Business & Social Science
IJRBS

Research in Business & Social Science

IJRBS VOL 11 NO 4 (2022) ISSN: 2147-4478

Available online at www.ssbfnet.com
Journal homepage: https://www.ssbfnet.com/ojs/index.php/ijrbs

Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions

Mandlenkosi Richard Mphatheni [(a)] *Witness Maluleke* [(b)] *

[(a)] *Doctor of Philosophy, Criminology candidate, Department of Criminology and Criminal Justice, University of Limpopo, Office No. 4010, Sovenga, 0727, South Africa*

[(b)] *Senior lecturer, Dr, Department of Criminology and Criminal Justice, University of Limpopo, Office No. 4015, New K-Block, Sovenga, 0727, South Africa*

ARTICLE INFO

Article history:

Received 11 March 2022
Received in rev. form 12 May 2022
Accepted 20 May 2022

Keywords:

African regions, Combating, Cybercrime, Cybersecurity, South Africa

JEL Classification:
F5

ABSTRACT

Cybercrime is touted as any harmful behaviour that is in some way related to a computer but does not have a specific legal reference. Therefore, the objective of this study was to explore cybersecurity as a response to combating cybercrime, focusing on demystifying the prevailing threats, while offering recommendations to the African regions. Moreover, this qualitative study employed a non-empirical research design: Systematic review methodology to analyse grey literature and primary research studies peer-reviewed and published, restricted from 2010-2022, not following yearly sequential consideration. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) and Critical Appraisal Skill Programme (CASP) were employed to ensure the trustworthiness of the findings of this study based on reviewed conventional and seminal literature studies on this subject. The main findings of this study rest on a lack of a common universal definition of cybercrime, this has an impact on its prevention and ignores enormous economic value associated with the commission of this crime across the world, African regions included. It was also observed that this criminal act is presently committed with internet usage, consisting of copyright infringements, computer-related fraud, child or adult pornography, and network security violations, amongst others. Equally, addressing this scourge in African regions requires advanced skills and knowledge; exceeding the average computer and internet user. It is also critical to recognise the importance of implementing efficient cybersecurity methods, as policing this crime remains an important component of the Law Enforcement Agencies (LEA), and more innovative strategies are required and a globally coordinated response to this problem is urgently sought.

Introduction

As human behaviour and interaction continue to be shaped by increasingly ubiquitous technologies, organisations must continuously adapt their capabilities to deal with and prevent malicious actors from taking advantage of the shifting technological landscape. Cybersecurity must be prioritised in all domains of society and the economy if we are to unlock the true potential of the digital economy. Cybersecurity is not a separate technology but rather a foundational set of systems spanning technology, people and processes for the Fourth Industrial Revolution [4IR], Jurgens (2022). World Economic Forum (2022) highlights that digital trends and their exponential proliferation due to the Coronavirus disease-2019 (Covid-19) pandemic have thrust the global population onto a new trajectory of digitalisation and interconnectedness. One of the starkest and most troubling new consequences of our digitalised existence is the increasingly frequent, costly and damaging occurrence of cyber incidents, sometimes even paralysing critical services

* *Corresponding author. ORCID ID: 0000-0002-6228-1640*

https://doi.org/10.20525/ijrbs.v11i4.1714

and infrastructure. This trend shows no signs of slowing, notably as sophisticated tools and methods become more widely available to threat actors at relatively low (Or in some cases no) cost.

Cybercrime is crime committed via the Internet and computer systems. One category of cybercrimes are those affecting the confidentiality, integrity and availability of data and computer systems; they include: unauthorised access to computer systems, illegal interception of data transmissions, data interference (Damaging, deletion, deterioration, alteration of suppression of data), system interference (The hindering without right of the functioning of a computer or other device), forgery, fraud, identity theft. Other types of cybercrimes are content-related, and involve the production, offering, distribution, procurement and possession of online content deemed as illegal according to national laws: online child sexual abuse material, material advocating a terrorist-related act, extremist material (Material encouraging hate, violence or acts of terrorism), cyber-bullying (Engaging in offensive, menacing or harassing behaviour through the use of technology). Cybercrime is part of a broader cybersecurity approach, and is aimed at ensuring Internet safety and security (Geneva Internet Platform, 2022).

Moreover, Malby, Mace, Holterhof, Brown, Kascherus and Ignatuschtschenko (2013) share that cybercrime includes all illegal acts committed through electronic use. It therefore requires electronic operations that are aimed at cracking the security of a computer system and compromising the data processed by the computer. In the commission of such crimes, the Internet plays a vital role. Saini, Rao and Panda (2012) define the Internet as "a collection of millions of computers [With] a network of electronic connections between computers." Based on the United Nations (UN) definition of cybercrime, it may be asserted that the scope of cybercrime goes way beyond the many well-known scams that are committed via emails, such as the infamous 'Nigerian 419' scam. Therefore, cybercrime, in addition to email scams, includes a host of other illegal operations that make use of ultra-sophisticated technological means (Fassassi & Akoussan, 2016). To understand and define cybercrime, Wall (2007) argues that it is crucial to explore the contribution that Information and Communication Technologies (ICT) make to global society and how they have transformed the world. Cybercrime is commonly understood as a "harmful behaviour that is somehow related to a computer, however, it has no specific reference in existing laws (Jahankhani, Al-Nemrat & Hosseinian-Far, 2014). McGuire and Dowling (2013) concur that cybercrime is a criminal offence that is committed by using a computer, computer networks, or any other form of ICT. Saini, Rao and Panda's (2012:202) definition is more incisive as they define cybercrime as "an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction". In legal terms, this means that a cybercrime must be legally determined and must be punishable by a conviction or fine.

According to the Bunga (2019), the 'Convention on Cybercrime' states that such criminal acts are committed over the Internet and other computer networks and tend to focus on copyright infringements, computer-related fraud, child or adult pornography, and network security violations. According to the Council of Europe's Cybercrime Convention (2019), cybercrime offences range from illegal activities to gain data access to content and copyright infringements. Jenalda and Kurebwa (2020) argue that the most commonly used definition of cybercrime is that it is "any crime committed using computers, computer networks, or hardware devices." While applying the works of LEA in the African regions, the lack of a clear and universal definition of the cybercrime phenomenon is problematic as it affects prevention measures. Jahankhani, Al-Nemrat, and Hosseinian-Far (2014) confirm that individuals, businesses and even governments have been victims of cybercrime. Contrary to traditional crimes that are committed in identifiable geographical areas, cybercrime is committed through cyberspace and the perpetrators are thus 'faceless' and difficult to trace. The latter scholars thus suggest that a "coordinated global response to the problem of cybercrime is required." This implies that international collaboration and the provision of cybersecurity are pivotal in addressing and eradicating this crime as it can be generally committed across National borders.

The global economic environment is ever changing and has become highly dependent on the use of the Internet and electronic devices. This is a vast shift from the pre twenty-first century era when economic and industrial growth was largely dependent on physical labour. Moreover, driving this major shift in economic activity does not require sophisticated offices or a vast labour force. In fact, our digital economy requires only sophisticated electronic systems, but ironically modern economic growth is threatened by cybercrime and it has become crucial to safeguard global economies by preventing and eradicating this devastating form of crime that has become increasingly threatening and invasive. For instance, Microsoft's Digital Crimes Unit (DCU) recently reported that there are in the region of 400 million victims of cybercrime annually (Ogwueleka & Aniche, 2021).

Globally, cybercrime has cost the economy between $300 billion and $1 trillion, or 0.4 to 1.4 percent of the global Gross Domestic Product [GDP] (Farahbod, Shayo, & Varzandeh, 2020). Morgan (2020) postulates that, globally, financial losses due cybercrime are expected to increase by 15% each year over the next five years. At this rate, it will hit an annual loss rate of $10.5 trillion by 2025 [R161 151 900 000 000,00], which will be an increase from $3 trillion [R46 047 000 000 000,01] in 2015. According to Bloomberg (Ransomware, 2021, June), in 2020 cyberattacks amounted to global losses in excess of $1000 billion [R15 349 000 000 000,00] in 2020, while in that year ransom demands (I.e. Ransomware) had escalated by 40% and malicious Internet infiltration by more than 600% since 2019. These rates are extremely worrisome if one considers that they occurred in a matter of 12 months only.

Kshetri (2019) argues that internet infiltration has already reached an unacceptably high level in many African economies. Economic losses due to cybercrime represent the most significant transfer of economic resources in history. This crime jeopardises incentives for innovation and investment and the financial losses that it causes are much greater than the cost of natural disasters in a single year (Morgan, 2020). Moreover, the African economy's growing exposure to cybercrime is a cause for concern, as developing countries on this continent are increasingly reliant on networked computer systems (Peter, 2017). African countries also often lack the infrastructure to counteract sophisticated cyberattacks. On this continent economic activities utilising digital technology range from data processing to a vast mosaic of social and economic activities, including millions of daily online banking transactions, communications, smartphone downloads of Television (TV) shows and music albums, as well as initiatives like electronic-government (e-government) -e-banking-e-health-e-learning, next-generation power grids, air traffic control and other services (Peter, 2017:50).

The majority of African countries have now begun to capitalise on the economic and social potential of the Internet while a few African countries are utilising the Internet even more extensively, such as Nigeria, South Africa, Angola, Morocco, Algeria, Tunisia, Egypt, Libya, and Sudan (Peter, 2017). Unfortunately, this reliance on networked computer systems is exposed to unprecedented vulnerabilities and many avenues for exploiting these weaknesses have been opened. At least five of Africa's top emerging economies are among the top 30 countries globally in which Internet penetration has caused devastating effects (Peter, 2017). What exacerbates this problem is that countries on this continent relies extensively on mobile banking services with the number of mobile subscribers steadily increasing (Museba, Ranganai & Gianfrate, 2021). According to Nwankwo and Ukaoha (2019), cyberspace applications have considerably affected and reformed various sectors on the African continent such as education, trade and commerce, manufacturing and production, banking and finance, agriculture, public service, LEA, and crime control. They have also affected the administration of justice, politics and governance, healthcare delivery, social relations, and media and communication.

Methodologically, this study adopted the non-empirical research design: Systematic review. Dan (2017) states that this research design is adopted to review progress in a specific study field [Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions]. This research design was employed to identify, evaluate and summarise the findings of this study, focusing on reviewed literature studies to making available evidence more accessible to decision-makers, by offering recommendations (Yannascoli, Schenker & Baldwin, 2013) and Bwanga (2020). To develop understanding and obtaining the relevant information on this subject, the collected data stemmed from relevant databases, such as ‘Google, Google Scholar, EbcoHost, Emerald Insight, Jstor, Internet sources, ProQuest, Sabinet, Sage Online and Science Direct,’ were visited (Maluleke, 2020), this was done following a set of predetermined steps of this research design. The selective keywords retrieved from the research topic were used to obtain relevant information on this subject, using non-probability: Purposefully sampling. The reviewed data were restricted to 2010-2022, not in order of importance and sequence. This was done exercising the exclusion and inclusion criterias of the required data. The PRISMA and CASP were employed to ensure trustworthiness of findings of this study relating to the emergence highlights the trends, strategies and associated challenges of policing cybercrime in Africa.

Despite the enormous benefits of digital services for internet users worldwide, global cyberspace exploitation by miscreants and criminals whose activities on the Internet and whose impact on computer resources have focused on wreaking havoc among legitimate consumers of such resources, has had a significantly adverse effect on the economy. Extensive and advanced cybersecurity has thus become a crucial requirement for safeguarding the global economy and governmental operations in order to ensure peace and security in all spheres of life (Nwankwo & Ukaoha, 2019). The application of technical solutions to combat cybercrime has always been the preferred option for most cybersecurity experts. However, most LEA in the African regions are not equipped with the requisite technological knowledge while most cybercriminals are experts in computer technology. Therefore, the premise of this study rests on cybersecurity as a response to combating cybercrime, to demystify the prevailing threats, while offering recommendations to the African regions.

Literature Review

This section provided synthesis of relevant literature in a manner, which demonstrated that the researchers were familiar with the key authors, texts and, central concepts relevant to this subject. The researchers showed how this study can contributes to what is already known, to fill the niche/gap identified in the introduction section, focusing on situating this study within the academic domain and substantiating the objective of this study as stipulated in the abstract section. The reviewed literature studies was deemed tom be adequate, demarcated sources from 2010-2022, not in sequence, moreover sources of high academic standing, offering integrated ideas, not separate writings on this topic [Cybersecurity as a response to combating cybercrime: Demystifying prevailing threats and offering recommendations to the African regions] were consulted.

Cybercrime and cybercriminals: Cybersecurity induction

hile many factors are driving cybersecurity policies forward, we identified through our survey that 81% of respondents believe that digital transformation is the main driver in improving cyber resilience. The accelerating pace of digitalisation due to the Covid-19 pandemic and the shift of our working habits is pushing cyber resilience forward. As many as 87% of executives are planning to improve cyber resilience at their organisation by strengthening resilience policies, processes and standards for how to engage and manage third parties, World Economic Forum (2022). The term cybercrime refers to several concepts that vary in specificity and impact. Some of these include illegal activities resulting in pecuniary losses while others include violent crimes against individuals or their property such as identity theft and blackmail (Jahankhani, Al-Nemrat, & Hosseinian-Far, 2014). Similar to traditional crimes, the commission of cybercrime relies on the crime triangle (Cross & Shinder, 2008), which constitutes Three (03) factors: 1) A victim, 2) A motive, and; 3) An opportunity.

The victim is the intended and/or actual victim of an attack (Physically or digitally), motive is what motivates the criminal to carry out the attack, and opportunity is what makes the commission of the intended crime possible (Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple, & Bellekens, 2021). However, cybercrime differs from other crimes in that they are physically non-violent as digital devices are used for outcomes resulting in pecuniary loss. However, the emotional and mental harm that cybercrime causes may be just as devastating and traumatising as the outcome of any physical crime. The ever-emerging new features that occur in cyberspace create ever-evolving opportunities for digital crimes. Jahankhani, Al-Nemrat, and Hosseinian-Far (2014:149) view these new features as "key transformative opportunities." They refer more specifically to the following:

i. *Globalisation (Provides offenders with new opportunities to exceed conventional boundaries).*
ii. *Distribution networks (Generate new opportunities for victimisation).*
iii. *Synoptics and panopticism (Allow improved surveillance capability to target victims remotely).*
iv. *Data trails (Create easily accessible opportunities for criminals to commit identity theft).*

Saini, Rao and Panda (2012) list perpetrators of this crime, such as crackers, hackers, pranksters, career criminals, cyber terrorists, cyber bullies, and 'salami attackers' who are cybercriminals that target various stakeholders who then become the victims of cybercrime. Criminality that occurs in cyberspace is known as cybercrime (Jahankhani, Al-Nemrat & Hosseinian-Far, 2014). Unfortunately, the escalation of such crimes seems unstoppable, as measures to curb them have not been adequate or efficient. It has thus become a matter of urgency to devise effective preventative measures to curtail cybercrime by means of effective cybersecurity (Jahankhani, Al-Nemrat, & Hosseinian-Far, 2014). To devise cyberspace security measures requires in-depth understanding of the nature and modus operandi of cybercriminals to expose their motives and operational methodologies. It is also important to understand whom the victims of cyberspace crimes are as it is important to understand how and why these individuals, businesses, and structures fall victim to such crimes. In essence, knowledge is power and this power should be used to create effective cyberspace security measures (Jahankhani, Al-Nemrat & Hosseinian-Far, 2014) to counteract the almost unlimited power that cybercriminals have claimed for themselves.

The execution of a cybercrime requires someone who possesses skills and knowledge that exceed those of the average computer and internet user (Jahankhani, Al-Nemrat & Hosseinian-Far, 2014). Unlike traditional crimes that occur in a particular physical space, cybercrime occurs in the intangibility of cyberspace where perpetrators can remain invisible and are often impossible to trace. The cybercriminal thus feels invincible and devises cyberattacks that are increasingly sophisticated, while it has become increasingly difficult to expose such criminals. Jahankhani, Al-Nemrat, and Hosseinian-Far (2014) argue that, with limited understanding of cybercriminals' whereabouts and modus operandi, it is challenging the existing LEA to address cybercrime effectively. The use of a computer or other similar technological devices, for example; a cellphone or tablet, to name the Two (02), play pivotal roles in the commission of cybercrime (Du Toit, Hadebe & Mphatheni, 2018). A website may even become a victim of cybercrime when access is denied to the legitimate user and when it is hacked and becomes compromised. The vehicle that hackers use is the computer and the victims are either individuals, companies, or even governmental institutions. However, if the computer plays such a significant role in the commission of cybercrime, it may also serve as a buffer between the offender and the victim if effective measures are built into its operating system to detect potential hacking or intrusion (Jahankhani, Al-Nemrat & Hosseinian-Far, 2014).

Forms of cybercrime and their characteristics

Cybercrime is escalating in Africa where it poses a challenge to the economic and social development of countries. Cybercrime, cyber espionage, cyber terrorism, and cyber warfare are all new types of cybercrime that pose a threat to African countries while ruthless cyber criminals such as hackers use cyber vulnerabilities to penetrate and destroy critical systems for financial gain or to hold users hostage (Peter, 2017). The 2020 ransomware attack in which an oil company in the United States of America (USA) was held hostage for a huge sum of money is a case in point (Cyberattack forces a shutdown of a top USA pipeline, 2020). To this course, Council of Europe [CoE] (2001) lists the following several cybercrime offences:

i. Intentional access without the right to the whole or part of any computer system.
ii. Intentional interception, without right, of non-public transmissions of computer data.
iii. Intentional damage, deletions, deterioration, alteration, or suppression of computer data without right, amongst others.
iv. Intentional and serious hindering of the function of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.
v. The production, sale, procurement for use, importation, or distribution of devices designed to commit any of the above crimes, or [I.e. Obtaining] passwords or similar data used to access computer systems, with the intent of committing any of the above crimes.

Considerably, table 1 summarises various cybercrime-related offences [This list inexhaustible].

Table 1: List of cybercrime-related offences

Child pornography
Computer-related forgery
Computer-related fraud
Copyright-related offences
Cyber laundering
Cyberwarfare
Data interference
Identity theft
Illegal access (Hacking, cracking)
Illegal data acquisition (Data espionage)
Illegal gambling and online games
Illegal interception
Misuse of devices
Phishing
Pornographic material
Racism and hate speech on the Internet
Religious offences
Spam and related threats
System interference
Terrorist use of the Internet
Trademark-related offences

Source: Tsakalidis and Vergidis (2017)

Furthermore, Jahankhani, Al-Nemrat, and Hosseinian-Far (2014:155) cite four cybercrime categories that are listed by Yar (2006):

i. Cyber trespassing: The crossing of cyber boundaries into other people’s computer systems to access spaces, where the right of ownership or title has already been established in order to cause damage, for example; hacking or virus distribution.

ii. Cyber deception and theft: These inflict different types of acquisitive harm in cyberspace. At one level are the more traditional patterns of theft such as the fraudulent use of credit cards and (I.e. Cyber) cash, but it is also concerning that there is an increasing potential for the raiding of online bank accounts as e-banking becomes more popular.

iii. Cyber pornography: The breaching of laws that address obscenity and indecency.

iv. Cyber violence: The violent impact of cyber activities on individuals, society, and political groupings or structures is concerning. While such activities may not necessarily result in direct manifestations of a violent attack, the victim will nevertheless experience violence and can bear long-term emotional and psychological scars as a consequence. These activities range from cyber-stalking and hate speech to tech-talk.

Cybercrime activities such as phishing, spamming, hacking, cyber harassment, identity theft, credit/cheque card fraud and Internet auction fraud have been extended to include the spreading of viruses and other malware (McGuire & Dowling, 2013). The identity theft is one of the most worrying forms of cybercrime. Several factors contribute to identity theft such as “Subscriber Identity Module or Subscriber Identification Module (SIM) swap fraud, a strong infrastructure of money wiring services, readily available Internet, prepaid cell phones, high levels of corruption in many companies and government agencies, and a lack of police resources/expertise to combat [I.e. These types] of crime” (South Africa, 2020). Identity theft is a skill that cybercriminals have mastered. For instance, in some cases the attacker can increase the hacked user's access within a system, which results in extended identity fraud, theft, and illegal access to sensitive data. Moreover, the integration of computing and communication capabilities within the power grid has resulted in numerous cyber-physical system vulnerabilities (Sun, Hahn & Liu, 2018).

The nature and extent of cybercrime and cybersecurity in Africa

All countries on all continents are affected by cybercrime. A significant number of infected electronics involving malware have been found in India, Pakistan, Egypt, Brazil, Algeria, and Mexico (Ogwueleka & Aniche, 2021). Cybercrime does not only affect governments and organisations, but individuals as well. According to estimates by Microsoft (2014), about half of all adults who use the Internet have been cybercrime victims. With reference to data provided by a British consulting firm, Kshetri (2019) estimates that about a billion people in Africa will have access to the Internet by 2022. It is also proposed that the increase in Internet access in Africa will be accompanied by various advantages and challenges as it will mean higher exposure to and a more significant number of people with Internet connectivity in Africa. One danger is that Africans will be exposed to the increased risk of becoming victims of cybercrime. Kshetri (2019) postulates that, by 2022, the projected billions of people in Africa with Internet access will not all be law-abiding citizens and that a significant number of these people will be opportunistic criminals. This threat has already reared its ugly head in Ghana where financial institutions experienced over 400 000 malware-related attacks, 44 million spam-related cases, and 280 000 botnet-related cases (Business Ghana, 2018). In 2013, Symantec observed that cybercrime in Africa was increasing more rapidly compared than in the rest of the world (Kshetri, 2019), while in 2016 it discovered that 24 million malware cases had already been experienced on this continent. These numbers undeniably suggest that the number of cybercrime victims in Africa is growing. Former International Telecommunication Union (ITU) Secretary-General, Hamadoun Toure noted this trend with trepidation and commented that cybercriminals saw Africa as a fertile ground for lucrative cybercrimes (Kshetri, 2019).

It is thus undeniable that changing and shifting economic activities that depend on digitisation attract cybercriminals, and African countries with fast-growing economies are well advised to be ready to protect critical documents, vulnerable digital systems, as well as industries and businesses from cyber threats (Peter, 2017). Institutions with financial resources are already investing heavily in cybersecurity to safeguard their resources but, if cyberattacks are on the increase, these vast amounts of money will have been spent in vain. In South Africa, many institutions, particularly those with significant financial capacity, are at high risk of cyberattacks (South Africa, 2020). Online banking is a particularly vulnerable target as about 86% of the population frequently uses online banking services in this country (Kshetri, 2019). Sadly, although cybercrime has been escalating significantly in South Africa, the lack of resources in and the poor technical capability of the South Africa Police Service (SAPS) have limited its efforts to combat the swelling wave of cybercrime and bring perpetrators to book. Therefore, as cybercrime figures continue to rise, South African citizens and business operators must become more resilient in their efforts to defend their operations and/or safeguard their customers. According to Mcanyana and Brindley (2020), iDefense suggests several measures to curb cybercrime such as improving security intelligence; devising protection against internal threats and people-based attacks; and focusing on compliance, standards, and best practices. This advice includes the following measures to ensure security and the threat of cyber invasion:

i. Protection against people-based attacks must be a top priority.
ii. Concentrate on safety/security compliance.
iii. Plan for when, not if (Mcanyana & Brindley, 2020).

According to Mcanyana and Brindley (2020), iDefense argues that security and threat intelligence is not only a central enabling technology for both discovery and investigation activities, but it is also a valuable source of information for understanding threats and making better use of resources in the face of an any impending cyberattack. Combating internal threats is still one of the most difficult challenges that business management teams face today. Because of the rise in phishing, ransomware, and malicious insider attacks, businesses must place great emphasis on cultivating a security-first culture. In this regard, training and education are critical for reinforcing safe behaviours within an organisation and across the entire business ecosystem (Mcanyana & Brindley, 2020). Many organisations already have data compliance tools and solutions in place to combat cybercrime. However, these tools are frequently misconfigured. Data compliance occurs automatically when business tools and services are correctly installed and configured and therefore particular emphasis should be placed on reducing ‘shadow’ ICT. Detection and ‘pre-breach’ preparation is thus vital in every business where clear procedures for post-breach incidents should be established to ensure incident-response capability, post-incident analysis, backed-up data, anti-Distributed Denial-of-Service (DDoS) measures, and access to Cloud security brokers (Mcanyana & Brindley, 2020).

Understanding the impact of cybercrime: A global phenomenon

Africa experiences hundreds of millions of cyberattacks annually (Kshetri, 2019). Internationally the economy remains heavily reliant on the Internet but it is vulnerable to various risks and threats posed by cyberspace criminals (Saini, Rao, & Panda, 2012). In the modern economy “stocks are traded via the Internet, bank transactions are performed via the Internet, and purchases are made using credit cards via the Internet” (Saini, Rao, & Panda, 2012:206). As the international economy thus largely depends on cyberspace, its disruption through cybercrime is a significant concern. Tsakalidis and Vergidis (2017) confirm that cybercrime offences pose a severe threat to international economies, financial security concerns, and the pecuniary and even physical well-being of organisations and individuals. A disruption in one region of the globe may have a ripple effect on many other regions and thus any disruption of the cyber economy may result in a shock wave that may shake the world. The economic collapse of the property market in the USA in 2008 that caused financial devastation across the global economy clearly demonstrates this point. About this crisis, Calvo (2010:1) writes the following in verbatim:

“The impact of the USA financial crisis that unfolded in 2008 has been global. It was felt in output, trade, and cross-border capital flows and transfers. Incomes have dropped and consumption patterns are changing, placing at risk the human development gains of the 1990s. At the heart of this global crisis is a credit crunch that has put financial strains on firms and individuals and has led to a large number of job losses and drops in income from other sources ...The global financial crisis has had a severe impact on South Africa. The economy went into recession in 2008/09 for the first time in 19 years. Nearly a million jobs were lost in 2009 alone and the unemployment rate continued to remain high with 25%.”

The cost of cybercrime to the world economy is estimated at USA $500 billion [R7 658,50]. About 20% of Small and Medium-sized Enterprises (SMEs) have been affected by the cybercrime scourge. More worrisome is that cybercriminals are targeting emerging economies as they are easy targets that cybercriminals view as “low-hanging fruit” (Kshetri, 2019:77). The African economy in particular has become a significant victim of cyber threats. Cybercrime in 2017 cost African economies USA $3.5 billion [R53 609

500 000,00] (Kshetri, 2019). According to Serianu [Sa] (in Kshetri, 2019), who works for a Kenya-based IT and business advisory firm, in Nigeria the annual total cost of cybercrime in 2017 was USA $649 million [R9 942 031 000,00] while Kenya lost USA$210 million [R3 216 990 000,00] to cybercrime. Kshetri (2019) further cites the South African Banking Risk Information Centre (SABRIC) that asserts that South Africa loses about USA$157 million [R2 405 083 000,00] annually due to cyberattacks.

Subsequently, this estimate is above South Africa's GDP, 350, USA$6 billion [R91 842 900 000,00], and the Nigerian GDP, which is 521, US$8 billion. These two African countries are the continent's biggest economies (Fassassi & Akoussan, 2016). Nigeria is reported to be severely suffering from the scourge of cybercrime as its economy is estimated to be losing USA$500 million per annum [R7 653 575 000,00] (Fassassi & Akoussan, 2016). McGuire and Dowling (2013) argue that the overall estimated cost of cybercrime in the United Kingdom (UK) is 27 billion euro. This figure was confirmed by by Detica (2011). The Ponemon Institute published its analysis of the total cost of cybercrime for 58 public and private organisations in the USA in 2015. According to this survey, the annual cost of cybercrime in this country had more than doubled since 2010, averaging USA$6.5 million [R99 530 925,00] (Ifinedo, 2018).

Banks and financial concerns that are the primary institutions used by the man on the street for financial support and safeguarding are also highly vulnerable to financial cybercrime. In fact, the frequency of attacks on them by hackers is increasing (Fassassi & Akoussan, 2016). Tsakalidis and Vergidis (2017) estimate that global cybercrime has cost the world USA$225 billion [R3 399 363 900 000,00]. Conversely, Fassassi and Akoussan (2016) estimate the global cost of cybercrime at USA$500 billion [R7 656 225 000 000,00]. Tsakalidis and Vergidis (2017) argue that technological advancements have posed a severe threat to global financial security and national economies as they are all threatened by cybercrime. Cybercrime affects both the financial sector and individuals as it ranges from identity theft to sexual exploitation (I.e. Particularly of children) and cyber harassment. The latter authors conclude that the impacts of cybercrime range from minor discomfort to severe mental harm as well as huge public and financial losses. The table below lists various aspects of discomfort and disruption caused by cybercriminals.

Table 1: Harm inflicted and disruption caused by cybercrime

Individual harm	Systematic harm	Generalised individual harm	Direct systematic harm
Emotional distress/fear	Aggregated individual harm	Deterioration of life quality	Chaos and anarchy
Loss of life	Accumulated loss of property	Civil disturbance	Erosion of essential government functions
Loss of property	Moral harm	Social disorder	Critical infrastructure shut down
Moral harm	Emotional distress	Moral decay	Countries' engagement in armed conflicts
Physical injury	Victims fear the same offence	Dispossession of wealth	
Substantial damage		Violation of social relationships	
		Economic depression	

Source: Tsakalidis and Vergidis (2017)

Based on a cybercrime victimisation survey, McGuire and Dowling (2013) argue that younger people and males who have access to the Internet are most vulnerable to computer virus attacks. Saini, Rao, and Panda (2012) believe that organised syndicates are now using the Internet to commit significant acts of fraud and theft and that cyberspace has opened up opportunities for criminals to shift their activities from traditional criminal methods and spaces to the Internet, which has become a fertile space for fraud, identity theft, and other computer-based acts of crime. Saini, Rao, and Panda (2012) add that these types of fraud have earned criminals millions annually while investors have lost huge amounts. Cybercrime has caused the devastating disruption of computer functions and the demise of many businesses and the financial collapse of numerous individuals. The development and improvement of technological products and services are dependent on the exchange of data between individuals and businesses (Olano, 2018), but Internet users are often unaware of the various cybercrimes that they might fall victim to and they thus do not take sufficient precautionary measures to protect themselves against cyberattacks.

If ignored, cybercrime is a phenomenon that can cause irreparable harm to companies' and individuals' privacy, finances, and data integrity. Cybercriminals use malicious codes to alter computer codes and data, which causes disruptions that fatally, compromises data, leading to cybercrimes such as identity theft and data hacking (Burnap, French, Turner & Jones, 2018). For example, a cyberattack on Sony resulted in irreparable damage when it lost an estimated USA$20 million [306 249 000,00] in revenue and another USA$32 billion [R489 873 280 000,00] due to losing control of customer data (Hou, Gao, & Nicholson, 2018). Maintaining privacy and data security has always been a problematic issue in the ICT domain as an extensive cyberattack could expose a large portion of the population to unprecedented financial loss. Everyone in the corporate world and in society who uses the Internet is vulnerable to cyber-criminals who are able to expose users' particular vulnerabilities. Cyber-victimisation results in significant economic and personal consequences for Internet users and has negative consequences for economies and the cyber infrastructure (Barosy, 2019).

National security imperatives

Recognising the need to implement cybersecurity and well-protected investments is pivotal in curbing cybercrime. Only when both the economic and social promise of the Internet are fully protected will economic dividends be secured, particularly in emerging economies with relatively high Internet penetration and digital network readiness. The absence of cyber protection initiatives and the implementation of effective measures pose high risks for both the public and private sectors (Peter, 2017). Pavlova (2020) highlights that 'peace and security' are essential for economic growth but, regrettably, they can be and are undermined by crime and in contemporary society, 'peace and safety' in both offline and cyberspace need to be ensured. It is unfortunate that governmental institutions in particular are persistently struggling to ensure the safety and security of citizens' data and information regardless of the implementation of various protective measures. It seems that cybercriminals are always one-step ahead as officialdom has not yet discarded the cloak of bureaucracy and red tape that has forever covered its operations like a shroud. One can only wonder how difficult it really is to ensure peace, safety, and security within the cyberspace world.

Policing cybercrime has been acknowledged as a vital component of the LEA in recent years, but Clark and Hakim (2016) stress that there is a need for more innovative strategies than those that have been used hitherto to deal with highly sophisticated acts of cybercrime. The first step will of course be to address and eradicate policing deficits that often render policing in this field ineffective. In this regard, the latter authors suggest that an integrated and collaborative approach should be adopted to ensure that all relevant stakeholders in the public and private domains work together to devise and implement workable safety and security policies. However, as policies are notorious poorly implemented and policed, practical implementation strategies need to be devised as a matter of urgency. Pavlova (2020) summarises various methods that role players should adopt to ensure the safety of the cyberspace domain. Clark and Hakim (2016) urge that the following measures are essential in securing cyber safety: **i)** Individuals need to play a critical role as frontline users of the Internet in the fight against cyberspace crime; **ii)** Individuals, organisations, and governments must frequently install anti-virus programmes, scour for viruses, and keep fire walls updated, and; **iii)** Individuals must be critical of what they put online and which websites they enter.

Using a soccer metaphor, Clark and Hakim (2016) refer to 'mid-field' role players who are organisations whose primary goal is not directed at safety in cyberspace but who function within the safety and security net that measures within cyberspace provide. For example, the services of Internet Service Providers (ISPs), hard- and software producers, and Internet hotlines such as Internet Crime Complaint Centre and the International Association of Internet Hotlines should be harnessed by both individuals and companies to track and bring cybercrime perpetrators to book (Clark & Hakim 2016). These structures should play the role of the mid-fielder to ensure safety and security within the cyberspace world. The ISPs also play a critical role in this regard, as they provide Internet access to individual computer users as well as to organisations and industries. Clark and Hakim (2016) also argue that the last line of defence against cyberspace threats is to rope in the support and services of existing institutions whose primary role it is to ensure the security of the cyberspace world. The criminal justice system and the private security industry are pivotal role players in this regard. For instance, commercial cybersecurity companies may be harnessed as key role players in combating criminal cyberspace acts, as they already possess virus scanners and the ICT infrastructure to detect and identify cyberspace criminals. Unfortunately such sophisticated services will come at great cost, and it seems logical that official LEA should invest their often wasted budgets in procuring the necessary infrastructure and human resources to drive effective and functional anti-cybercrime units that are not debilitated by red-tape and bureaucratic inefficiency.

Factors that enhance exposure to cybercrime

The Cybersecurity Exposure Index (CEI), which regularly surveys 108 countries on all continents worldwide (I.e. Europe, America, Asia-Pacific, and Africa), lists the countries that are least and most affected by cybercrime. In terms of cybersecurity threats, Africa is the most affected continent while Europe is the least exposed to cybersecurity threats (CEI, 2020). Finland, Denmark, Luxembourg, Australia, and Estonia are the countries that are least exposed to cybercrime while African countries are highly vulnerable to cybercrime as there is no single country on this continent that appears on the list of the world's most minor cybersecurity-exposed countries. Afghanistan is the most vulnerable to cybersecurity threats, followed by Myanmar, Ethiopia, Palestine, and Venezuela. In Africa Ethiopia is the country that experiences that highest threat to cybersecurity followed by Tanzania, Zimbabwe, Algeria, and Cameroon. Namibia the least exposed to cybersecurity on the African continent. Countries in Africa with a high level of commitment to cybersecurity are Mauritius at the top, followed by South Africa, Egypt, Kenya, Nigeria, Tunisia, and Uganda. Statistically, table 2, 3 and 4 showcased the most exposed countries to cybercrime, regional and international, together with the ranking of African countries. Specifically, table reveals that on the international front, the United States ranked number one, followed by the UK and Saudi Arabia, both in second place (Larnyoh, 2021).

Table 2: The most exposed countries to cybercrime

Country	Rank	Exposure score
Afghanistan	85	1.000
Myanmar	84	0.910
Ethiopia	83	0.866
Palestine	82	0.855
Venezuela	81	0.807
Libya	80	0.793
Bolivia	79	0.783
Nepal	78	0.762
Bangladesh	77	0.759
Pakistan	76	0.755

Source: The CEI (2020)

Table 3: Cybercrime Security Exposure Index ranking of African countries

Country	Africa Rank	World Rank	Score
Mauritius	1	12	0,200
South Africa	2	34	0,414
Egypt	3	48	0,548
Kenya	4	48	0,548
Nigeria	5	58	0,614
Tunisia	6	58	0,614
Uganda	7	61	0,634
Namibia	8	65	0,679
Cameroon	9	69	0,707
Algeria	10	70	0,721
Zimbabwe	11	71	0,724
Tanzania	12	72	0,731
Ethiopia	13	83	0,910

Source: The CEI (2020)

Table 4: Top 10 countries in Global Cybersecurity Index

Country	Score	Rank
USA	100	1
UK	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Republic of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada	97.67	8
France	97.6	9
India	97.5	10

Source: Larnyoh (2021)

Furthermore, in Africa, Mauritius ranked top, but was 17th on the global ranking. Egypt was second in Africa, followed by Ghana, as illustrated in table 5.

Table 5: Top 10 African countries in Global Cybersecurity Index

Country	Overall score	Regional rank
Mauritius	96.89	1
Tanzania	90.58	2
Ghana	86.69	3
Nigeria	84.76	4
Kenya	81.7	5
Benin	80.06	6
Rwanda	79.95	7
South Africa	78.46	8
Uganda	69.98	9
Zambia	68.88	10

Source: Larnyoh (2021)

The cyber threat landscape in South Africa

It seems that cyberspace offenders perceive industries and businesses in South Africa as inadequately defended compared to those in affluent countries and they thus seize every opportunity to commit cyberspace offences here. Cyberspace criminals calculate the risk of being caught − or receiving limited punishment when caught − and they thus target South Africa for the notoriety of its lenient cybercrime policy (Africa Tech, 2020; and Mcanyana & Brindley, 2020). Cybercrime offenders have now started focusing on South Africa due to insufficient and ineffective efforts to provide cybersecurity, the ineffective implementation of a policy framework and the LEA instructions to curb cybercrime, and a lack of public knowledge on the cyberspace menace. Many other African countries make inadequate cybersecurity investments due to being plagued by high crime rates, inequity and poverty, high unemployment rates, and a skilled labour shortage. While many developing economies consider cybersecurity necessary, businesses frequently lack the resources to invest in such protection. This limits their ability to implement measures to prevent and mitigate advanced threats in cyberspace (Mcanyana & Brindley, 2020).

Cassim (2011) remains a critical researcher on this subject focusing on African countries,' as it is noted that the available LEA inadequacy to deal with cyber offences. The agencies in developing countries are generally not well equipped in terms of human resources, intelligence networks, and infrastructure and they have inadequate and limited legislation to address cybercrime comprehensively. For example, in South Africa, the National Assembly passed the Cyber Crimes Bill only in January 2020 as intense public scrutiny of its impact on privacy and freedom of expression has resulted in delays. Furthermore, while the SAPS is now authorised to prosecute such crimes, a lack of cybercrime training may pose challenges in the short term (Mcanyana & Brindley, 2020). According to the Africa Tech (2020), most developing countries consider cybersecurity necessary but they cannot invest adequate funds due to pressing needs such as crime prevention, food deprivation, inequality, unemployment, and a lack of skilled labour. Insight into the Cyber threat Landscape in South Africa (2020) supports the assertion that cybercrime occurs mainly because of insufficient efforts to provide cybersecurity in South Africa. Cassim (2011: 127) agrees with the view that African countries' priorities are not directed a cybersecurity as they are facing urgent challenges such as "...alleviating poverty, the Aids crisis, the fuel crisis, political instability, ethnic instability, and traditional crimes such as murder, rape, and theft". It is therefore logical that efforts to address cybercrime and investments in cybersecurity are lagging.

Insight into the Cyber threat Landscape in South Africa (2020) also concurs with the notion that developing countries deem cybersecurity important. However, they are unable to invest in such protection due to insufficient funds. Insight into the Cyber threat Landscape in South Africa Insight into the Cyber threat Landscape in South Africa Insight into the Cyber threat Landscape in South Africa. Moreover, industries in developing countries that can invest sufficient funds in cybersecurity are unable to do so because of the lack of skilled practitioners in cybersecurity. It thus seems reasonable to argue that industries and organisations need to instil a safety culture within their organisations and that businesses need to prioritise training and education for safe behavioural reinforcement. The changing dynamics of the Internet that include the expansion of Internet capabilities and easy internet accessibility are directly linked to new forms of criminal behaviour in cyberspace (Cassim, 2011). Such offences seem limitless, as the cyber offender does not need to meet the victim at a certain place and time. This new form of crime thus requires specialised policies to effectively address and curb them (Cassim, 2011). The call for new specialised laws to address cybercrime and provide cybersecurity has been intensified because of the inability of existing laws to address the challenges offered by cyber offences in all countries and in countries in Africa particularly.

South Africa has Africa's second-highest GDP and the second-fastest Internet and investments in new technological start-ups here is brisk. The country is thus shifting to technological tools to meet a wide range of business and social needs. Analysts at iDefense, however, note that South African Internet users are less experienced and technically 'savvy' than users in developed countries (Mcanyana & Brindley, 2020). While cybercrime perpetrators continue to attempt to exploit digital platforms such as banking sites and other locations that store financial data, the mitigation strategies these entities employ are typically robust but individuals remain vulnerable to cybercrimes due to their low levels of technical acumen. For instance, personal devices and applications used on business networks can pose a significant risk by acting as entry points for ransomware or other infection vectors to infiltrate a network. According to iDefense analysts, the use of shadow ICT or applications and infrastructure without knowing an enterprise's ICT department is common in South African businesses (Mcanyana & Brindley, 2020).

Conclusions

It is concluded that cybercrime and cybersecurity are concepts that have emerged in the last few decades. As a result, there is no widely accepted definition for these concepts. Various scholars and international organisations have defined both concepts. However, it is worth noting that one of the most popular definitions of cybercrime is a criminal activity that occurs in cyberspace and involves a computer network and a network user. With the assistance of a computer, criminal activity can be committed against the computer or the computer user. In contrast to traditional crime, cybercrime has no geographical boundaries. It does not necessitate any physical contact between the offender and the victim. An individual, a company, or a country against someone or a company on a different continent can commit it. Thus, Cybersecurity is a framework or set of measures in place or to be implemented to counteract any cybercrime exposure. As a result, various industries, organisations, and countries developed cybersecurity frameworks. The global economy's reliance on cyberspace, combined with cybersecurity's failure to combat cybercrime, has had a significant economic impact. The already struggling African economy has taken a significant hit because of cybercrime. African nations have made little progress in combating the scourge of cybercrime. African countries appear to be vulnerable to cyberspace criminal activities due to a lack of skilled labour and insufficient investment in cybersecurity by African nations. The struggle to combat traditional crimes and poverty in Africa has resulted in less investment in cybersecurity. Collaboration between the government, scholars, and organisations where information is shared is a shared interest in combating cybercrime and strengthening Cybersecurity.

There is currently no comprehensive international legal framework addressing Cybersecurity. International efforts to address the issue have been limited in scope, focusing primarily on data privacy regulations and human rights, at the expense of a broader effort to define and differentiate various levels of cyber aggression and codify an international response to its challenges. Nations will continue to face difficulties assessing the legality of their response to a given attack in the absence of a comprehensive international definition of the types of cyber aggression. The researchers' further recommends that prevention measures aimed at combating cybercrime are insufficient due to a lack of a universal definition of cybercrime. As a result, international organisations and the global community must reach an agreement on what constitutes cybercrime. A shared understanding of what constitutes cybercrime will aid in the effective prosecution of cybercrime. Combating cybercrime and ensuring cybersecurity necessitate global collaboration.

Moreover, local and regional organisations and businesses should have departments/units dedicated to dealing with cybercrime and cybersecurity breaches. Personnel with advanced knowledge of cyberspace must be assigned to such a unit or department. Personnel with extensive knowledge of cyberspace will deduce cybercriminals' motivations and assist in apprehending the criminals and devising new measures to prevent future cyberspace breaches. Cooperation among relevant stakeholders, including the public and private sectors, is needed to implement safety and security policies. In addition, there should be an alternative strategy in place to address policing deficiencies. African countries should collaborate to find effective ways of combating cybercrime and implementing cybersecurity measures that bring peace, safety, and security to their respective nations. Cooperation among African countries will result in a stable and robust cybersecurity infrastructure on the African continent. Avoiding cybercrime necessitates a focus on security awareness training. Priority must be given to communication and the enforcement of security policies.

Acknowledgement

All authors have read and agreed to the published version of the manuscript.
Author Contributions: Conceptualisation, M.R and W; methodology, W; validation; W; formal analysis, M.R and W; investigation; M.R and W, resources, M.R and W; writing original draft preparation, M.R and W; writing review and editing, W; supervision, W; project administration, M.R and W.
Informed Consent Statement: The researchers took the following into account to ensure ethicality: The University of Limpopo (UL) research ethics policies and exercising honesty in terms of acknowledging 'all' sources used in this study, aided by the list of references and avoiding of plagiarism.
Data Availability Statement: The data presented in this study are available on request from the corresponding author.
Conflicts of Interest: The authors declare no conflict of interest.

References

Africa Tech. (2020). *South Africa has the third-highest number of cybercrime victims globally report*. Retrieved from: https://africabusinesscommunities.com/tech/tech-news/south-africa-has-third-highest-number-of-cybercrime-victims-globally-report/.

Aishwarya, K., Pratiksha, S., Hule, P & Sayli, M. (2018). Survey on Network security. *International Journal of Current Trends in Science and Technology,* 8(1), 47-53.

Barosy, W. (2019). *Successful operational cyber security strategies for small businesses*. Unpublished Doctoral Business Administration Thesis. Minneapolis, Minnesota: Walden University.

Bunga, D. (2019). Legal Response to Cybercrime in Global and National Dimensions. *Padjadjaran Journal of Law*, 6(1), 69-89.

Business Ghana. (2018). *Bank of Ghana launches cyber security directive for financial institutions.* Retrieved from: https://www.businessghana.com/site/news/business ....

Bwanga, O. (2020). How to conduct a qualitative systematic review to guide evidence-based practice in Radiography? *International Journal of Sciences: Basic and Applied Research*, 52 (1):205-213.

Calvo, S.G. (2010). *The global financial crisis of 2008-10: A view from the social sectors*. Retrieved from: http://hdr.undp.org/en/content/global-financial-crisis-2008,10?utm ...

Cassim, F. (2011). Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players. *The Comparative and International Law Journal of Southern Africa*, 123-138.

Clark, R.M & Hakim, S. (Editors). (2016). *Cyber-physical security: protecting critical infrastructure at the state and local level* (Vol. 3). London: Springer.

Cyberattack forces a shutdown of a top USA pipeline [Online]. (2020). Cyberattack. Retrieved from: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.

Cybersecurity Exposure Index [Online]. (2020). Cybersecurity Index shows the most exposed countries. Retrieved from: https://www.securitymagazine.com/articles/92614-cyber ...

Dan, V. (2017). *Empirical and non-empirical methods*. Retrieved from: https://www.ls1.ifkw.uni-muenchen.de/personen/wiss_ma/dan_viorela/.

Detica [Online]. (2011). *The cost of cybercrime.* Retrieved from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf.

Du Toit, R., Hadebe, P.N & Mphatheni, M. (2018). Public perceptions of Cybersecurity: a South African context. *Acta Criminologica: African Journal of Criminology and Victimology*, 31(3), 111-131.

Farahbod, K., Shayo, C & Varzandeh, J. (2020). Cybersecurity Indices and Cybercrime Annual loss and economic impacts. *Journal of Business and Behavioural Sciences*, 63.

Fassassi, A & Akoussan C.F. (2016). Cybercrime in Africa: Facts and figures. Retrieved from: https://www.scidev.net/sub-saharan-africa/features/cybercrime-africa-facts-figures/.

Geneva Internet Platform [Online]. (2022). Retrieved from: Cybercrime. https://dig.watch/topics/cybercrime.

Jahankhani, H., Al-Nemrat, A & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In: *Cyber Crime and Cyber Terrorism Investigator's Handbook* (Pp. 149-164). Amsterdam: Elsevier Science.

Jenalda, M & Kurebwa, J. (2020). Multilateral Responses to Cybercrimes in the SADC Region: The Case of Zimbabwe and South Africa. *Canadian Social Science*, 16(12), 1-10.

Jurgens, J. (2022). *Preface*. Cologny, Switzerland: World Economic Forum.

Kshetri, N. (2013). *Cybercrime and Cybersecurity in the global South. Basingstoke*. United Kingdom: Palgrave Macmillan: Houndmills.

Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C & Bellekens, X., (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security*, 105, 102248.

Larnyoh, M.T. (2021). Ranked: Top 10 African countries in Global Cybersecurity Index: The International Telecommunication Union (ITU) has released the latest Global Cybersecurity Index (GCI). July 01, *Business Insider Africa [Online]*. Retrieved from: https://africa.businessinsider.com/local/markets/ranked-top-10-african-countries-in-global-cybersecurity-index/bfrmkgk.

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S & Ignatuschtschenko, E. (2013). *Comprehensive study on cybercrime.* United States of America: United Nations Office on Drugs and Crime.

Maluleke, W. (2020). The African scare of Fall Armyworm: Are South African farmers immune? *International Journal of Social Sciences and Humanity Studies*, 12 (1), 207-221.

Mcanyana, W., Brindley., C., 2020. *Accenture. Insight into the cyberthreat landscape in South Africa*. Retrieved from: https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf.

McGuire, M & Dowling, S. (2013). Cybercrime: A review of the evidence. *Summary of key* findings and implications. *Home Office Research report*, No. 75.

Morgan, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybercrime Magazine*, 13.

Museba, T.J., Ranganai, E & Gianfrate, G. (2021). Customer perception of adoption and use of digital financial services and mobile money services in Uganda. *Journal of Enterprising Communities: People and Places in the Global Economy*, No. 1.

Nwankwo, W & Ukaoha, K.C. (2019). Socio-Technical perspectives on Cybersecurity: Nigeria's Cybercrime Legislation in Review. *International Journal of Scientific and Technology Research*, 8(9), 47-58.

Ogwueleka, F.N & Aniche, A.D. 2021. Information and communication technology, cyber-security and counterterrorism in Africa. In *The Routledge Handbook of Counterterrorism and Counterinsurgency in Africa* (Pp. 129-151). United Kingdom: Routledge.

Pavlova, P. (2020). Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups. *Peace Human Rights Governance*, 4(3).

Peter, A.S. (2017). Cyber resilience preparedness of Africa's top-12 emerging economies. *International Journal of Critical Infrastructure Protection*, 17, 49-59.

Ransomware [Online]. 2021. Retrieved from: https://www.bloomberg.com/subscriptions.

Tsakalidis, G & Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(4), 710-729.

World Economic Forum. (2022). *Global Cybersecurity outlook 2022: Insight report January 2022*. Cologny, Switzerland: World Economic Forum.

Yannascoli, S.M., Schenker, M.I & Baldwin, K. (2013). *How to write a systematic review: A step-by-step guide?* Retrieved from: https://www.semanticscholar.org/paper ...

Publisher's Note: SSBFNET stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.