



## **A Cybersecurity Culture Framework for Grassroots Levels in Zimbabwe**

**GABRIEL KABANDA<sup>1\*</sup> and TINASHE CHINGORIWO<sup>2</sup>**

<sup>1</sup>Zimbabwe Academy of Sciences, Trep Building, University of Zimbabwe Harare, Zimbabwe.

<sup>2</sup>Zimbabwe Open University, Corner House, Samora Machel Avenue/ L.takawira Street Harare, Zimbabwe.

### **Abstract**

Cybersecurity is a combination of technologies, processes and operations that are designed to protect information systems, computers, devices, programs, data and networks from internal or external threats, harm, damage, attacks or unauthorized access.<sup>1</sup> The research was purposed to develop a cybersecurity culture framework which ensures that grassroot users of cyberspace are secured from cyber threats. Literature review showed that in Zimbabwe, no research had attempted to come up with a cybersecurity culture framework for grassroot users of cyberspace. The research was guided by the interpretivist paradigm and employed a qualitative methodology. A descriptive research design was used to answer the research questions and unstructured interviews were done to ascertain the cybersecurity needs and challenges of grassroot users of cyberspace. A cybersecurity culture framework was then crafted based on the research findings. The researchers recommended that Zimbabwe should have a cybersecurity vision and strategy that cascades to the grassroot users of cyberspace. Furthermore, the education curricula should be revised so that it incorporates cybersecurity courses at primary and secondary school level. This will then ensure that ICT adoption is matched with cyber hygiene and responsible use of cyberspace.



### **Article History**

Received: 15 July 2021

Accepted: 19 February 2022

### **Keywords**

Artificial Intelligence;  
Big Cloud Computing;  
Culture Framework;  
Cybersecurity,  
Data Analytics,  
Internet Of Things;  
Machine Learning,

### **Introduction**

#### **Background**

Cybersecurity is a combination of technologies, processes and operations that are designed to protect

information systems, computers, devices, programs, data and networks from internal or external threats, harm, damage, attacks or unauthorized access.<sup>2</sup> The essence of cybersecurity is to consolidate the

**CONTACT** Gabriel Kabanda ✉ mmshinde2009@gmail.com 📍 Zimbabwe Academy of Sciences, Trep Building, University of Zimbabwe Harare, Zimbabwe.



© 2021 The Author(s). Published by Oriental Scientific Publishing Company.

This is an  Open Access article licensed under a Creative Commons license: Attribution 4.0 International (CC-BY).

Doi: <http://dx.doi.org/10.13005/ojst14.010203.03>

confidentiality, integrity, and availability of computing resources, networks, software programs, and data into a coherent collection of policies, technologies, processes, and techniques for the prevention of the occurrence of cyber-attacks.<sup>3</sup> The key cybersecurity applications are the detection of intrusion and malware. The Network Intrusion Detection Systems (NIDS) distinguishes between malicious users and the legitimate network users with a view to ascertain anomalous violation of security policies.<sup>4</sup> NIDS are categorized into two taxonomies, anomaly detectors and misuse network detectors. According to Bloice and Holzinger,<sup>5</sup> the components in Intrusion Detection and Prevention Systems (IDPSs) can be sensors or agents, servers, and consoles for network management. Hackers are now able to devise innovative ways of breaking into network systems secured by firewall, encryption, antivirus software, secure protocols, etc.

The attitudes, assumptions, behaviour, beliefs, values and knowledge exhibited by people during their interaction with the information assets is what constitutes the cybersecurity culture.<sup>6</sup> According to Malyuk and Miloslavskaya<sup>7</sup> and United Nations,<sup>8</sup> the solution of emerging cyber security challenges will not be rectified by government or law enforcement bodies alone but in conjunction with society. A strong cybersecurity culture influences the security behaviour and mindsets of people, and will stand as a human firewall against threats without coercion.<sup>9</sup> Currently, there is a general lack of knowledge and information on cybersecurity matters in Africa.<sup>8</sup> The establishment of a cybersecurity culture is an essential approach to cybersecurity.<sup>10</sup> Cybersecurity legal frameworks to fight cybercrime are still being developed and in their infancy. Twenty-one countries in Africa have Data Protection Legislations of which 13 have both Data and Cyber Security Legislation. Zimbabwe is one of the African countries that has a provision for a Data Protection Authority together with the Cape Verde, Equatorial Guinea, Ghana, Lesotho, Malawi, Mauritius and South Africa. By April 2016, 11 countries notably, Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia seemed to have basic substantive and procedural law provisions in place. Substantive and procedural law provisions are partially in place in only 12 African countries namely Algeria, Benin, Gambia, Kenya, Madagascar,

Morocco, Mozambique, Rwanda, South Africa, Sudan, Tunisia and Zimbabwe. Sadly, the majority of African countries are still yet to put in place in full force specific legal provisions on electronic evidence and cybercrime.

### **Statement of The Problem**

The greatest risk of cyber-attacks has increased phenomenally due to the astronomical increase in internet-connected systems.<sup>3</sup> The gross limitations of firewall protection against external threats have proved their inadequacy. The rapid development of computing and digital technologies has necessitated the need to revamp cyber defense strategies for most organizations. Consequently, there is an imperative for security network administrators to be more flexible, adaptable, and provide robust cyber defense systems in real-time detection of cyber threats. Progress in the ICT industry in Zimbabwe is hampered by the lack of a framework which provides direction, focus, guidance and a standardised way of addressing cybersecurity. As an integral part of the development into information societies, the protection of valuable information, infrastructure and individuals from cyber-attacks has become of primordial importance in countries like Zimbabwe. What is required under the circumstances to prevent cyber-attacks in Zimbabwe is a cybersecurity culture framework.

### **Purpose of Study**

The research was purposed to develop a cybersecurity culture framework which ensures that grassroot users of cyberspace are secured from cyber threats.

### **Research Objectives**

The research objectives were to:

- a) Ascertain the cybersecurity challenges being faced in Zimbabwe
- b) Investigate cybersecurity needs of grassroot users of cyberspace in Zimbabwe
- c) Develop a cybersecurity culture framework for grassroots users of cyberspace in Zimbabwe

### **Research Questions**

The main research question was:

*How is a cybersecurity culture framework developed to thwart the cybersecurity risks for the grassroot users of cyberspace in Zimbabwe?*

The sub questions were:

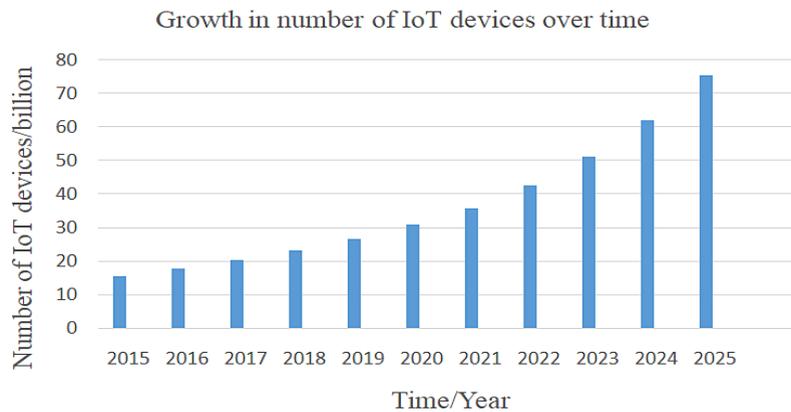
- a) What are the cybersecurity challenges being faced in Zimbabwe?
- b) How can the cybersecurity needs of grassroots users of cyberspace in Zimbabwe be met?
- c) How can a cybersecurity culture framework be developed for grassroots users of cyberspace in Zimbabwe?

**Literature Review**

**Internet of Things (IoT)**

The era of the Internet of Things (IoT) generates huge volumes of data collected from various heterogeneous sources which may include mobile devices, sensors and social media. The Internet of Things (IoT) involves the interconnection among the interconnected devices. The transmission method can be wired or wireless depending on the devices.<sup>11</sup> The exponential rise of the IoT support the fact that cyberspace is growing at an exponential rate and will continue to grow with no sign of slowing down. Secure consumption of cyberspace is contingent upon the cultivation of a cybersecurity culture.<sup>12</sup>

Hackers are now targeting the Internet of Things (IoT).<sup>13</sup> Due to the advances in IoT, the technological integration and collaboration is envisaged to increase in complexity which precipitates cybersecurity risk.<sup>14</sup> Interconnectivity of people, devices and organizations in this digital era unveils access points where cyber criminals can get in. The cloud also presents a good chance for Internet of Things to flourish but security is always an issue. The use of the internet via smartphones and tablets has presented accessibility of organizations' data anywhere anytime. The number of Internet of Things (IoT) devices is increasing phenomenally as we use these IoT devices daily on the network.<sup>15</sup> The Internet of Things (IoT) industry was projected in 2015 to grow to a worthiness of \$US19 trillion by 2020 globally<sup>16</sup> Figure 1 below shows an upward growth trend in the number of Internet of Things (IoT) from the year 2015 to 2025. According to SANS,<sup>17</sup> the number of Internet of Things (IoT) devices is anticipated to quintuple within a period of 10 years from 2015 to 2020.



**Fig. 1: Projection of the growth in number of IoT devices. Source: SANS<sup>17</sup>**

The growth in Big Data and Cloud Computing industries also presents great chances for the Internet of Things (IoT) industry to flourish. However, cybersecurity risk continues to be a key challenge with the advent of IoT. Hackers are likely to penetrate an organization's network through the IoT devices<sup>18</sup> or through the cloud environment which the Internet of Things (IoT) devices heavily rely on.<sup>19</sup> The cybersecurity risk of IoT devices together with

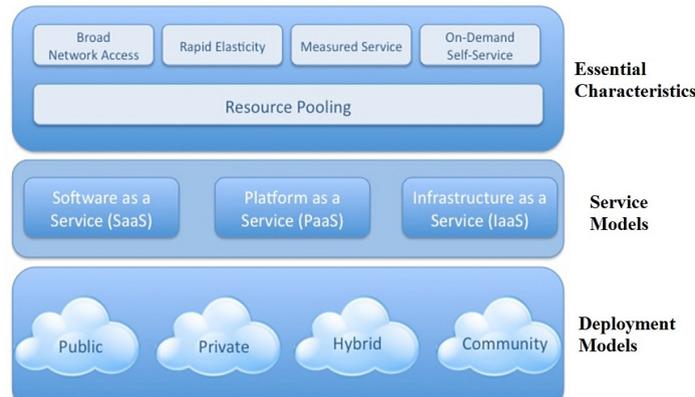
the users is high and its importance is of great significance.<sup>15</sup>

**Advances in Cloud Computing**

Cloud computing entails the provision of internet services through a hired software operating on a hired hardware provided through someone else's data center.<sup>20</sup> Cloud Computing is the provision of computing as an on-demand, pay-as-you-go

service availed in the form of virtualized distributed processing, storage, and software resources and a service. The NIST Cloud computing framework states that cloud computing is made up of five essential characteristics, three service models and

four deployment models,<sup>21</sup> as shown on Figure 2. The five (5) essential characteristics of Cloud Computing are briefly explained follows:



**Fig. 2: Cloud Computing service and deployment models**

**On-Demand Self-Service**

A consumer can unilaterally provision computing capabilities such as server time and network storage as needed automatically, without requiring human interaction with a service provider.

**Broad Network Access**

Heterogeneous client platforms available over the network come with numerous capabilities that enable provision of network access.

**Resource Pooling**

Computing resources are pooled together in a multi-tenant model depending on the consumer demand in a location independent manner.

**Rapid Elasticity**

This is the rapid and elastic provisioning or purchase of unlimited capabilities to quickly scale out; and rapidly released to quickly scale in.

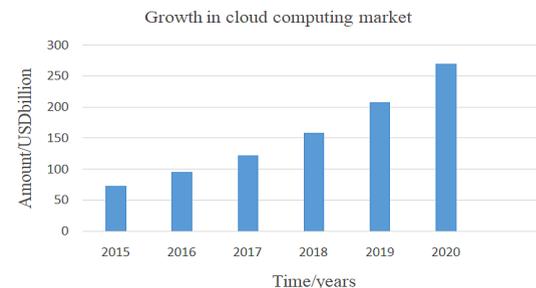
**Measured Service**

Cloud computing systems can be automatically controlled and optimized with a transparent metering capability at some level of abstraction appropriate to the type of service.

Cloud computing has many benefits for the organizations and these include cost savings, scalability, anytime anywhere access, use of latest

software versions, energy saving and quick rollout of business solutions. The general benefits of cloud computing according to Gerke<sup>22</sup> and Murugan and Rajan<sup>23</sup> include:

- free capital expenditure
- accessibility from anywhere at anytime
- no maintenance headaches
- improved control over documents as files will be centrally managed
- dynamically scalable
- device independent
- instant (Cost-efficient and Task-Centrism)
- private server cost



**Fig. 3: Projection of growth of the Cloud Computing market. Source: KPMG<sup>19</sup>**

The cloud computing market was projected by KPMG<sup>19</sup> to grow 4 times between 2015 and 2020 as depicted Figure 3 above with the associated business growth rising from US73 billion to US270 billion, respectively. The situation is exacerbated by cybercriminals who use the cloud services as warehouses to store their malicious software and as launchpads for Denial of Service (DOS) attacks.<sup>18</sup>

**National Institute of Standards and Technology (NIST) Cybersecurity Framework**

According to National Institute of Standards and Technology,<sup>24</sup> the NIST Cybersecurity framework

was developed with the sole purpose to curb cyber risk and improve security to the critical infrastructure. The NIST Cybersecurity framework is premised on Control Objectives for Information and Related Technologies (COBIT), International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). Since different organizations face different cybersecurity risks, this framework is not a one size fits all framework. The framework comprises the framework core, implementation tiers and the framework profile. The five sub-components of the NIST framework are shown below on Figure 4.



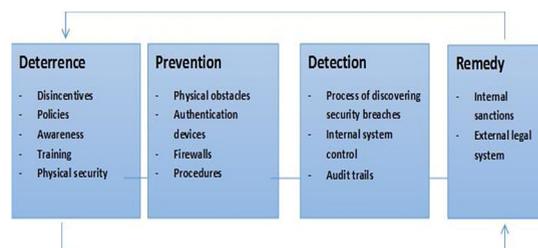
**Fig. 4: NIST Cybersecurity Framework Core components. Source:National Institute of Standards and Technology<sup>24</sup>**

The framework core comprises a set of cybersecurity activities, references and desired outcomes applicable and common across all sectors. According to Alcaraz and Zeadally,<sup>25</sup> critical infrastructure is made up of assets and systems which can be either virtual or physical that are of great importance to a nation.<sup>1</sup>

**General Deterrence Theory (Gdt)**

The General Deterrence Theory posits that the use of counter means such as strong deterrents and penalties can dissuade the occurrence of cyber-attacks and other crooked self-centered activities<sup>26</sup> In order to eliminate the threats and mitigate against cyber risks, counter measures can be adopted that include training and education, backups and disaster recovery. With deterrence activities, activities that counteract criminal abuse of cyberspace can be

embarked on.<sup>27</sup> The main components of the General Deterrence Theory are Deterrence, Prevention, Detection and Remedy as illustrated in Figure 5 below.<sup>27</sup>



**Fig. 5: Elements of the General Deterrence Theory (GDT).Source: Alanezi et al<sup>27</sup>**

The General Deterrence Theory unpacks the risk management approach to cybersecurity which provides a technical blueprint that ensures that grassroots users of cyberspace are shielded against cyber-attacks.

### Game Theory

Game theory presents multi-person decision scenarios as games where each player opts for actions that result in the best possible rewards for self. A game presents a narrative of the strategic reciprocal actions between opponents but with no specific actions taken.<sup>28</sup> The dispute between the cyber attackers and the cyber victims with regards to decision strategies is adequately handled by Game theory. In this research this theory helped in the provision of the strategic direction in the allocation of resources and the technical measures for the dynamic cybersecurity ecosystem.

### Developing countries are facing the following cybersecurity challenges:

- Infrastructure<sup>10</sup>
- Legal frameworks<sup>29</sup>
- Harmonization of legislation<sup>30</sup>
- Balancing harmonization and country specific needs<sup>31</sup>
- Systems<sup>32</sup>
- Education and awareness<sup>32</sup>
- Cybersecurity knowledge<sup>8</sup>
- Affordability and funding<sup>33</sup>
- Perceived low susceptibility to attacks<sup>34</sup>
- Lack of adequate frameworks that speak to their cybersecurity needs<sup>34</sup>
- Reporting cybercrime<sup>35</sup>
- Data sharing<sup>8</sup>

### Cryptography

Data is valuable and needs to be protected. There is need to protect data from unauthorised personal within an organisation, or from external parties with malicious intentions. Encryption or cryptography preserves electronic data in protected formats that restrict access only to the intended users. This method of protecting data is defined as follows:

*'The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can*

*decipher (or decrypt) the message into plain text. ... Cryptography is used to protect e-mail messages, credit card information, and corporate data.'*<sup>36</sup>

Cryptographic algorithms can be categorised based on their use or on the number of keys used for encryption and decryption. The three common types are the Secret Key Cryptography (SKC), Public Key Cryptography (PKC) and Hash Functions.<sup>37</sup>

### Significance of Cryptography

The central focus of cryptography in computer technology is on Authentication, Integrity and Confidentiality.

*Authentication* refers to correctly identifying a user of a system before they are granted access, Authentication is the process by which a user establishes his identity to a system or application.<sup>37</sup> Hitachi categorises authentication into three forms.<sup>38</sup>

- *Something the user knows, i.e., a secret, such as a password, PIN or the answer to a security question.*
- *Something the user has, such as a one-time password token, smart card or mobile phone.*
- *Something the user is, meaning a biometric measurement of the user -- his voice print, finger print, vein pattern scan, iris or retina scan or some behaviour, such as his typing cadence*

*Integrity*, in the context of computer systems, refers to methods of ensuring that data is real, accurate and safeguarded from unauthorized user modification<sup>39</sup>. This gives users confidence that they are dealing with authentic system developers or owners.

*Confidentiality* means that 'you can keep your information secret especially when you send sensitive data over a network'<sup>40</sup>. Cryptography addresses the quest for preserving your online transactions, personal data, or any other secret information.

### Applications of Cryptography

Cryptography is applied in many areas of computer technology including the use of cryptography in the creation of virtual money, called crypto-currency. *Crypto-currency* has a very high to keep this money secure on the various platforms. The types of crypto-

currency that exist so far are Bitcoin, EOS, Cardano (ADA), NEO, Monero (XMR), DASH, Zcash (ZEC), Ripple (XRP), Ether and Litecoin (LTC) as list by.<sup>41</sup>

Other applications for cryptography are:

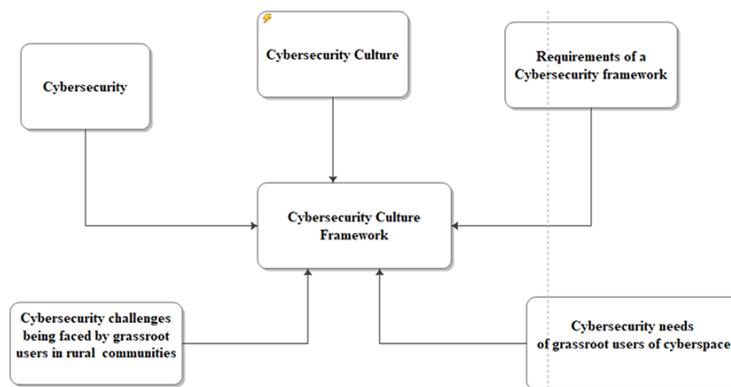
- Protecting stored files, e.g. ‘in the Encrypting File System that is integrated into Microsoft Windows, the user’s private key is decrypted by the operating system when the user logs in’.<sup>42</sup>
- Virtual private networks (VPN) are a way of creating an encrypted connection between a remote user and a site.<sup>43</sup>
- Secure web browsing is required particularly when users visit sites that facilitate financial transactions or communication that must be confidential.
- Secure messaging is a requirement for most social media platforms, such as Skype,

WhatsApp, GoogleTalk and Facebook Messenger.

- Protecting Confidentiality in Cloud or Third-Party Computing.

**Conceptual Framework**

A conceptual framework helps the researcher in the identification and crafting of his/her world view on the phenomenon under investigation<sup>44</sup> and reflects the thoughts around the entire research process.<sup>44</sup> It can be viewed as a researcher’s idea on how to explore the research problem. It is hinged on the concepts which are the key variables in a study and is specific and it narrows down to ideas that are used by the researcher.<sup>46</sup> It helps in the clarification of concepts and in the proposition of relationships among concepts in a study.<sup>47</sup> In this research, the researchers used the conceptual framework that is depicted in Figure 6 below.



**Fig. 6: Conceptual framework**

In order to come up with a cybersecurity culture framework, the researchers took into account the following factors:

- Cybersecurity
- Cybersecurity culture
- Requirements of a cybersecurity framework
- Cybersecurity challenges being faced by grassroots users of cyberspace
- Cybersecurity needs of grassroots users of cyberspace

**Research Methodology**

A *research paradigm* is way of thinking philosophically or a world view that enlightens the meaning or

interpretation of research data.<sup>48</sup> It also gives a reflection of the researcher’s opinions or beliefs about the world that s/he exists in or want to exist in. The research paradigm is a conceptual lens through which the researcher scans the methodological facets of their research to decide on the research methods that will be used and how the data will be analysed.<sup>48</sup>

*Epistemology* has a main focus on the theory of knowledge.<sup>49</sup> Epistemology helps the researcher in the establishment of the faith that s/he puts in his/her data.<sup>48</sup> Ontology as a division of philosophy deals with the assumptions that are put in place in order to believe that something is real or makes sense.

Scott and Usher<sup>50</sup> as cited by Kivunja and Kuyini<sup>48</sup> add that *an ontology* provides an understanding of the things that constitute the world as it is known. A methodology is an umbrella term used to cover research methods, research design and procedures used in a planned investigation to find out something.

*Axiology* refers to the ethical issues worthy of consideration when doing research.<sup>48</sup>

The research used the Interpretivist Paradigm, whose components are shown on Table 1 below and the justification given.

**Table 1: Interpretivist paradigm components and explanation**

<i>Paradigm component</i>	<i>Explanation</i>
Subjectivist epistemology	Researcher uses his/her own thinking and cognition to derive meaning from the research findings arrived at through interactive processes with the respondents
Relativist ontology	Multiple realities exist in the given setting Meaning is derived from the realities through interactions between the researcher and subjects as well as among participants
Naturalist methodology	Researcher makes use of data collected through text messages, interviews, conversations and reflective sessions as a participant observer
Balanced axiology	Research outcome will reflect the researcher's values, reporting research findings in a balanced manner

According to Mohajan,<sup>51</sup> *research methodology* can also be viewed as a procedural or step by step outline or framework within which research is done. In this research, a *qualitative research methodology* was used in order to fulfil the objectives of this study. The Interpretivist paradigm guided the choice of the qualitative research methodology that sought to understand the thought process of respondents in a certain context and generate new concepts or theories. This study was purposed to develop a cybersecurity culture framework to cushions grassroot users from cyber risks. The framework that this research sought to come up with had to be informed by grassroot users of cyberspace hence the contextual nature of this research demanded a qualitative methodology as underpinned by the interpretivist philosophy.

The research sought to dig deep and bring fourth the complicated cybersecurity aspects within a rural setting and a case study is the best approach. A *case study* was done for a rural community in Murewa District in Mashonaland East in Zimbabwe. Depending on the nature of the research objectives, research designs can be combined in a single study.<sup>49</sup> In this research a descriptive research design was used to answer the research questions. According

to Kothari<sup>52</sup> and Nassaji<sup>53</sup>, *descriptive designis* a study designed to describe the participants and the phenomenon to be studied in an exact way. Other data collection methods used include interviews, questionnaires and visual records.<sup>49</sup> The 'what' nature of the objectives could only be addressed through a descriptive research design which sought to find out answers as things happened in a natural setup hence the use of the descriptive research design in this research.

*Research methods* are the techniques or procedures or methods used to conduct research.<sup>49,52</sup> According to Kothari<sup>52</sup>, these research methods fall the categories that include data collection methods; statistical techniques used in the establishment of relationships between variables; and methods to evaluate accuracy of research findings. Research methods are a part of the research methodology.<sup>52</sup> Data was collected from the respondents namely through interviews, observations, questionnaires and focus groups.

In this research, unstructured interviews were done in order to ascertain the cybersecurity needs as well as the challenges that grassroot users of cyberspace face. There was great need for preparation

of questions based on the different age groups of respondents, hence the need for flexibility in wording and the way issues were clarified to them. In order to counteract weaknesses in the questionnaire, interviews were also used. Furthermore, the observation technique was used so as to achieve the following:

- double-check information provided by respondents through other means such as interviews and questionnaires and compare it with that which will be observed and note consistencies and inconsistencies
- get fresh insights or even discover new things that respondents may not wish to reveal in interviews or will not think of mentioning because they think they are not relevant
- get an understanding of the challenges and needs of the grassroots users of cyberspace as they actually use their internet devices.

*Questionnaires* were used to support interview obtained data to widen the scope of data collection. Both close ended and open ended questions were used. These questionnaires were made to be

interactive and written in clear and simple English so that respondents could understand and respond accordingly.

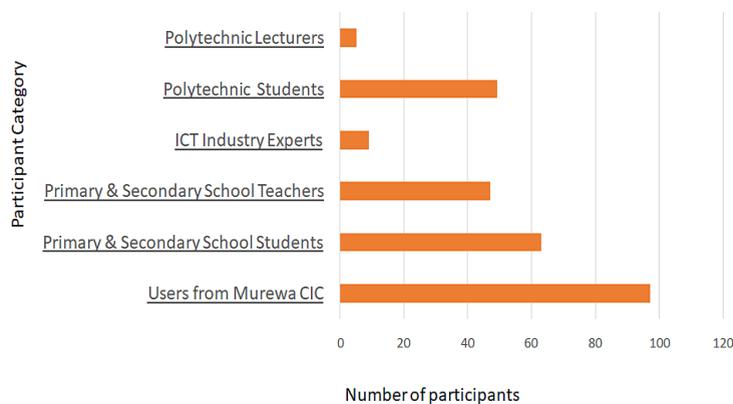
Murewa district in the Mashonaland East Province of Zimbabwe was chosen for this study. The target population comprised of teachers, pupils and parents or guardians who stay in the rural areas of Murewa. A sample size is the number of respondents from which the researcher gets the required information.<sup>54</sup> In this research, non-probability sampling techniques were used. Triangulation was used in this research in order to ensure validity and reliability of findings so as to build a complete picture from the research findings. This was achieved by analysing data collected through interviews, questionnaires and observations and themes were built.

**Results and Analysis**

A total of 270 respondents participated in this research from which a total of 31 interviews were conducted and 239 questionnaires were answered. Table 2 below shows the response rates obtained from the study.

**Table 2: Response rate from survey**

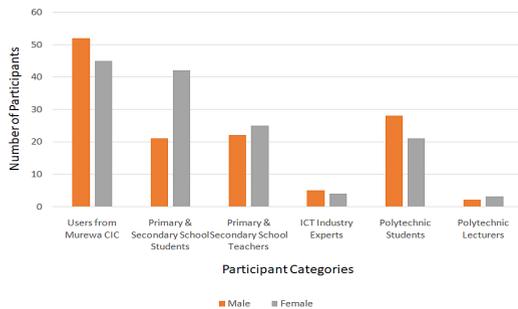
Research Instrument	Distribution	Response	Response rate
<i>Interviews</i>	45	31	68.89 %
<i>Questionnaires</i>	302	239	79.13 %
<i>Total</i>	347	270	77.81 %



**Fig. 7: Research participant categories**

The composition of respondents that took part in the research is shown on Figure 7.

A total 270 participants took part in the research. There were more female primary and secondary school student participants than males due to the fact that there is normally more female enrolments than their male counterparts. More male polytechnic students participated in the research than their female counterparts because generally more males tend to take up science related courses. The participants grouping by gender is shown on Figure 8.



**Fig. 8: Participant grouping by gender**

The findings from this research were summarised according to the themes from the research objectives.

### **Cybersecurity Challenges Being Faced By Grassroot Users of Cyberspace In Zimbabwe**

A detailed summary of the cybersecurity challenges being faced by grassroot users of cyberspace is given below:

#### **Poor and Unreliable Internet Connectivity**

Internet connectivity was found to be one of the biggest challenges being faced by respondents. It affected the surfing of the internet for purposes of doing research as well as online

#### **Identity Theft**

Respondents indicated that they had their personal and credit card details stolen through their emails by people they do not know. Some even lost huge sums of money in the process.

#### **Social Media Account Hacking**

Some respondents also indicated that they had their Facebook accounts hacked after they had clicked

some links that popped whilst they were surfing the internet.

### **Limited Cybersecurity Courses in the Education Curricula**

Some participants from the education fraternity highlighted that the Zimbabwean education system had limited or zero courses on cybersecurity at primary or secondary level and yet the persons who fall in these age groups frequently use the cyberspace and are exposed to cyber risks.

### **Difficulties in Prosecuting Cybercriminals**

Participants indicated that tracking the perpetrators of cybercrime and bringing them to book was a challenge. They felt that the police was not well equipped and knowledgeable enough to handle cybersecurity cases and victims.

### **Exposure to Pornography**

Participants also revealed that unnecessary pop ups of pornographic disturbed smooth internet surfing and lured the users into visiting more pornographic websites.

### **Limited Research on Cybersecurity**

Respondents also pointed out that research in cybersecurity is still in its infancy in Zimbabwe and to some extent this is attributed to lack of proper ICT equipment that necessitates a practical cybersecurity research approach.

### **Cybersecurity Skills Gap**

A cybersecurity skills gap in Zimbabwe was also identified as one of the biggest challenges as there is only a few people pursuing information security or cybersecurity as a course or career. Brain drain was also identified a major contributing factor to this cybersecurity skills gap.

### **Fake News**

Fake news was also highlighted as a challenge as it was causing unnecessary panic, destruction of property, marriage breakdowns as well as defamation of character amongst citizens.

### **Lack of Ministerial Role Clarity on Cybersecurity Issues**

Some respondents highlighted that in Zimbabwe, there is a lack of ministerial role clarity on cybersecurity matters.

**Poor Customer Service from Internet Service Providers**

Participants underlined the poor customer service from internet service providers in the event of service disruption.

**No Proper Policies and Regulations To Counter Cyber Threats**

Participants also indicated that there were no well-developed policies and regulations to counter cyber attacks.

**High Internet /Data Charges**

High cost of the internet or data was also a major hindrance in accessing cyberspace.

**Shortage of Ict Teachers Who Can Teach Cybersecurity**

Some school heads indicated that the biggest challenge they were facing was that of lack of skilled ICT staff who could teach Computer Studies and cybersecurity.

**Lack of Cyber Security Capacity Building for Teachers**

Some rural school teachers complained of the lack of ICT and cybersecurity capacity building initiatives such as workshops and trainings to keep them abreast with the changing technology space.

**Lack of Supporting Infrastructure**

Participants reiterated the fact that several computerization programmes had been launched in many rural schools but had not been equally matched with electrification initiatives such that the computers remained idle due to lack of electricity infrastructure.

**Limited Understanding of Ict and Cybersecurity Issues**

The researcher noted that most participants were not well conversant with issues to do with ICTs in general and cybersecurity was a big word to them.

**Cybersecurity Needs of Grassroot Users of Cyberspace in Zimbabwe**

The following is a summary of the findings on the cybersecurity needs of grassroot users of cyberspace in Zimbabwe.

**Cybersecurity Technical Measures**

Participants highlighted the need for adoption of technical measures that are implementable in the Zimbabwean environment. These range from internet and social media policies, backups, antiviruses, access controls as well as other physical and logical security measures.

**Cybersecurity Awareness**

Cybersecurity awareness programmes were identified as an important need for grassroot users of cyberspace as they promote thoroughness and cautiousness in the conduct of cyber activities in the cyberspace.

**Cybersecurity Skills Training**

Respondents indicated that cybersecurity skills gaps should be addressed in order to reduce errors that may lead to cyber breaches and compromised security.

**Cybersecurity Education**

Participants reiterated the fact that there is need for the introduction of mandatory cybersecurity courses at certificate, diploma and degree levels. As for non-graduates, the courses could be introduced at primary and secondary level.

**Cybersecurity Training for Law Enforcement Agencies**

Respondents pointed out that the Zimbabwean law enforcement agencies need to be equipped through cybersecurity training and education in order to handle cybercrime cases.

**Physical Security of Ict Equipment**

Participants from schools revealed that strong physical security of ICT equipment was required because vandalism and theft of computers and computer accessories was quite rampant in some primary and secondary schools in Murewa.

**Payment Systems**

Respondents pointed out that the Government of Zimbabwe should chip in provision of a national payment system that can guarantee availability, dependability and reliability of services of national significance at better service charges.

**Improved Payment Service Availability**

Respondents revealed the need for online and offline

transaction facilities to be made available at all times to ensure service availability even in instances where the network is down.

#### **Cybersecurity legislation**

Cybersecurity legislation needs to be instituted as a way of tackling some of the cybersecurity challenges being faced in Zimbabwe.

#### **Special Call Centre for Reporting Cybercrimes**

Some respondents pointed out the need for a dedicated cybersecurity call centre where cyber incidents could be reported and relevant assistance offered to those in need.

#### **Cybersecurity Knowledge Sharing**

Knowledge sharing particularly on issues to do with cybersecurity was also identified as a need by participants.

#### **Requirements of A Cybersecurity Culture Framework**

This section will summarise findings on the requirements of a cybersecurity culture framework

#### **Shared Cybersecurity Vision and Communication Strategy**

ICT experts reiterated the need for the crafting of a cybersecurity vision supported by an effective communication strategy as a means of aligning all the citizens to a cybersecurity strategy. The nation's leadership has to drive the vision and strategy through effective communication to every citizen and everyone should be made to understand it and make them realize their positions in the cybersecurity ecosystem.

#### **Stakeholder Engagement**

Respondents highlighted the need for stakeholder involvement in coming up with a clear cybersecurity vision and strategy that is also implementable in the Zimbabwean grassroot environment. It should be shared by every Zimbabwean and not only by a minority group of individuals and organizations. In that regard, grassroot user consultations are key in coming up with cybersecurity solutions that address their cybersecurity needs.

#### **Cybersecurity legislation**

Participants revealed that cybersecurity is central in the safety of the public, prosperity of the economy

and also the security of government. In that regard, enactment of laws that guide the reporting of cyber breaches and how the criminals will be dealt with is very important so as to effectively apply the law when a crime has been committed.

#### **Cybersecurity Education and Awareness**

Respondents indicated that empowerment through education in cybersecurity is an important ingredient in the making of a cybersecurity culture framework. This will go a long way in fostering awareness and instilling a culture of cybersecurity.

#### **Cybersecurity Research and Development**

Participants pointed out that research and development in cybersecurity should be well supported and funded by the Government of Zimbabwe so as to stimulate research in the field of cybersecurity.

#### **Cybersecurity Emergency Readiness**

Respondents revealed that emergency readiness is a key pillar in a cybersecurity framework

#### **Local and International Cooperation**

The need for local and international cooperation on cybersecurity issues was also unveiled by respondents as a key element of a cybersecurity framework.

#### **Existing Cybersecurity Frameworks In Use**

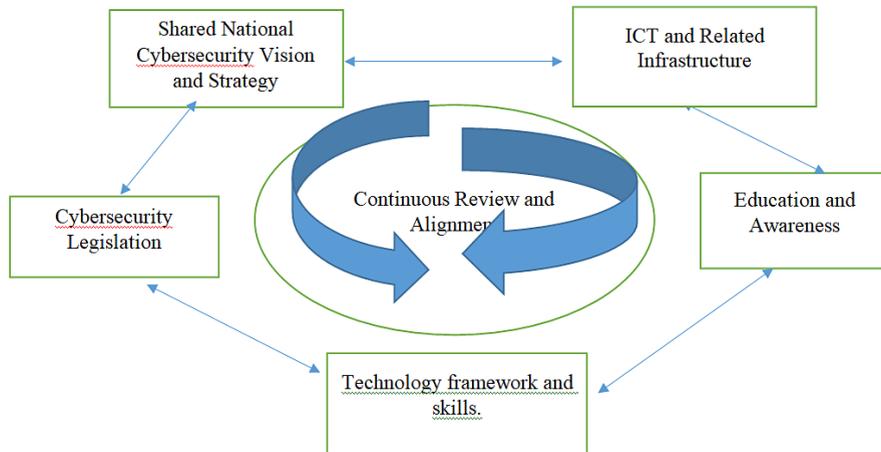
The research unveiled some of the cybersecurity frameworks that are in use across the globe. These include the following:

- NIST Cyber Security Framework
- Italian Cyber Security Framework
- International Information Systems Security Certification Consortium (ISC)2 Common Body of Knowledge (CBK)
- The International Organization for Standardization (ISO) 27032:2012
- Council on Cybersecurity Critical Security Controls
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Cybersecurity Version 5
- Health Information Trust Alliance (HITRUST) Common Security Framework (CSF)

**Proposed Cybersecurity Culture Framework for Grassroot Users of Cyberspace in Zimbabwe**

A cybersecurity culture framework for grassroot users of cyberspace was then crafted based on the research findings as shown in Figure 9 below. It is made up of five pillars which are:

- Shared National Cybersecurity Vision and Strategy
- ICTs and Related Infrastructure
- Cybersecurity Legislation
- Education and Awareness
- Technology framework and skills



**Fig. 9: Proposed cybersecurity culture framework.**

These pillars should be subjected to a process of continuous review and alignment in line with the changing technology and cyber threat landscape.

be flexible and giving room for continuous review and alignment in line with the prevailing technology and cyber threat landscape.

**Shared National Cybersecurity Vision and Strategy**

Zimbabwe has to have a cybersecurity vision and strategy that should also cascade to the grassroot users of cyberspace. The national cybersecurity strategy should set clear, top- bottom direction to institute and develop cybersecurity for the government, organizations, and citizens at large.

**Education and Awareness**

The grassroot users of cyberspace have to be educated and made aware of cyberspace, cyber risk and cybersecurity. This education should be introduced in early stages of schooling such as at primary school level so that the culture of cybersecurity can be inculcated earlier.

**Ict and Related Infrastructure**

ICT and Related Infrastructure such as base stations and electricity are very important as they help to shape the communication landscape that facilitates access to cyberspace. Without provision of infrastructure, it is difficult to cultivate a culture of cybersecurity due to limited access to information and rollout of education and awareness programmes.

**Technology Framework and Skills**

Technology skills to administer cybersecurity technologies and impart cybersecurity skills are extremely important. Cybersecurity controls, products and systems should be put in place to also help in the cushioning of the people against cyber-attacks. Cyber emergency readiness and prevention should be enacted through the setting up of CERTs at government and sectorial levels.

**Cybersecurity Legislation**

Cybersecurity laws should be enacted so as to pave way for the prosecution of cybercriminals and to prevent and deter cybercrime. These laws should

**Conclusion**

**Conclusions of the Key Findings**

The following conclusions were drawn from the research findings:

- (a) ICT supporting infrastructure such as electricity, base stations is much required to fully support all cybersecurity efforts in Zimbabwe
- (b) Rural school teachers in Zimbabwe do not have the requisite knowledge and skills in cybersecurity to pass on to the pupils.
- (c) There is limited understanding of the dangers posed by cyberspace in most rural communities in Zimbabwe.
- (d) Cybersecurity awareness campaigns being coordinated by the Ministry Of ICT, Postal and Courier Services are bearing fruit in rural communities in Zimbabwe. However, more support from the private sector players is required to sustain the momentum.
- (e) The Zimbabwean education curriculum falls short in offering cybersecurity courses that foster awareness and secure habits of using cyberspace.
- (f) The law enforcement agencies in Zimbabwe are not equipped enough to handle cybersecurity cases and victims in the communities they stay.
- (g) Cooperation between Zimbabwe and other countries regionally and internationally in the fight against cybercrime is yet to gain momentum although various memoranda of understanding have been signed.
- (h) Cooperation and synergies between the Zimbabwean Government and the private sector in tackling cybersecurity challenges that confront the citizens is slowly materialising although some incentives have to be considered by Government to bring more active players on board.
- (i) There is no clarity as to the Ministry responsible for cybersecurity in Zimbabwe as some issues are handled by Ministry of Home Affairs, some by the Ministry of Defence and some by the Ministry of ICT, Postal and Courier Services
- (j) Research in cybersecurity is still in its infant stages in Zimbabwe.
- (k) Cybersecurity Emergency readiness structures such as CERTs are yet to be set up in Zimbabwe
- (l) There is zeal and interest amongst rural learners to pursue ICT related subjects but supporting infrastructure such as electricity is a major setback

**Recommendations**

Based on the fore going conclusions, this research proffered the following recommendations:

- a) In order to address the electricity challenges being faced in rural schools which inhibit the teaching of computer studies, solar systems should be installed as an alternative source of energy.
- b) The education curricula should be revisited so that it incorporates cybersecurity courses at primary and secondary school level so that ICT adoption can be matched with cyber hygiene and responsible use of cyberspace.
- c) Government of Zimbabwe in conjunction with other players in the private sector should ensure that capacity building workshops and training in cybersecurity are conducted regularly for teachers to be aligned to current trends in technology and cybersecurity.
- d) Government of Zimbabwe should consider tax rebates for ICT and cybersecurity equipment in order to grow the industry and also stimulate research in the field of cybersecurity.
- e) Government of Zimbabwe should clarify the Ministry responsible for cybersecurity or even consider the setting up a new Cybersecurity Ministry solely responsible for cybersecurity or a special arm under the Ministry of ICT, Postal and Courier Services or the Ministry of Defence. A clear segregation of duties and responsibilities will pave way for meaningful structures and institutions to be put in place to address cybersecurity challenges and needs of citizens.
- f) Cybersecurity emergency readiness in Zimbabwe should be instituted through the setting up of CERTs at Governmental, sectorial and community levels.
- g) The cybersecurity legislation in Zimbabwe should be constantly reviewed and aligned with the changing technologies and cyber threats.
- h) The law enforcement agencies should receive relevant cybersecurity training in order for them to be able to handle cybersecurity cases and victims in the communities they stay
- i) Cooperation between Zimbabwe and other countries regionally and internationally in the

fight against cybercrime should be prioritised since cybercrimes have no geographical boundaries

### Research Contributions

This study came up with a Cybersecurity culture framework for grassroots users of cyberspace in Zimbabwe. It is the first research of its type to be carried out in the context of ICT4D in Zimbabwe. Literature review showed that in Zimbabwe, no research had attempted to come up with a cybersecurity culture framework for grassroots users of cyberspace. This study, therefore, is expected to stimulate debate on the new knowledge generated. However, the pillars presented in the framework may need to be elaborated further by more research studies.

### Areas of Future Research

The field of cybersecurity is still fairly new and as such presents a fertile ground for research particularly in developing countries like Zimbabwe. Internet adoption and usage is still growing and as such, a lot has to be done to ensure that cybersecurity issues are also taken on board. In that regard, the researcher feels that more cybersecurity frameworks can also be crafted in the following areas to cushion various users against cyber-attacks:

- Cybersecurity framework for local government particularly for urban and rural municipalities in Zimbabwe.
- Cybersecurity framework for the health services sector
- Cybersecurity framework for Small to Medium Enterprises or the informal sector in Zimbabwe.

### Integrative Conclusion

According to the International Telecommunications Union,<sup>9</sup> the creation of a cybersecurity culture is an essential approach to cybersecurity. The research was purposed to develop a cybersecurity framework that supports a cybersecurity culture to prevent cyber-attacks in Zimbabwe. The research objectives were to: a) Ascertain the cybersecurity challenges being faced in Zimbabwe b) Investigate cybersecurity needs of grassroots users of cyberspace in Zimbabwe c) Develop a cybersecurity culture framework for grassroots users of cyberspace in Zimbabwe. The researchers used the conceptual framework

to come up with a cybersecurity culture framework cognisant of Cybersecurity issues, Cybersecurity culture, Requirements of a cybersecurity framework, Cybersecurity challenges being faced by grassroots users of cyberspace, and Cybersecurity needs of grassroots users of cyberspace.

In this research, in order to come up with a cybersecurity framework for grassroots users of cyberspace in Zimbabwe, it was critical to study respondents in detail within their rural context in order to derive concepts that will be input to the framework. In this research, a qualitative research methodology was used in order to fulfil the objectives of this study. The framework that this research came up with had to be informed by grassroots users of cyberspace hence the contextual nature of the research problem demanded a qualitative methodology as underpinned by the interpretivist philosophy. A descriptive research design was used to answer the research questions and unstructured interviews were done in order to ascertain the cybersecurity needs as well as the challenges that grassroots users of cyberspace face. The observation technique was also used so as to achieve the following:

- double-check information provided by respondents through other means such as interviews and questionnaires and compare it with that which will be observed and note consistencies and inconsistencies get fresh insights or even discover new things that respondents may not wish to reveal in interviews or will not think of mentioning because they think they are not relevant.
- get an understanding of the challenges and needs of the grassroots users of cyberspace as they actually use their internet devices.

The findings from this research were summarised according to the themes from the research objectives. The key challenges to progress on Cybersecurity include limited research on cybersecurity. Respondents also pointed out that research in cybersecurity is still in its infancy in Zimbabwe and to some extent this is attributed to lack of proper ICT equipment that necessitates a practical cybersecurity research approach. There is a Cybersecurity skills gap in Zimbabwe as one of the biggest challenges as there is only a few people pursuing information

security or cybersecurity as a course or career. However, specific Cybersecurity needs of grassroots users of cyberspace in Zimbabwe were identified and these include Cybersecurity education where participants reiterated the fact that there is need for the introduction of mandatory cybersecurity courses at certificate, diploma and degree levels. Other needs include Cybersecurity legislation which needs to be instituted as a way of tackling some of the cybersecurity challenges being faced in Zimbabwe. Respondents indicated that empowerment through education in cybersecurity is an important ingredient in the making of a cybersecurity culture framework. With regards to Cybersecurity research and development, participants pointed out that research and development in cybersecurity should be well supported and funded by the Government of Zimbabwe so as to stimulate research in the field of cybersecurity. A cybersecurity culture framework for grassroots users of cyberspace was then crafted based on the research findings. Zimbabwe has to have a cybersecurity vision and strategy that should also cascade to the grassroots users of cyberspace. Furthermore, the education curricula should be revisited so that it incorporates cybersecurity courses at primary and secondary school level so

that ICT adoption can be matched with cyber hygiene and responsible use of cyberspace.

With regards to research contributions, this study came up with a Cybersecurity culture framework for grassroots users of cyberspace in Zimbabwe. Literature review showed that in Zimbabwe, no research had attempted to come up with a cybersecurity culture framework for grassroots users of cyberspace.

#### **Acknowledgement**

The authors deeply appreciate the Atlantic International University (AIU) and the Zimbabwe Open University (ZOU) for supporting this research work for Gabriel and Tinashe, respectively.

#### **Funding**

The author(s) received no financial support for the research, authorship, and/or publication of this article.

#### **Conflict of Interest**

There is no conflict of interest associated with this publication.

#### **References**

1. Kabanda G. Performance of Machine Learning and other Artificial Intelligence paradigms in Cybersecurity. *Orient.J. Comp. Sci. and Technol*; 13(1).
2. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. Cybersecurity data science: an overview from machine learning perspective, 2020. *Journal of Big Data*. <https://doi.org/10.1186/s40537-020-00318-5>
3. Berman, D.S., Buczak, A.L., Chavis, J.S., and Corbett, C.L. Survey of Deep Learning Methods for Cyber Security; 2019. doi:10.3390/info10040122
4. Bringas, P.B and Santos, I. Bayesian Networks for Network Intrusion Detection, Bayesian Network, Ahmed Rebai (Ed.), ISBN: 978-953-307-124-4; 2010. InTech, Available from: <http://www.intechopen.com/books/bayesian-network/bayesian-networks-for-network-intrusion-detection>
5. Bloice, M. and Holzinger, A. A Tutorial on Machine Learning and Data Science Tools with Python. Graz, Austria, 2018: s.n.
6. Gcaza, N., Solms, R. Von, & Vuuren, J. Van. An Ontology for a National Cybersecurity Culture Environment,. *In Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015) (1-10)*; 2015.
7. Malyuk and Miloslavska. Cybersecurity Culture as an Element of IT Professional Training; 2015
8. United Nations. Policy Brief. Tackling the challenges of cybersecurity in Africa; 2014
9. Al Hogail M. How is the ministry fostering public-private partnerships (PPPs) with local private developers?, 2015. <https://oxfordbusinessgroup.com/interview/right-home-obg-talks-majed-al-hogail-ministerhousing>.

10. International Telecommunication Union. Global Security Report; 2008.
11. Sharma R. Study of Latest Emerging Trends on Cybersecurity and its Challenges to Society, 2012. *International Journal of Scientific and Engineering Research. Vol 3 Issue 6, June 2012*
12. Wamala, F. ITU National Cybersecurity Strategy Guide. Chemistry & Geneva, Switzerland; 2011
13. Symantec .Cybercrime and cybersecurity trends in Africa; 2016
14. Ernst and Young. Cybersecurity and the Internet of Things; 2015
15. Concierge. Concierge Security Report. Cybersecurity: Trends from 2017 and Predictions for 2018, 2018
16. ACS .Cybersecurity: Opportunities, Threats and Challenges; 2016
17. SANS Cybersecurity Threat Landscape Survey; 2017
18. McAfee Labs Threats Report; 2018
19. KPMG .Clarity on Cybersecurity. Driving growth with confidence; 2018
20. Cox, R. & Wang, G. Predicting the US bank failure: A discriminant analysis. *Economic Analysis and Policy, Issue 44.2, pp. 201-211; 2014*
21. Yang, C., Yu, M., Hu, F., Jiang, Y., & Li, Y. Utilizing Cloud Computing to address big geospatial data challenges. *Computers, Environment and Urban Systems; 2017* <https://doi.org/10.1016/j.compenvurbsys.2016.10.010>
22. Gercke, M. Cybercrime Understanding Cybercrime, Understanding cybercrime: phenomena, challenges and legal response; 2012
23. Murugan, S., and Rajan, M.S. Detecting Anomaly IDS in Network using Bayesian Network, 2014. *IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p- ISSN: 2278-8727, Volume 16, Issue 1, Ver. III (Jan. 2014), PP 01-07; 2014* [www.iosrjournals.org](http://www.iosrjournals.org)
24. National Institute Of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1; 2018
25. Alkaraz C. and Zeadally S. Critical Infrastructure Protection: Requirements and Challenges for the 21st Century. *Journal of Critical Infrastructure Protection (IJCIP), volume 8, Elsevier Science, pp. 53-66, 01/2015; 2015*
26. Schuessler J.H .General Deterrence Theory: Assessing Information Systems Security Effectiveness In Large Versus Small Businesses, 2009. Accessible on: [https://digital.library.unt.edu/ark:/67531/metadc9829/m2/1/high\\_res\\_d/dissertation.pdf](https://digital.library.unt.edu/ark:/67531/metadc9829/m2/1/high_res_d/dissertation.pdf)
27. Alanezi, M.A., Kamil, A., & Basri, S. A proposed instrument dimensions for e-government service quality, 2010. *International Journal of u-and e-Service, 3(4), 1-18.*
28. Chukwudi A.E, Udoka E, Charles I. Game Theory Basics and Its Application in Cyber Security; 2017. *Advances in Wireless Communications and Networks. Vol. 3, No. 4, 2017, pp. 45-49. doi: 10.11648/j.awcn.20170304.13*
29. Norwegian Institute of International Affairs, 2018
30. Bande .Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities, 2018. *International Journal of Cyber Criminology Volume 12 Issue 1 January-June 2018*
31. ITU . Measuring the Information Society 2012; 2012
32. Schia N.N. The cyber frontier and digital pitfalls in the Global South, 2018. *Third World Quarterly, 39(5): 821-837.*
33. Muller P.L. Cybersecurity Capacity Building in Developing Countries. Opportunities and Challenges, 2015.
34. Kortjan, N. & Von Solms, R. A conceptual framework for cybersecurity awareness and education in SA, 2014. *South African Computer Journal, 52, 29-41., 2014(52), pp.29-41.*
35. The Republic of Mauritius Cybercrime Strategy 2017-2019, 2017
36. <https://www.webopedia.com/TERM/C/cryptography.html>
37. <https://www.garykessler.net/library/crypto.html>
38. <https://hitachi-id.com/resource/iam-concepts/authentication.html>);
39. <https://www.techopedia.com/definition/10284/integrity>).

40. <https://www.eukhost.com/blog/webhosting/importance-of-cryptography-in-degital-world/>
41. <https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/>
42. <https://www.nap.edu/read/25010/chapter/4#20>
43. <https://www.nap.edu/read/25010/chapter/4#22>.
44. Grant C and Osanloo A. Understanding, Selecting and Integrating a Theoretical Framework in Dissertation Research. Creating the Blueprint for House;2014 . *Administrative Issues Journal. Connecting Education, Practise and Research* .pp 12-24
45. Ravitch, S. M. & Carl, N. M. Qualitative Research: Bridging the Conceptual, Theoretical and Methodological. Los Angeles, U.S.A.: SAGE Publications, Inc;2016
46. Adom, D., Joe, A.-A., & Hussein, E. K. Theoretical and Conceptual Framework: Mandatory Ingredients of Quality Research, 2018. *International Journal of Scientific Research*, 7, 438-441.
47. Akintoye, A. Developing Theoretical and Conceptual Frameworks;2015
48. Kivunja C and Kuyini B. Understanding and Applying Research Paradigms in Educational Contexts, 2017. *International Journal of Higher Education*. Vol 6 No 5;2017
49. Walliman N. Research Methods the basics. Taylor and Francis e-Library,2011
50. Scott. D. & Usher, R. Researching education: Data, methods, and theory in educational enquiry. New York: Continuum; 2004
51. Mohajan H.K. Qualitative Research Methodology in Social Sciences and Related Subjects, 2018. *Journal of Economic Development, Environment and People*, 7(1): 23-48
52. Kothari, C. Research Methodology Methods and Techniques, 2nd Edition. New Age International Publishers; 2004
53. Nassaji H. Qualitative and descriptive research: Data type versus data analysis, 2015. *Language Teaching Research* 2015, Vol. 19(2) 129–132
54. Kumar, R. Research Methodology: A step by step guide for beginners 3rd ed. London: Sage Publishers;2011