologies.

Cybersecurity is the method or approach, used to prevent damage, attack, or unauthorized access to the integrity and reliability of programs, data, and networks. It involves protecting information and systems from critical cyber risks, such as cyber spying, cyber warfare, and cyber terrorism. Cybersecurity is the array of technology, information and telecommunications systems that can be used to secure the cyber environment and resources of nations, companies, and users. Cybersecurity aims to ensure that the security properties of the organization and user's assets are attained and maintained against the relevant security risks in the cyber environment. Cybersecurity refers to the collection of technologies, procedures, and applications, aimed at protecting networks, devices, programs, and information from attack, injury, or unauthorized access. Cyber-security is the set of rules for cyber-space protection. At this juncture, it is crucial

to know that as we become more dependent on cyberspace, we equally face new risks, associated with cybercrime, on a daily basis. [17]

Cyber insecurity, as noted in one of the analytical writings of Olofinbiyi on cyber threats, entails an unauthorized invasion of cyber privacy, trespassing, thefts, as well as denial of services attacks and malfunction, caused by any human factor in any system that is dependent on the internet using computer devices; and such trespassing may include hacking into a nation's or an individual's critical infrastructure [18]

Cybercrime indisputably connotes a sort of crime that embraces internet or computer facilities as a medium to commit crime. Precipitating issues around this type of crime have become high-profile, particularly those surrounding hacking, phishing, cyber terrorism, malware, identity theft, child pornography, spam et cetera. Cybercrime refers to the series of organized crime that attacks cyberspace as well as cybersecurity. Among other things, sophisticated cyber criminals present risks to national security and economy of nation-states. This act also ranges from the illegal downloading of music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offences, such as the creation and distribution of viruses to other computers or posting on the Internet of confidential business information. One of the most common types of cybercrime is identity theft, where hackers use the Internet to steal other users' personal information for dubious activities. Essentially, cybercrime denotes "A criminal activity, involving an information technology infrastructure, including illegal or unauthorized access, illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud"[19]. Common forms of cybercrime include:

Identity theft: This a crime situation where offenders obtain information about an individual to convince an organization, such as bank or any customer service unit that they are the victim. The offenders do this by impersonating the identity of the victim.

Phishing: This is a crime situation where criminals try to cajole unsuspecting people into clicking on a malicious e-mail attachment or URL to steal the login details that they can then use to obtain unauthorized access to the financial accounts of the victims.

Ransomware: This is a crime situation where your computer has a hacker's encrypted files. Paying the hijacker in cryptocurrency, like Bitcoin, is the only way to get the files back. On the other hand, it also refers to a kind of malicious software, designed to block access to a computer system until a ransom or a sum of money is paid.

5. Result

The State of Cybersecurity in South Africa

According to the Global Risks Report, the world faces an increasing number of complex and interconnected challenges – from persistent economic inequality and sluggish global growth to geopolitical tensions, climate change, and the Fourth Industrial Revolution's accelerating speed. Each of these is daunting challenges, besetting the world simultaneously. The Global Risks Report of the World Economic Forum (WEF) in the year 2019 highlighted "technological instability" as a threat – with "massive data/money fraud and theft" – being ranked number four global risk (by likelihood of over a 10-year horizon) and cyberattacks (disruption of operations and infrastructure), following closely at number five global risk. Cyber-risks were placed in the high impact alongside environmental risks in the Global Threats Landscape quadrant of the annual report [20]. In South Africa, experts warn that the threat has been so severe – with companies, of all sizes across sectors, at risk of being compromised by increasingly experienced cybercriminals.

South Africa, currently, has the world's third-highest number of cybercrime victims. According to the South African Banking Risk Information Centre (SABRIC) Annual Crime STATS, the country loses an estimated R2.2bn per year to cyber-attacks. The report adds that combined gross card fraud losses on issued South African cards increased by 18 % from 2017 to 2018, totalling R873 394 351, with credit card fraud, rising by 18.4 % and debit card fraud, rising by 17.5 %. Card Not Present (CNP) credit card fraud in South Africa remained the leading contributor to the country's gross fraud losses, accounting for 79.5 % of all losses. These losses are more than financial terms as victims of cybercrime often spent an average of two working days, addressing the aftermath of the attack. Furthermore, Missing and/or Stolen debit card fraud in 2018 rose to 42.5 per cent of all debit card frauds; and bank customers tend to be victims of ATM fraud when trading. Criminals approach victims on the pretext that they are helpful and even pose as a bank official in many instances. They then steal the card of their victim and shoulder surf to get the PIN.

Moreover, the SABRIC report states that R262 826 888 in gross losses amounted to 23 466 incidents across mobile banking, online banking and banking apps. It is worrisome that incidents across these channels have risen by 75.3 %. Mobile banking incidents saw a 100 per cent increase, with R28 941 040 gross losses, while online banking incidents showed a 37.5 per cent increase with

R129 002 523 gross losses. Incidents with the banking app increased by 55.4 per cent, with R104 883 325 gross losses for the same period. Evidently, criminals are highly skilled in psychological intelligence and will use social engineering techniques to manipulate any human weakness to extract confidential information, such as a PIN or password, to steal money. As a result of this, South Africans must beware of phishing emails asking you to click on a link when it comes to online banking. The link will guide you to a "spoofed" website for contact details or other confidential financial information to be collected, checked, or updated [21].

These numbers could only be the proverbial tip of the iceberg. Many local experts maintain that most cyber-attacks on small, medium, and micro enterprises (SMMEs) remain unreported. There is, therefore, no reliable way to measure how much damage is being done, whether financial, reputational, or otherwise. In other countries, there are dedicated hotlines and other initiatives to keep track of hits, but this is absent in South Africa, and reports to the police are on the low side. Companies and business leaders are afraid that they will not remain anonymous if they report cybercrimes to authorities. As a result, the reputational risk outweighs everything, because if customers were to find out about an infringement, the business would be facing ruin.

At SMME level, Hubbard observes that the threats come primarily in the form of phishing, whereby unsuspecting individuals are tricked by criminals into clicking on an email attachment to steal their login details or a malicious URL – which they can then use to obtain illegal access to the victim's financial accounts or internal corporate networks. Progressively, the phishing attacks of today involve some form of social engineering, whereby hackers gather personal information from social media accounts, such as LinkedIn and Facebook, to give the attack some 'credibility'. These hackers will only get details, such as your location, the names of your friends, your company, and your birthday, by scanning your social media accounts.

Furthermore, local SMMEs faced a spike in what was termed 'sextortion' attacks and scams in 2018 – where hackers pretend to have sexual images, history of your surfing, or videos and threaten to expose victims on the internet. Individuals were tricked into paying heavy fines and disclosing personal financial information to avoid potential embarrassment. In October 2018, one of the biggest data breaches occurred in the country, during which more than 30million personal information from South Africans was exposed online. It was predicted, that the potential for so-called 'cyber storm' events would continue to grow in 2019, where hackers were disrupting large numbers of companies by targeting public infrastructure dependencies.

Some of the prevalent cybercrimes in South Africa include hacking, ransomware, phishing scams, identity theft, online child sexual abuse (child pornography), electronic fund transfer fraud, social media cloning, cyber-impersonation, and cyber-bullying. It is crucial to know, that cyber-bullying can escalate as fast as face-to-face bullying. For instance, someone who spends time 'stalking' another person through the victim's different internet profiles may ultimately decide to stalk the person directly, and somebody who attempts to threaten or extort you online may decide to publish harmful images against you [22]. Other forms of cyber-bullying include:

– Character assassination through malicious, slanderous, defamatory "anonymous" emails.

– Harassment via Facebook, MySpace, Twitter, LinkedIn, and other social networking sites.

– Libellous online content through the use of websites to defame your character.

– Online stalking, harassment, blackmailing, or online disturbance through one's status updates.

Besides, artificial intelligence (AI) or machine learning is becoming more sophisticated and ubiquitous, with increasing potential to worsen existing threats or create new ones, especially as the Internet of Things connects billions of devices. The role of AI in the rise of "media echo chambers and fake news" are among its most common and disruptive impacts. Consistently, fake news outperformed those containing factual information. This is because of the interplay between technology and emotions, which is becoming an ever more disruptive force. The rise of mysterious new think-tanks and foundations with even more mysterious funders and organized trolling campaigns against journalists and other public figures (often spurred on by politicians) is increasingly characterized by social media and public dialogue in South Africa [23]. The parallel to all these advances in technology and the efforts by cybercriminals to exploit people involves the use of technology to protect users and organizations. This can be achieved through machine learning and artificial intelligence, which maximize the vast quantity of information, produced by user-system interactions and information processing.

Data protection and privacy continue to be the underlying issues that connect through every discourse on cybersecurity. Just as technology continues to evolve, the way it is used also changes and evolves, which in turn, leads to cybercriminals looking for new ways to take advantage of it. The deepening integration of digital technologies into every aspect of life has caused new instabilities as can be seen in the wave of attacks on individuals, governments, and financial institutions in South Africa.

Review of Cyber Attacks on Banks, Municipalities and Public Corporations

In October 2019, two seemingly separate groups of hackers threatened to close down the finance sector and local government at a time when South Africans should be paying municipal bills and gaining

access to their bank accounts. The South African Banking Risk Information Centre (SABRIC) confirmed a wave of ransom-driven Distributed Denial of Service (DDoS) attacks, directed at different public services across multiple banks. A DDoS attack is a criminal attempt to crash a website by overwhelming it with a flood of fake traffic or digital demands [24]. The attacks started with a ransom note, sent to all unattended and staff email addresses by phone, all of which were available to the public. The banking sector was asked to pay a ransom of two Bitcoins (R219000) or the DDoS attack would be launched [25]. Threat intelligence by SABRIC revealed that this is a "multi-jurisdictional attack," which meant that several countries were targeted in the onslaught. The infamous hacking group 'Fancy Bear', linked to the Russian government, claimed to be behind the attack [26]. Correspondingly, the City of Johannesburg was equally hit in this wave of attacks. Locals could not use their websites to log queries or pay for their e-bills. The hackers reportedly demanded the payment of 4.0 bitcoins (R437, 000) and failure of any kind would release sensitive information about residents of Johannesburg. Employees received the ransom note, which reads, "All your servers and data have been hacked…. we have dozens of back doors inside your city…. we have control of everything in your city….we also compromised all passwords and sensitive data, such as finance and personal population information." [27].

In February 2019, South Africa's state-owned power company, Eskom, left a database, containing customer names, addresses, CVV numbers, and partial credit card numbers exposed online. It is still obscure how Eskom's 5.7 million customers were affected in the attack [28]. The company allegedly ignored cybersecurity researcher -Devin Stokes' alert on the issue. This incident unveiled that banks and companies need to have a system in place where suspected breaches to their database can be reported by the public. These vulnerability reports can be sent to a dedicated email where a prompt response can be dispatched. With these developments on cyber-attacks in South Africa, it is imperative, that the level of awareness and preparedness of the population will be more enhanced.

Synopsis of Review Results

Overall, the results show that a vast number of South Africans do not fully understand the concept of cybercrime and its fast-growing trends; and thus, those who have experienced an event of cybercrime, do not have the technological know-how on what to do and who to report the incident to. Studies unveiled that South African men in particular are at a higher risk of experiencing cybercrime because of their more active engagement in business ventures that entail high technologies. This suggests that men probably have a better working understanding of the concepts and prevalence of cybercrime than women; however, except for online romance scam. It was further observed, that women believe that their online activities do not put them at risks of encountering an incident of cybercrime [29, 30]. Password protection has been highlighted as the most common and important method of protection against acts of cybercrime, while a small proportion of research inquiries indicates that fewer members of the community report the criminal act to the police.

In general, it was uncovered, that the South African laws offer no protection against cybercrime and are unsure of whether cybercrime can be controlled by the South African laws. Corroborating this sentiment, the Electronic Crime Unit of the South African Police Service (SAPS) under the HAWKS asserts, "Technological developments are trending globally, increasing the threat of cybercrime. At ground level, we are still faced with a challenge of responding to cybercrime. When a complainant reports a crime on hacking or any other related computer crime, we are still left wanting" [31]. Hence, most legal and regulatory acts must be adopted to fill this vacuum; there is also the need to develop, train and equip people to be able to respond to all forms of cybercrime-related complaints. Likewise, members of the civil society need to stay abreast of trends in the scourge of cybercrime.

6. Discussion

Legislative Framework on Cybersecurity in South Africa

The National Cybersecurity Policy framework (NCPF) in South Africa is predicated on the need to have effective law enforcement/criminal justice responses. The country recognises the need for an approach that balances prevention and/or enforcement through the establishment of specialised investigative capacities, intelligence-led investigation, and prosecution of criminals. Across the world, there are various legislations against cybercrimes like the United Nations Convention against Transnational Organised Crime; Council of Europe's Cybercrime Convention (Budapest); African Union Convention on Cyber Security/Data Protection. Other legal instruments include [32]:

– United Nations Convention Against Transnational Organised Crime.

– United Nations General Assembly Discussion Guide, focusing extensively on the combating of transnational organised crime, specifically in relation to the phenomenon of cybercrime.

– Economic Community of West African States (ECOWAS) Directive on fighting Cybercrime.

– Common Market for Eastern and Southern Africa (COMESA) Cyber Security Model Bill.

– East African Community (EAC) Legal Framework for Cyber laws

– Southern African Development Community (SADC) Law on Computer Crime and Cybercrime.

In South Africa, the Electronic Communications and Transactions (ECT) Act 25 of 2002 objectives aim to: encourage the use of e-government services; prevent abuse of information systems; promote universal access to electronic communications/transactions; provide for the development of a national e-strategy; provide for facilitation/regulation of electronic communications/transactions, among others. Section 86 of the Act criminalizes unauthorized access to, interception of or interference of data, while section 87 contains legislative versions of forgery/fraud/extortion violations in common law, specifically tailored to the electronic media. While Sec 88 criminalizes any attempt, aiding and abetting of offences, referred to in Sec 86/87.

In addition, the Cybercrimes Act 19 of 2020 intends to: create offences, which have a bearing on cybercrime; criminalise the disclosure of data messages, which are harmful; provide for interim protection orders; further regulate jurisdiction in respect of cybercrimes; further regulate the powers to investigate cybercrimes; further regulate aspects, relating to mutual assistance in respect of the investigation of cybercrimes; provide for the establishment of a designated Point of Contact; further provide for the proof of certain facts by affidavit; impose obligations to report cybercrimes; provide for capacity building; provide that the Executive may enter into agreements with foreign States to promote measures, aimed at the detection, prevention, mitigation and investigation of cybercrimes; delete and amend provisions of certain laws; and provide for matters, connected therewith [33] .

More specifically, In South Africa, the Cybercrimes and Cybersecurity Act (Act) was signed into law by South African President Cyril Ramaphosa in early June 2021, bringing the country's cybersecurity legislation in line with global standards. The Act compels electronic communications service providers and financial institutions to act when they become aware that their computer systems have been involved in a cybersecurity breach, as defined by the Act. They must, according to the Act, report such offenses to the South African Police Service within 72 hours of becoming aware of the offense, and preserve any information, which may be of assistance in the investigation. Non-compliance with this provision is a criminal offense and massive fines can be imposed [34].

The Act further criminalizes harmful data messages, such as those that invite or threaten violence or damage to property, as well as those that contain intimate images. Data, however, is broadly defined in the Act as "electronic representations of information in any form." The Act also criminalizes cyber fraud, extortion, forgery and the theft of incorporeal property. Also listed as an offense is the unlawful accessing of a computer system, data storage medium or personal data. Those found guilty of a cybersecurity offense face hefty fines and lengthy prison sentences of up to 15 years.

The legislative policy stretched further that, In South Africa, data security is also governed by the Protection of Personal Information Act (POPIA). Consequently, on the 1st of July, 2021, the substantive implementation of key provisions of POPIA became enforceable. This legislation, among other things, promotes the protection of personal information, processed by public and private bodies, outlines the rights of data subjects, regulates the cross-border flow of personal information, introduces mandatory obligations to report and notify data breach incidents, and imposes statutory penalties for violations of the law [35].

One of the conditions for lawful processing in terms of POPIA is the use of security safeguards, which prescribe that the integrity and confidentiality of personal information must be secured by a person in control of that information. This is prescribed by POPIA in order to prevent loss, damage or unauthorized access to, or destruction of personal information. As we have seen, all these legislations have not produced the desired results as regards, curtailing the increased trends of cybercrime in South Africa. At this juncture, and given the borderless nature of cybercrime, it should become paramount to understand, that the international legislation should be considered and strengthened alongside the local laws to submerge the cyberwarfare in the nation. It is also germane to know, that the implementation of legal policies and laws cannot absolutely address this enigma; but consultation with technologically advanced security experts will represent a more promising step forward to fortify the existing legislative framework on cyber security. More importantly, considering the current humans' rapid transition to digitally-focused business models, the implementation of international legal protections and guidance should become an urgent priority, not only for South Africa but also all nations on the African continent.

Limitation in Terms of the Research Method that was Employed. The study is limited in terms of raw empirical data, which could have strengthened the findings of the study. It is believed, that such data could have supplemented the findings of the review by incorporating more valid and reliable data through the use of survey and in-depth interviews. Consequent upon the nature of the research questions and method, chosen for the study, questionnaires were not administered, and interviews were not conducted; and thus, the study could not involve the testing of any hypotheses and thematic analysis of materials.

Defining the Generalizability of the Findings. Due to the nature of the method, employed for the study, defining the generalizability of the findings was also enlisted as a limitation to this study. Actually, the fact that the study was relatively limited in scope in terms of the participants, locations and techniques, employed for data collection, makes this impossible to define. The study had access to published and unpublished studies, journal and newspaper reports, print media, electronic media and institutional

data as the main sources of information relevant to the study. Irrespective of this array of limitations, this research can still be used as a baseline informative research for much broader future research inquiries on cybersecurity or related studies.

7. Conclusion

Based on the meta-analytical evaluation of literature, the following concluding remarks were drawn:

1. There is evidence that South Africa has not done enough to protect its cyberspace and citizens from malicious internet criminals, despite the existing legislations and policies on cybersecurity. For the past two decades, criminal minds have exploited the cyberspace to perpetrate all sorts of crime. Looking at the magnitude of cyber-attacks and data breaches that occurred in South Africa in 2018 – a very ugly evidence-based reality that portends that the global cyber threat has come to stay and terrorize our existentiality. The implication is that each time we log in to our device, use our smartphone, open an e-mail, we are exposed to the threats of cybercrime almost every time we connect with technology. Thus, implementing cybercrime legislation is a pressing issue, as South Africa has one of the world's highest numbers of victims of cybercrime.

2. The study demonstrates that the level of awareness of the dangers, associated with cybersecurity, among the South African populace is very poor, while the legislations, put in place, have done little to shield the general population from cyberwarfare. Consequently, several unsuspecting individuals and organizations have fallen prey to the scourge and dangers of cyber scams, which seemed to spike quite fast in recent years. From this standpoint, there is need for the establishment of diverse professional and academic institutes to deliver hands-on educative services to the society through research-led activities to ensure South Africa is resilient to the growing threats. Even in the light of the standing legislative framework and government's incessant efforts to curtail the horrible trends within the general population, cybercrime begins to grow in strength and magnitude to the detriment of national economy and sustainable development.

3. Nevertheless, given the borderless nature of cybercrime, the storm is not yet over until South Africa begins to intensify indefatigable efforts towards incorporating the Joint Cybercrime Action Taskforce (J-CAT) alongside the local laws and necessitating the establishment of police-oriented learning centres, where citizens can be educated on the preeminent dangers of cybercrime and its devastated impacts on national development. With the drive towards digital economy and advanced global technologies, there is the need for further consolidation of South Africa's cybersecurity system with a view to ensuring the safety and security of national infrastructure, society, and global economic relations from malicious online crime spree.

Conflicts of interest

The authors declare that they have no conflicts of interest.

References

1. The Global Risk Report (2019). Insight Report. World Economic Forum in partnership with Marsh & McLennan Companies and Zurich Insurance Group. Available at: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf Last accessed: 03.10.2020
2. Oforji, J. C., Udensi, E. J., Ibegbu, K. C. (2017). Cybersecurity Challenges in Nigeria: The Way Forward. Sos Poly Journal of Science & Agriculture, 2.
3. Makeri, Y.A., (2017). Cyber Security Issues in Nigeria and Challenges. International Journal of Advanced Resaerch in Computer Science and Software Engineering, 7 (4), 315–321. doi: https://doi.org/10.23956/ijarcsse/v6i12/01204
4. Nakata, K. (2019). Global threat intelligence report. NTT Security. Available at: https://www.nttsecurity.com/docs/ librariesprovider3/ resources/2019gtir/2019_gtir_report_2019_uea_v2.pdf Last accessed: 8 November 2021).
5. Brende, B. (2019). Preface. The Global Risk Report. World Economic Forum in partnership with Marsh & McLennan Companies and Zurich Insurance Group, 5. Available at http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf Last accessed: 01.062022
6. Lucas A. (2017). 'How prepared is Nigeria for cyber-attacks?' The Nation. Available at: https://thenationonlineng.net/prepared-nigeria-cyber-attacks/
7. Privacy and Intrusion in the Global Village: Eset Cybersecurity Experts (2019). Cybersecurity Trends Report. Available at: https://cdn1.esetstatic.com/ESET/US/resources/white-papers/Cybersecurity_Trends_2019_Final.pdf Last accessed: 03.04.2021
8. The Global threat intelligence report (2019). NTT Security. Available at: https://www.nttsecurity.com/docs/librariesprovider3/ resources/2019gtir/2019_gtir_report_2019_uea_v2.pdf Last accessed: 11.11.2020
9. Symantec Internet Security Threat Report (2019). Symantec. Volume 24. Available at: https://www.symantec.com/content/dam/ symantec/docs/reports/istr-24-2019-en.pdf Last accessed: 11.11.2020
10. Bayern, M. (2019). 71 % of organizations view quantum computing as dangerous. Tech Republic. Available at: https://www.techrepublic.com/article/71-of-organizations-view-quantum-computing-as-dangerous/ Last accessed: 05.06.2022
11. Arslan, B., Ulker, M., Akleylek, S., Sagiroglu, S. (2018). A study on the use of quantum computers, risk assessment and security problems. 6th International Symposium on Digital Forensic and Security (ISDFS), 1–6. doi: http://doi.org/10.1109/isdfs.2018.8355318

12. Chigada, J., Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. SA Journal of Information Management, 23 (1). doi: http://doi.org/10.4102/sajim.v23i1.1277
13. Khan, N. A., Brohi, S. N, Zaman, N. (2020). Ten deadly cybersecurity threats amid COVID-19 pandemic. IEEE. Berlin. doi: http://doi.org/10.36227/techrxiv.12278792
14. South African Banks Risk Information Centre (2020). Identity theft viewed.
15. Impact of COVID-19: The World has changed and so have we (2020). Price Waterhouse Coopers. Available at: https://www.pwc.co.za/en/about-us/integrated-report-2020/impact-of-covid-19.html
16. Crisanto, J. C., Prenio, J. (2020). Financial crime in times of COVID-19 – AML and cyber resilience measures, bank for international settlements. Available at: https://www.bis.org/fsi/fsibriefs7.htm
17. What is Cybersecurity? (2017). Cyberpedia Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security Last accessed: 04.02.2022
18. Olofinbiyi, S. A. (2022). Cyber insecurity in the wake of COVID-19: a reappraisal of impacts and global experience within the context of routine activity theory. ScienceRise: Juridical Science, 1 (19), 37–45. doi: http://doi.org/10.15587/2523-4153.2022.253820
19. Olofinbiyi, S. A., Singh, S. B. (2020). The role and place of COVID-19: An opportunistic avenue for exponential world's upsurge in cybercrime. International Journal of Criminology & Sociology, 9 (11), 221–230.
20. Hubbard, J. (2019). 'SA business underplaying the danger of cybercrime?' Finweek. Available at: https://www.fin24.com/Finweek/Business-and-economy/sa-business-underplaying-the-danger-of-cybercrime-20190313 Last accessed: 01.10.2021
21. SABRIC Annual Crime STATS, (2018). The South African Banking Risk Information Centre. Available at https://www.sabric.co.za/media-and-news/press-releases/sabric-annual-crime-stats-2018/ Last accessed: 04.11.2021
22. Cyber-Crime and South Africa. (2019). Rick Crouch and Associates, private investigators. Available at http://rickcrouch.co.za/wp/cyber-crime-and-south-africa/ Last accessed: 02.12.2020
23. Thompson, M. (2016). In a world of fake news, real journalism must be paid for. The Guardian. Available at: https://www.theguardian.com/commentisfree/2016/dec/16/fake-news-journalism-digital Last accessed: 01 October 2021
24. Head, T. (2019). SA banks targeted by "cyber-attack" – here's how it affects us. The South African. Available at: https://www.thesouthafrican.com/business-finance/banks-cyber-attack-friday-25-october-can-i-use-my-card/ Last accessed: 01.11.2020
25. SA banks hit by ransom attacks (2019). Fin24. Available at: https://www.fin24.com/Companies/Financial-Services/sa-banks-hit-by-ransom-attacks-minor-disruptions-expected-20191025 Last accessed: 02.11.2019
26. Smillie, S. (2019). Hackers give City of Joburg, banks until Monday to pay 'ransom. IOL News Available at: https://www.iol.co.za/saturday-star/news/hackers-give-city-of-joburg-banks-until-monday-to-pay-ransom-35957235 Last accessed: 05.052022
27. City of Joburg shuts down all systems after cyber-attack demanding bitcoin ransom, (2019). News24. Available at: https://www.news24.com/SouthAfrica/News/city-of-joburg-shuts-down-all-systems-after-cyber-attack-demanding-bitcoin-ransom-20191025 Last accessed: 03.05.2022
28. Daniel, E. (2019). South Africa's state-owned power company Eskom hit by double security breach. Verdict. Available at: https://www.verdict.co.uk/eskom-cybersecurity-breach/ Last accessed: 01.162022
29. Whitty, M. T., Buchanan, T. (2012). The online romance scam: A serious cybercrime. CyberPsychology, Behavior, and Social Networking, 15 (3), 181–183. doi: http://doi.org/10.1089/cyber.2011.0352
30. Bulbulia, Z., Maharaj, M. (2013). Factors that influence young adults' online security awareness in the Durban in South Africa. Journal of Information Warfare, 12 (1), 83–96.
31. HAWKS (2015). Workshop for Policy Design towards Digital Security, Cybercrime and Cybercrime Prevention. Electronic Crime Unit of the Directorate for Priority Crime Investigation in South Africa. Held at Emperors Palace. Available at: http://www.nstf.org.za/wp-content/uploads/2015/10/BrigPieterse.pdf Last accessed: 07.11.2019
32. The National Cybersecurity Policy Framework (NCPF, 2015). Available at: http://www.gpwonline.co.za/ Last accessed: 05.06.2022
33. Electronic Communications and Transactions Act (No. 25 of 2002). Available at: https://cisp.cachefly.net/assets/articles/ attachments/00068_electroniccommunications.pdf
34. Cybercrimes Act 19 of 2020. Available at: https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000 Last accessed: 01.06.2022
35. Cybersecurity and Infrastructure Security Agency (CISA, 2021): Cybersecurity Awareness Month Theme and Schedule. Available at: https://www.cisa.gov/cybersecurity-awareness-month Last accessed: 04.06.2022

Received date 03.05.2022
Accepted date 24.05.2022
Published date 28.06.2022

Sogo Angel Olofinbiyi, PhD, Department of Criminal Justice, School of Law, University of Venda, Private Bag X5050, Thohoyandou, Limpopo, South Africa, 0950
E-mail: olofinbiyis@gmail.com