MYKOLAS ROMERIS UNIVERSITY
FACULTY OF PUBLIC GOVERNACE AND BUSINESS

RASHEED ODEJAYI

CYBER SECURITY MANAGEMENT: THE SECURITY IMPLICATIONS OF THE DIGITAL ECONOMY ACROSS SUB-SAHARAN AFRICA COUNTRIES

Master's thesis

Thesis Supervisor:
Professor Dr. AstaValackienė

VILNIUS, 2022

MYKOLAS ROMERIS UNIVERSITY
FACULTY OF PUBLIC GOVERNANCE AND BUSINESS
INSTITUTE OF BUSINESS AND ECONOMICS

RASHEED ODEJAYI

CYBER SECURITY MANAGEMENT: THE SECURITY IMPLICATIONS OF THE DIGITAL ECONOMY ACROSS SUB-SAHARAN AFRICA COUNTRIES

Cybersecurity management Master's thesis
Study programme - KSVvAmns21-1

Thesis Supervisor:
Professor Dr. AstaValackienė

Performed by Rasheed Odejayi

VILNIUS, 2022

CONTENT

INTRODUCTION

1.0	**LITERATURE REVIEW ON THE LINK OF DIGITAL ECONOMY AND CYBER SECURITY**	**14**
1.1	**The concept of digital economy**	**14**
1.2	**Cybercrime concept**	**18**
1.3	**Different types of cybercrimes**	**20**
1.4	**Cybercrime as an economic problem**	**21**
1.4.1	**The attacker's incentives**	**22**
1.4.2	**Incentives in cybercrime**	**22**
1.4.3	**Modeling attack and defense**	**23**
1.4.4	**Cyber crime and intermediaries**	**23**
1.5	**Global cyber-threats from Africa**	**25**
1.5.1	**Key cyber threats in Africa**	**26**
1.5.2	**Increasing cyber-victimization in Africa**	**30**
1.5.3	**Situation of cybercrime in Sub-Saharan African countries: (Nigeria and Cameroon)**	**30**
1.6	**The nature of cyber security**	**32**
1.6.1	**Trends changing cyber security**	**33**
1.6.2	**Cyber security techniques**	**34**
1.6.3	**Investment in cyber security**	**35**
1.6.4	**Policies and regulations on cyber security and empirical reviews**	**35**
1.7	**Uncertain times, unsettled lives: Shaping our future in a transforming world we live in a world of worry.**	**39**
1.7.1	**Digital technologies and threats to human Security**	**40**
1.7.2	**Cyber insecurity and unintended consequences of technology**	**41**
1.7.3	**Technological innovation opens new possibilities**	**41**
1.7.4	**Technological advances are offering transformative potential**	**42**
1.7.5	**Cyber ethics**	**42**
2.0	**RESEARCH METHODOLOGY**	**44**
2.1	**Theoretical framework for research methodology construction**	**44**
2.1.1	**Protection motivation theory**	**45**
2.1.2	**Theory of planned behaviour**	**46**
2.1.3	**National security of developing countries model by Alagappa (1987)**	**46**
2.2	**Research design and methods development**	**49**
2.3	**Population and area of the study**	**49**
2.4	**Sample size and sampling technique**	**49**
2.5	**Research instrument and method of data collection**	**51**
2.6	**Other data sources**	**51**

2.7 Criteria for informants' selection 52
2.8 Method of data analysis 52
3.0 ANALYTICAL PART: EMPIRICAL ANALYSIS 53
3.1 Data analysis 53
3.2 Presentation and distribution of respondents' demographic Characteristics 54
3.3 Test of hypothesized research questions 55
3.4 Discussion of the research results 62
CONCLUSIONS AND RECOMMENDATIONS 66
REFERENCES 70
ANNEXES 79
ANNEXE No.1 INTERVIEW CHECKLIST 79
ANNEXE No 2- 5 INTERVIEW TRANSCRIPTS 84
ANNEXE No 6. ACADEMIC INTEGRITY PLEDGE 108
SUMMARY 109
ANNOTATION 110

LIST OF TABLES

Table 1: The Networked Readiness Index 2016 **17**

Table 3.2 Distribution of respondents' demographic characteristics **54**

Table 3.3: Analysis on the past and current trend of cyber crimes perpetrated in the digital economy of the selected sub-Saharan African countries **55**

Table 3.4 Analysis on the nature and types of cyber security protocols and already established laws in combating cyber crimes in the digital economy of the selected sub-Saharan African countries **56**

Table 3.5 Analysis on the perceived roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes in the digital economy of the selected sub-Saharan African countries **58**

Table 3.6 Triangulation findings of the semi-structured experts interview content analysis **60**

LIST OF FIGURES

Figure 1: Bogus Invoice Scheme **27**

Figure 2: CEO Fraud **28**

Figure 3: Account Compromise **28**

Figure 4: Three Stages to Building a Botnet **29**

Figure 5: Protection motivation theory (Source: Branley-Bell et al, 2021) **45**

Figure 6: Theory of Planned Behaviour (Source: Branley-Bell et al, 2021) **46**

Figure 7: The National Security of Developing States: A Framework of Analysis **47**

KEY TERMS/DEFINITION OF OPERATIONAL TERMS

Cyber: refers to the characteristics of the culture of computers, Information technology (IT) and virtual reality. It includes electronics, digital, internet, web, communication networks, online services etc.

Cyber Crime: Cybercrime is a term used to describe criminal activities that are committed using the internet or other forms of digital communication technology.

Cyber Security: are established cyber protocols and/or laws that guide against illegal activity that uses a computer for the storage of evidence.

Digital Economy: The digital economy refers to the economic system that relies on the use of digital technologies, such as the internet, mobile devices, and social media, to facilitate economic activity. It includes the production, distribution, and consumption of goods and services that are bought and sold online. It is a convergence of communications, computing, and information.

ICT: is the infrastructure and components that enable modern computing.

Computer: is an electronic device which could be used as a mean of manipulating and processing of facts and data in off/online process.

INTRODUCTION

The relevance of research and background to the study- Today, man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data had being transmitted or sent to the other person safely without any leakage of information (Reddy & Reddy, 2017). Innovation is highly promoted and integrated into the structure of many societies because of its capacity to generate dual value both for costumers and organizations, they can also bring broader benefits for the society by providing the previously unavailable or highly improved products and/or processes. It can be stated, that innovation is one of the major drivers of intensive economic growth and determinants of economy‘s performance The interaction evolving between business and technology innovations leading to the internet of everything and consumerization have brought security into focus in the cyber space (UBM Tech, 2014).

However, the innovation activities are rather risky for firms, causing a market failure. In today’s digital economy, many latest technologies are constantly changing the face of the mankind and due to these emerging technologies hosts of organization and government all across the globe are becoming more venerable at safeguarding private and institutional information in a very effective way as cybercrimes are increasing day by day. In order to address responsibility issues during the innovation process more effectively, firms could apply the solutions suggested by responsible innovations and strategy of cyber security management.

Today, more than 60 percent of total commercial transactions are done online, and this has left the cyber space highly vulnerable, hence, requiring a high quality of security for transparent and best transactions. In a bid to mitigate this global menace as posed by cyber criminals, security spending has significantly increased as security has shifted from being a nonfunctional requirement to everyday business and governance requirement.

The concept of cyber security has evolved into one of the key engines driving todays and future digital economies. The concept of cyber security was developed of a basis of two line of argumentation: 1) technology development involves numerous risks on the environment and the society, 2) improvement of the innovation process on digital economy by making it more secure. The foundation of any digital economy is exclusively based on the interplay between data, business value, and management decision-making, which is today's gold and diamond. The digital economy has had a significant impact on traditional industries, including retail, media, and finance, as well as on the way we work and communicate. It has also created new opportunities for entrepreneurs and innovators to enter the market and create new products and services.

However, the digital economy also presents challenges, including issues of privacy, security, and the potential for increased income inequality. Governments and regulatory bodies are working to address these issues in order to create a fair and sustainable digital economy.

Hence, it is important to implement an adequate cyber security management policy, which would encourage the innovation activities and lead to an economic growth, as it can also promote the restructuring processes inside the economy, thus, making it more dynamic and adaptive to the global economic tendencies.

Security impact on digital economy is viewed as a social license for business to operate increasing a firm legitimacy and acceptance in society. Within this field, the privacy and security of the data/information will always be top security measures that any organization or country takes care. Consequently, cyber security is making sure your organization's data is safe from attacks from both internal and external bad actors. It can encompass a body of technologies, processes, structures, and practices used to protect networks, computers, programs, and data from unauthorized access or damage. We are presently living in a world where all the information is maintained in a digital or a cyber form.

According to Branley-Bell, Gomez, Coventry, Vila and Briggs, (2021), cyber insurance (sometimes also referred to as cyber risk or cyber liability insurance) is a form of insurance cover designed to protect and individual or business from digital threats. Although, in this digital economy.

Taking into account the fact that despite the continuous progress in the area of cyber risk management, it is impossible for current and even for the future cyber security systems to predict and to prevent all potential cyber attacks. The term "Cybercrime" is any illegal act fostered or facilitated by a computer, whether the computer is an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime' (Royal Canadian Mounted Police, 2000, in Hinduja & Schafer 2009). Cybercrimes are those crimes which are committed in the online or electronic environment (Saban, McGivern & Saykiewicz, 2002).

According to (Reddy & Reddy, 2022) cybercrime as expands to include any illegal activity that uses a computer for the storage of evidence. The Council of Europe's Cybercrime Treaty defines "Cybercrime" as offences ranging from criminal activity against data to content and copyright infringement. In general, cybercrime may be referred to as an activity that consists in using systems, computer networks in general and the Internet in particular to perpetuate crimes prohibited by law (Ekoa & Mungwe, 2018).

However, with a new decade beginning, the continent of Africa which was regarded as "backwards" has been able to get a leap into the world of ICT. This leap has not come without a heavy price. The rapid rate of diffusion of cybercrime in Africa has been a call for concern (Eric, Isaac & Chanika, 2011).This concern even gets more sickening when literature indicate that, out of the top ten countries in the world with a high level of cybercrime prevalence, Sub Sahara Africa is host to four of these countries (Nigeria, Cameroon, Ghana and South Africa). Today, the digital economy of most nations in the world is accessible through the aid of electronic through the internet. The increasing rates of cyber criminality in the society have become a strong threat to nations' e-commerce growth. Many Sub Sahara African countries reputation internationally has been affected because of the continuous rise of cybercrime (Ekoa & Mungwe, 2018).

In a bid to tackle cybercrime Cameroon Ministry of Posts and Telecommunications and the University of Bloomsburg in the US enters an agreement to trains young Cameroonians on how the country's cyberspace can be best protected. The category and nature of cybercrime in Nigeria is endless. Nigeria ranks one of the top most African country concentrations with cyber criminals, also called 'Yahoo boys's" (Adeniran 2008; Longe & Chimeke 2008; Tade & Aliyu 2011). Most of these cyber criminals include young people and university students (Adeniran 2008; Tade & Aliyu 2011).

This appreciation for the critical nature of cyber security controls and enforcements is applicable across almost every nation and industry. According to UBM Tech (2014), 83 percent of businesses surveyed plan to increase their security budgets in the next few years. Allowing external users, such as contractors and partners, to access data that they are not authorized to see can create a significant security risk for an organization. While technical measures can help prevent cybercrimes, it is also important for law enforcement to be able to investigate and prosecute them. Governments around the world are enacting strict laws to protect against the loss of sensitive information, and it is important for individuals to be educated about cyber security to protect themselves from these crimes. Thus, the fight against cyber crime needs a comprehensive and a safer approach and new applied research on cyber security management, seeking to highlight security impact on digital economy in African countries.

Statement of the problem and the level of the topic's examination- Africa has more than 500 million internet users, placing the region ahead of other regions such as North America, South America, and the Middle East (Campbell, 2019). "This volume of users relative to population equates to about 38%, which implies the number is expected to grow in the coming years, given the accelerated digitalization". The leading countries are Kenya with 83% of its population being online, Nigeria with 60% and South Africa with 56% (Campbell, 2019). Mobile banking in particular is noted to be used widely within these three countries, contributing to Africa's active role in digital financial services (Cision, 2020). Mobile devices are becoming increasingly vulnerable to malicious apps, which pose a significant future threat. While online mobile banking is in high demand, the digital divide remains a challenge, particularly in Africa as member countries strive to integrate digital infrastructure into their societies, including government, banking, business, and critical infrastructure. This transformation highlights the urgent need to ensure cyber security parameters and standards meet the demands and future needs of this community, including financial inclusion (International Finance Corporation, Digital Access, 2015).

However, the absence of these standards is pervasive in Africa. 90% of African businesses are operating without the necessary cyber security protocols in place (CGTN, 2020). Without these protocols, threat actors are able to exploit increasing vulnerabilities as they continue to invent new cyber attack vectors. This leads to significant financial loss. In 2016, cybercrime has cost the Kenyan economy about 36 million USD, the South African economy 573 million USD and the Nigerian economy 500 million USD (Fassassi, 2016). A research study from Deloitte indicated

the financial loss for financial institutions in Kenya, Rwanda, Uganda, Tanzania, and Zambia since 2011 to be more than 245 million USD.

In the past year, the COVID-19 pandemic has accelerated the cybercrime ecosystem (Symantec, 2016), with a persisting digital divide and increasing cyber security vulnerabilities across the region. This was predominantly present in South Africa and Botswana. For instance, South Africa's Life Healthcare Group, responsible for managing 66 health facilities, was hit by a serious and sustained cyber attack (Morgan, 2020).

In identifying the drastic effect of the problem caused by cyber threats in Africa, Against the backdrop, this study seeks to investigate how the cyber space can be effectively monitored, secured and protected by cyber security protocols amidst the dynamic cyber attacks on some selected sub-Saharan African digital economies and also prefers possible solutions that will help mitigate this menace as posed by cyber criminals.

Emphasizing the importance of cyber security management and preventing cybercrime in the digital economy in African countries, the **research problem** was identified and the main research question was constructed, ***what is the effect of cyber security management policy on digital economy growth and how this impact varies depending on the sub-Saharan African countries?***

Object of Research- Cyber security on digital economy across sub-Saharan African countries.

Aim and Objectives of the study- The **aim -** is to examine the security impact of cyber security management on digital economy across sub-Saharan African countries using Nigeria and Cameroon as a case study. However, other specific **objectives of the research are**:

1. To highlight the key link of understanding of the digital economy and cybersecurity management; to provide the main frameworks and to examine the past and current trend of cybercrimes perpetrated in the digital economy of the selected sub-Saharan African countries.
2. To examine the nature and types of cyber security protocols and already established laws in combating cyber crimes in the digital economy of the selected sub-Saharan African countries.
3. To evaluate the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes in the digital economy of the selected sub-Saharan African countries.

The scientific novelty of the study- This research focuses on cyber security management and it security implications on the digital economic of sub-Saharan African countries. The study among others makes an attempt to find and come up with useful facts on the past and prevailing current trend of cyber crimes perpetrated in the digital economy of the selected sub-Saharan African countries and proffers possible solutions on mitigating it causes and effects on the sustainability of digital economic of sub-Saharan African countries under study.

Furthermore, the findings of the study on the nature and types of cyber security protocols and already established laws in combating cyber crimes in the digital economy of the selected sub-Saharan African countries will be of immense benefits to economic stakeholders as to determine

the rate and level of effectiveness of cyber security protocols and laws so formulated in deterring future cyber crimes in the digital economy.

Also, findings of this study helps in repositioning and enforcing viable laws of cyber security agencies operating in the selected sub-Saharan African countries towards combating cyber crimes effectively in their respective digital economies. This will help create awareness for safeguarding measures. Finally, the study will create an opportunity for investments in the area of public-private partnership to foster development for more innovation of digital economy.

To support this thesis, ***three fundamental hypotheses were formulated as follows (H_1;H_2;H_3).*** *It can be stated, that the following research questions had been validated in the course of this empirical research:*

H_1. What is the past and current trend of cybercrimes perpetrated in the digital economy of .the selected sub-Saharan African countries?

H_3. What is the nature and types of cyber security protocols and already established laws in combating cybercrimes in the digital economy of the selected sub-Saharan African countries?

H_3. What are the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cybercrimes in the digital economy of the selected sub-Saharan African countries?

The testing/verification of the above-outlined hypotheses will explain the interaction of cyber security management and its impact on the digital economy in Sub-African countries.

Scope of the study/method development - A study of this kind is highly considered to be **descriptive and expository** in nature, i.e., constructed on **mixed research strategy** (quantitative and qualitative methods; primary and secondary data collection and analyzing). Hence, this study will be centered on sub-Saharan African countries using Nigeria and Cameroon as a case study. This case study is chosen for this study because among other sub-Saharan African countries, cybercrime is on the rise in Nigeria and Cameroon.

Practical implementation of the study- In a bid execute and attain the objectivity of this study the researcher identifies the relevant stakeholders who are most relevants to the subject matter of cyber security, and cybercrime, digital economy and national security. This will equip the researcher with proper guardian on how to establish adequate contact with specific agencies and ministries towards the consultation of staff or units on cyber security and its implication of digital economy. Hence, the most informed personnel will be interviewed based on the condition of anonymity and confidentiality. Moreover, personnel(s) to be consulted will be chosen based on accessibility in addition to their possession of in-depth knowledge on cybercrime and cyber security and its implication on digital economy with preference for sub-Saharan African countries.

The structure of the study- ***The Introduction presents*** the context, problem statement, aim, research questions, significance, scope and organization of the research. ***Chapter One*** examines the conceptual Framework, theoretical review on cyber security and digital economy. ***Chapter Two*** deals with research methodology, research design, target population, sampling design,

rationale for sample selection, data collection instruments, validity of the research instrument, reliability, data analysis and ethical considerations. ***Chapter Three*** presents empirical findings of the data analysis and the practical interpretation. This paper concludes with general overall ***conclusions, summarizes the analyzed findings,*** *makes relevant* ***recommendations*** and at the same time gives suggestions for further studies.

CHAPTER ONE
LITERATURE REVIEW ON THE LINK OF DIGITAL ECONOMY AND CYBER SECURITY

This chapter consists of the reviews of past literature of other scholars. The review comprises of the conceptual, empirical reviews and theoretical frameworks.

1.1 The concept of digital economy

The dynamic development and growth in the use of ICTs, including digital technologies, is a driver of change in shaping modern economies (United Nations, 2019). It is evident that the major two countries with rapid digital transformation are America and China which other coutries struggles to match the pace. These two countries are responsible for 75% of patents related to block-chain technologies, 50% of global spending on the IoT, more than 75% of the cloud computing, and 90% of the market capitalization value of the world's 70 largest digital platforms (United Nations, 2019).

The new economy shows a structural shift from the industrial economy toward a digitalized economy characterized by information, intangibles and services and a parallel change toward new work organizations and institutional forms. Many new terms have been coined for this new economy such as "knowledge-based economy," "borderless economy," "weightless economy," "networked economy," "digital economy," "the information-based economy," and "the networked economy" to name a few (Sharma et al., 2004). A digital economy is a convergence of communications, computing, and information. The new economy is basically about coordination, innovation, selection and learning (Gärdin, 2002).

Despite the concept of digital. Don Tapscott (1995) was one of the first to describe the digital economy in his book *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*, published in 1995. He listed 12 features distinguishing the digital economy from the industrial economy: knowledge, digitization, virtualization, molecularization, integration and collaboration through the Internet, exclusion of unnecessary intermediaries, convergence, innovation, prosumers, real time, globalization, and the era of threats and anxiety (Tapscott, 1995). Some definitions, especially the first ones, emphasize the use of Internet Protocol (IP) – enabled communications and networks in digital economy (Brynjolfsson and Kahin, 2002). Johansson, Karlsson and Stough (2006) highlight the role of rapid development, adaptation, and use of ICTs innovations in the transformation of the economy and all sectors towards the digital economy. Due to this evolutionary process, society has access to new products, production processes, and services.

The definition proposed by Knickrehm et al. (2016) takes a broad approach and explained "The digital economy is the share of total economic output derived from a number of broad 'digital' inputs" (Knickrehm et al., 2016). What is specific about the definition is the distinction between digitalized economy defined as broad in scope (e-Business, e-Commerce, Industry 4.0, Precision agriculture, and Algorithmic economy) and digital economy defined as narrow in scope (Digital services, Platform economy) along with Sharing and Gig Economy being borderline between them, the core of which is Digital (IT/ICT) sector (United Nations, 2019).

This distinction highlights digitalization of many economic sectors that apply digital products or are transformed by digital technologies, in which new operations or new business models have emerged. Lovelock (2018, pp.5–6) stated that "the digital economy relies on enhanced interconnectivity of networks and the interoperability of digital platforms in all sectors of the economy and society to offer convergent services", thus emphasizing not only the broad scope but also the social dimension.

According to the definition of (ILO, 2020) The digital economy refers to the economic system that has been developed as a result of the widespread adoption of computer and information technologies, which has led to the creation of new forms of economic activity, new ways of conducting business, and new types of work and employment."

Researchers and practitioners have plenty of scope to study the digital economy from the perspective of: its share in GDP, impact on the ICT availability, transparent legislation environment, tax regulations, measures, and digital policy supporting the development of infrastructure necessary for the digital economy and benefits for humanity (e.g. new ways of shopping – e-commerce, digitization of goods and services, increased access to information and products without any geographical borders), as well as social costs (Kehal and Singh, 2005; Druică, 2012). The digital economy is changing the labour market, creating demand for new skills related to ICTs and other fields, which affects employment levels in various sectors (Johansson, Karlsson and Stough, 2006).

Digitization is the conversion of analogue data and processes into a machine-readable format (OECD, 2019). Digital forms enable an increase in search speed, replication, and sharing of virtual products or their use in real time streaming at much lower costs, which may even be close to zero (Goldfarb and Tucker, 2019).

Digitization is a significant and essential component of digitalization, which is in turn the driving force of the digital economy (Nowicka, 2019). There is a consensus in the understanding of the term digitalization, although it is sometimes equated with digitization. Definitions of digitalization indicate changes in business and organization based on the application of digital technologies (Brennen and Kreiss, 2014). They also underline changes in the value creation process or organizational changes, leading to a new operating model (i.e. types of goods and services provided to customers) or a new business model. The OECD (2019, p. 18) defined digitalization as "the use of digital technologies and data as well as interconnection that results in new or changes to existing activities". The application of modern technologies results in changes to existing goods, industries, and occupations.

Digitalization affects societies and people as well, and is expected not only to improve people's lives but also to ensure cyber security and increase human well-being (Salminen and Zojer, 2020).

Digital transformation "refers to the economic and societal effects of digitization and digitalization" (OECD, 2019, p. 18). It implies a much wider and significant change of economic and social parameters, such as the development of an information society (Lovelock, 2018).

Digital transformation, along with digitization and digitalization, accelerates global societal changes and makes the digitality of society itself possible\ (Bowen and Giannini, 2014).

A dynamic development of digital technologies and the digital economy contributes to the development of digital society (Bax, 2011; Helbing, 2015). A society in which the Internet and intensified interconnections in the virtual world are central becomes more digital because digital technologies increase access to information, its storage, and dissemination (Serpa, Ferreira, and\ Sa Santos, 2020), enabling new avenues of engagement. The society becomes more digital as a result of adopting and integrating ICTs, computer, and business sciences and humanities whether at home, at work, at educational institutions, or at leisure centres (Faulkner and Lie, 2007).

Digital technologies have the potential to build a sustainable economy and society, as emphasized in the United Nations SDGs. The document stresses that access to ICTs and affordable access to the Internet is one of the goals of the global economic transformation (Pluta-Zaremba & Szelągowska, 2021). Society is one of the beneficiaries of the digital transformation. The technological development increases quality of life and contributes to human well-being, but it may also bring threats of employment levels, unequal distribution of wealth and information (Nakanishi, 2019), ethical, legal, and social challenges and increase the need for security and privacy that should be protected (Center for Research and Development Strategy: Japan Science and Technology Agency, 2016). However, failure to adapt to changes and digital transformation would be a much greater threat to economies, societies, industries, and organizations and it could even lead to digital destruction\ (Goliński, 2018).

The combination of networked computing technologies and new business models is creating entirely new markets, industries, businesses, and work practices today to form a digital economy. The new economy or digital economy is based more in the form of intangibles, information, innovation, and creativity, in expanding economic potential (Persaud, 2001) and is based on the exploitation of ideas rather than material things.

The modern industrial enterprise is largely a producer of services integrated or embedded in the product. A large part of this service production concerns the use of information in some form (Gärdin, 2002).

The new economy is a combination of services and ICT. Malone, Yates and Benjamin elaborate on the growing concern that the benefits of the digital economy are not evenly distributed within society (Bouwman, 1999). The growth and potential of digital economy depend on the trust on the internet and in cyberspace. Digital economy is estimated at 22.5% of the world economy and yet it has not been fully exploited (Mulligan, 2017).

The leader in digital economy, the US, amassed USD 5.9 trillion through digital economy, which equates 33% its Gross Domestic Product (GDP) (Mulligan, 2017). Digital investments have growth multiplier effect in national GDP, where it increases the national economic output. In US, this digital investment is expected to translate into additional 2.1% of GDP in 2020, equivalent to additional USD 421 billion (Mulligan, 2017). Nations are at the infancy of the Fourth Industrial Revolution, transitioning to new era where digital, biological and physical world merge (Al-Khouri, 2012).

In this digital revolution, opportunities and growth rest on conducive regulatory and business environment, ICT readiness on emerging technologies, and usage of ICT in societal-wide adoption and leverage (Knickrehm, Berthon & Daugherty, 2016). For a nation to thrive and prosper in this century, digital intervention is unavoidable. World Economic Forum published Networked Readiness Index (NRI) to assess and compute nations' readiness to capture and reap the benefits of emerging technologies in digital economy (Knickrehm et al, 2016). The top ten nations based on NRI are listed in Table 1.

Table 1: The Networked Readiness Index 2016

RANK	NATION / ECONOMY	INCOME LEVEL *	GROUP **
1	SINGAPORE	HI	ADV
2	FINLAND	HI-OECD	ADV
3	SWEDEN	HI-OECD	ADV
4	NORWAY	HI-OECD	ADV
5	UNITED STATES	HI-OECD	ADV
6	NETHERLANDS	HI-OECD	ADV
7	SWITZERLAND	HI-OECD	ADV
8	UNITED KINGDOM	HI-OECD	ADV
9	LUXEMBOURG	HI-OECD	ADV
10	JAPAN	HI-OECD	ADV

Source: World Economic Forum - The Global Information Technology Report 2016:
Innovating in the Digital Economy, Income Level: HI = high income economies that are not members of the OECD; HI-OECD= high income OECD Members Group: ADV= Advanced Economies

In this digital revolution, the opportunities are coupled with risks. Hyper connectivity exposes nations to cyber threats. Digital economy raises the issues of security, privacy and trust (Weill & Woerner, 2013). Nations and governments need to employ new technologies to capture the benefits and to improve cyber security to mitigate cyber risks. Cyber security is key enabler for digital-enabled economy and society. The opportunities and boom in cyberspace are coupled with risks and cyber threats. As digital economy is expanding, cybercrime is a growth industry. In 2014, global cybercrime cost more than USD 400 billion annually, the number rose to USD 450 billion in 2016 (Schwab, 2016).

Another record reported global cybercrime cost reached USD 575 billion annually (Baller, Dutta & Lanvin, 2016). For the top four largest economies (US, China, Japan and Germany), total loss

in cybercrime reached USD 200 billion (Schwab, 2016). In cybercrime, the loss not limited to actual losses due to the attack, as it involves recovery and opportunity costs. A study in Italy reported that losses in cybercrime was USD 875 million, yet the cost of recovery and opportunity lost was USD 8.5 billion (Schwab, 2016). Cybercrime also affects company reputation, goodwill and stock prices. Year 2013 is the beginning of cybercrime-driven mega data breaches, with eight mega breaches (McAfee, 2014).

A mega breach is defined as a breach of more than 10 million records (Baller, et al, 2016). In 2015, the trend of mega breaches grew to loss of 429 million identities in mega breaches and yet this number hides a bigger number that remained unreported (Baller, et al, 2016). For a nation to protect its ICT investment and enable digital economy, articulation and publication of national cyber security strategy is identified as an essential element (Hathaway, 2013). To achieve the necessary economic outcome, the NCSS need to state the strategic objectives, identify the responsible and accountable entity, develop specific, measurable, attainable, results-oriented and time-measurable (SMART) outcomes, and commit implementation plan based on available resources and support (Schwab, 2016).

According to Aslam, et al (2020, p.1), in the modern business environment, characterized by rapid technological advancements and globalization, abetted by IoT and Industry 5.0 phenomenon, innovation is indispensable for competitive advantage and economic growth. As authors notes, the business environment has become more dynamic and hypercompetitive. To deal with this scenario business models are also evolving at a considerable pace and businesses are now relying more heavily than ever on innovation for survival (Aslam, et al (2020, p.2) it means, that the technological advancement and business application of IoT are rapidly increasing and giving birth to the next industrial revolution, i.e., Industry 5.0, hence necessitating human/user-centered, technically feasible, financially viable, and marketable products that can create value for both customers and entrepreneurs.

Follow to Szelągowska and Pluta-Zaremba (2021), it is rapidly changing corporate structures, business processes, and work culture. Thus, will allow to point, that the cyber security is essential for the smooth management of these processes in the economy and business.

1.2 Cybercrime concept

Many definitions have evolved, trying to define cyber crime; Grabosky's (2001) using a metaphor describes cybercrime as a case of 'old wine in new bottles'. Thomas and Loader (2000) defines cybercrime as 'computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks'.

Across the globe, many companies have come forward claiming to have been the victims of industrial espionage- some sophisticated actor has copied vast amounts of their most precious intellectual property and trade secrets. For instance, Department of Defense Deputy Secretary William J. Lynn calls intellectual espionage "the most significant cyber threat faced by the United States" (Lynn, 2010). While copying data does not destroy its utility, exposing a firm's secrets can

cripple its future competitiveness. When this happens at a national scale, it can wreak devastation and cripple an innovation-driven economy. Yet assessing its scope is quite hard, since many companies are reluctant to disclose an attack. Actual numbers are hard to come by.

Also, a report by the U.K. government estimates that U.K. businesses lose over £16 billion (Detica, 2011), greater than 1 percent of the value of the entire British economy in 2010. On the other hand, the report is "based on assumptions and informed judgments rather than specific examples of cyber crime, or from data of a classified or commercially-sensitive origin," so it is hard to determine how valid these numbers are.

In general, companies have demonstrated great reluctance to come forward and disclose details of espionage, or even acknowledge it occurred. It is also hard to assess the scale of cybercrime. The Chief Security Officer of AT&T testified that cybercrime yielded $1 trillion in revenue. This would put cybercrime on course to be close to 2 percent of the global economy, larger than the entire pharmaceutical industry. A common vector of extracting value is credit card fraud. Here, again, there is a conflict in the numbers. One estimate puts card fraud at $8.6 billion (Aite Group, 2009), while another suggests $37 billion (Javelin, 2011). These two estimates point us to either a fraud rate of 0.25 percent or 1.1 percent of the $3.34 trillion in credit card transactions in 2009 (Federal Reserve System, 2011). Even these numbers mislead, given how inefficient many cyber schemes are. One researcher discovered that it takes 350 million spam emails to convert just 28 sales (Kanich, 2008).

Crime also has a limited impact, with incidence largely contained in sectors of value. Cyber crooks attack banks and bank-like services, as well as identity platforms, because "that's where the money is." No one likes crime, and policies should be set to reduce the crime rate, but no one argues that we should aim for zero crime. Fraud has become a built-in expense in most business models, particularly in open infrastructures like identity and payment. Indeed, there is a trade-off between fraud reduction and enabling transactions such as e-commerce. The original diffusion of payment cards in the U.S. is due, in part, to consumer protection laws that allowed consumers to carry and use cards without bearing much of the risk of fraud (Friedman, 2011).

"Crime as a question of public interest poses a two-fold threat. First, it imposes a direct, marginal cost on the sectors attacked. This development might be seen as the cost of doing business, similar to shop-lifting: deserving of government attention, but not a huge priority. As fraud grows, though, it might approach a tipping point. That is, if attacks on a certain digital platform or application grow too large, components of the information infrastructure could be abandoned" (Friedman, 2011). The potential critical failure of a major component of the internet ecosystem raises concerns about national security. It is difficult to determine an acceptable level of compromise in this area, and it is also unclear who bears the responsibility for addressing the problem and paying for the solution. Cybercrime is a widespread problem that undermines trust in the digital economy, but it may not be as significant a threat as attacks on critical infrastructure by foreign powers. Preparing for these threats takes time and coordination, and it may be more effective to focus on building a stronger, more resilient network over the long term rather than trying to immediately address vulnerabilitie

1.3 Different types of cybercrimes

Although there are several types of cyber crimes, however, the following cyber crimes are identified and discussed in this dissertation.

1. **Cyber harassment:** The term is normally used to refer to the use of the Internet, e-mail, or other electronic communications devices to harass another person (Black and Kenneth, 2010).
2. **Digital Piracy**. Gunter, Higgins & Gealt (2010) defined digital piracy as the act of copying digital goods that include software, documents, audio (including music and voice), and video for any reason other than to back up without explicit permission from and compensation to the copyright holder using computer technology.
3. **Hacking:** Hacking is the act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access' (Kunz & Patrick, 2004).
4. **DDoS***:* A distributed denial of service attack is a type of cyber-attack where the attacker seeks to make a website or online service unavailable to its intended users by overwhelming it with traffic from multiple sources. To do this, the attacker often creates botnets and malware that infects networks and creates "zombie" machines that can be remotely controlled and used to send a large number of requests to a server. This can cause the server to become overloaded and unable to handle the volume of requests, making it unable to provide services or resources to its intended users. In other words, DDoS attacks use malicious software and a network of infected devices to flood a server with requests, making it unable to function properly. According to Neustar survey in (2012) over 300 businesses were targeted by DDoS attacks. Mostly web based industries such as financial services, telecom services, retail, travel, IT were victimized often.
5. **Phishing** *is a term used to describe a type of cyber-attack that involves tricking people into giving out* sensitive information, such as passwords, credit card numbers, and account numbers. This is typically done by pretending to be a trustworthy organization or individual and sending messages through SMS, email, or other forms of communication. The goal of a phishing attack is to obtain valuable information that can be used for nefarious purposes, such as identity theft or financial fraud. According RSA Anti-Fraud Command Center (2017) reported the total no of fishing attacks was 59% higher than 2011 in 2012.The global losses estimated at $ 1.5 billion 2012 that was 22% higher than 2011.
6. **Social engineering**: is a technique that involves using psychological tricks to obtain critical information from individuals, such as login credentials or other sensitive information. This information is obtained through social interactions with the target, rather than through direct hacking of the system.
7. **Data breach or information loss***:* In order to quickly manipulate, analyze, and research data, it is important for an organization to store it electronically in their system. This data is often very valuable to the organization, and if it is accessed by unauthorized users, it can result in significant losses. Data can be lost due to carelessness, malicious attacks, or system malfunctions. Attackers can manipulate or sell the data, or even make it public, which can harm the organization's reputation, trust, and revenue (Hetram & Shashant, 2014). The largest

breach that was reported in December actually occurred during November, where 40 million identities were exposed (Symantec, 2013).

8. **Malware:** Malware is a general label for malicious software that spreads between computers and interferes with computer operations (Kirwan and Power, 2012). It can installed by e-mail, downloading attachment and sometime by USB or other external devices. In public sector 1 e-mail out of 72 in public sector, 163 in education, 218 in finance, 235 in marketing, 236 in accommodation industry contains a malware (Symantec, 2013).
9. **Social sites:** Through online social media many other competitive organizations attempt to decrease the reputation, brand. They post or tweets negative propagations against an organization so that it reduces the trust among the people.
10. **Spam:** Kunz and Patrick (2004) defined Spam mail as the distribution of bulk e-mail that offers recipients deals on products or services.
11. **Cyber-theft**: occurs when a criminal uses the internet to steal the personal or financial data of a victim with the intent to use that information for criminal purposes. Cyber theft can happen to anyone or any business.
12. **Financial fraud**- fraud committed with the application of computers, computer networks, information and communication systems and the Internet. Eurasian group (2014).
13. **Identity theft, credit card theft, fraudulent electronic mails (phishing):** Phishing is an act of sending an e-mail to a user falsely claiming to be an established legitimate
14. **Cyber laundering**- is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.
15. **Website cloning**: cloned website creation is one of the serious threat in Wireless network or internet. The password stealing of humans is done by the hackers mostly through internet. (Arun Anoop, 2016)
16. **Intentional damage:** The enterprise's communications networks can be harmed through zapping, the process of damaging or erasing data and information, causing problems for both the enterprise and the customer (Wienclaw, 2008).
17. **Viruses and worms** is a very major threat to normal users and companies. Viruses are computer programs that are designed to damage computers. It is named virus because it spreads from one computer to another like a biological virus. A worm is a program that spreads to other computers through networks, without the use of an infected host file.

1.4 Cybercrime as an economic problem

The economic approach to information security focuses on the incentives of the actors involved in maintaining the security of cyberspace, and whether those incentives align with a socially optimal level of security. This approach considers the systems, networks, and protocols that make up cyberspace, as well as the stakeholders and influencers who shape the security of those systems. It also examines the incentives of attackers and defenders, and the ways in which market distortions can inhibit investment and risk-reducing behavior.

1.4.1 The attacker's incentives

The creators of the internet ecosystem were not motivated by any specific gain, but today's attackers typically have a specific goal in mind, such as obtaining valuable data or causing destruction. By understanding the importance of the attacker's goal and the resources they are willing to invest in achieving it, we can develop better defense strategies.

The main goal is the disruption of systems looking from the angle of National security. National security, of course, is a high priority for any country, and there is every reason to expect a large willingness to pay for offensive capacity (Friedman, 2011).

The attacker in a case involving intellectual property is likely to have a similar budget to those in national security or espionage cases. This budget will be based on the value of the intellectual property to the attacker and may have upper limits based on the potential cost of obtaining the information through other means. The attacker's budget will include an intelligence component to allow for valuing and analyzing stolen data and targeting specific systems. The attacker must have a high level of knowledge and expertise in order to carry out the attack successfully and avoid detection

1.4.2 Incentives in cybercrime

In one recent case, the United States Secret Service apprehended an individual found in possession of over 300,000 credit card accounts, which have been linked to some $36 million in fraud Reddy & Reddy (2021). Yet the best estimates in the criminal filing claim that "In all, the defendant personally received over $100,000 from his credit card fraud scheme" (United States vs. Hackett, 2011). While this is hardly a pittance, this is not an astronomical sum. Estimates vary on the value of credit card information on the black market, but the low end is almost always less than one dollar for a usable credit card number and expiration date, while the upper estimates seldom rise above a few tens of dollars (Moore, 2009; Symantec, 2011; Panda Security, 2011).

The low returns for those who steal credit card information is due to the large number of stolen accounts flooding the market, leading to lower prices. This creates a demand for mechanisms to extract value from the stolen accounts without being detected. As a result, a complex system has emerged to launder money through networks of handlers and mules. While laws have been passed and law enforcement has had some success in investigating and pursuing attackers, the anonymity of the internet and jurisdictional issues can hinder investigations and give attackers a sense of immunity to continue their crimes. Overall, it is unlikely that law enforcement can completely deter all crimes in this area. The international nature, and fluid nature of many online crimes make it difficult to engage in enforcement models specifically designed to deter crime, such as those described by Kleiman and Kilmer (2009).

Wang and Kim (2009) found that cyber-attacks originating from countries that have recently joined the Council of Europe Convention on Cybercrime fall between 15 percent and 25 percent. Wang and Kim (2009) found out that the reduction could be explained by direct cooperation between

signatory states, it is also possible that joining the treaty is indicative of a broader effort to take cybercrime more seriously.

1.4.3 Modeling attack and defense

Modelling of attack and defense strategies is a crucial aspect of cyber security research, and there are various approaches that can be used to analyze and optimize these strategies. Phishing gangs switched from using domains registered in Hong Kong (.hk) to domains registered in China (.cn) as the Hong Kong Authorities became more proficient in shutting them down quickly (Moore and Clayton, 2007). Similarly, Day, Palmen, and Greenstadt (2008) show that websites hosting malware shift to more lax hosting providers as enforcement incentives are brought to bear. Another approach is to use machine learning algorithms to predict and mitigate potential attacks (Xu et al., 2019). These algorithms can be trained on historical data to identify patterns and trends in attack behavior, allowing the defender to proactively defend against potential attacks. Understanding the attacker can aid in better understanding defense. Bohme and Moore (2009) begin with an assumption that the attacker will begin by trying to compromise the weakest link in the defenses, although they do not expect the defender to know which component is the weak link.
Gao et al. (2013), posit that the optimal strategy for the defender was to allocate resources evenly across all potential attack vectors, while the attacker's optimal strategy was to focus on the most vulnerable attack vector.

1.4.4 Cybercrime and intermediaries

"The cybercrime ecosystem is supported by a range of actors who make up the infrastructure of the digital economy. Many types of cybercrime can be detected to some extent, and these intermediaries have the ability to intervene. It is possible to identify points of concentration in the cybercrime network, where the pool of actors is more concentrated, less diverse and often subject to regulation. This makes these intermediaries an ideal target for policy interventions that align the interests of preventing crime with the ability to limit damage and raise the costs to the attackers.

"Criminals rely on these intermediaries to access the internet, host web servers and domain name servers, and even transfer and extract money. Different intermediaries can play a crucial role in tackling different aspects of crime. There is no one-size-fits-all approach, but interventions need to be evaluated for their feasibility for the intermediaries and their potential to cause inconvenience for the bad actors.

"Malicious activity on the web requires a web presence, which requires some form of hosting. Bad actors often seek out hosting from firms who do not respond to complaints from banks or other private companies. These hosts are resistant to legal interventions and are often located in jurisdictions that are less vulnerable to foreign law enforcement. While geographically diverse,

these hosts are somewhat economically concentrated. Taking out one host can have a significant impact on a range of malicious operations. The disconnection of a California server hosting company called McColo led to a large drop in global spam volumes (Clayton, 2009). This case also illustrates the potential to target intermediaries through their own bottlenecks. McColo was knocked off the Internet when security journalist Brian Krebs shared research about its nefarious activities with McColo's internet service providers, who decided to withdraw their services. Schachtman (2011) proposes systematizing this approach by publishing a list of the most offending hosting companies by some consensus process, drawing this to the attention of their ISPs and even threatening those ISPs with further punishment by going after their upstream providers.

"Internet Service Providers (ISPs) are the ultimate intermediary on the Internet, providing the needed connectivity to good and bad actors alike. also notes that because of their key role in enabling Internet communication, there is general aversion in the United States to relying on ISPs to police content. Additionally, from the service providers' perspective, once they start monitoring for any specific behavior, it opens the door to broader duties. However, it was argues that "some malicious behavior is not only relatively easy to detect, but it also benefits the service providers". For example, "discusses how high traffic malicious activity, such as denial of service attacks used in financially- and politically-motivated attempts to prevent public access to specific web sites and servers, poses a cost to the ISP in the form of packets it must send to other networks". It further notes that on scales large enough to disable websites, this can represent an appreciable cost.

Further studies shows how large ISPs have begun cooperating by detecting ongoing distributed denial of service attacks across different networks and blocking the involved traffic from their own subscribers. This raises the question of what an ISP should do once it has identified a subscriber as a source of malicious traffic. It was argues that the wrinkle in this question lies in the distinction between the individual customer, and the device under his control that is attached to the network. Since many attacks depend on botnets of compromised machines, it is highly unlikely that the customer is actually aware of the malicious activity. It is worthy to notes that while this makes assigning responsibility difficult, it also allows the ISP to frame subscriber intervention as a value-added security service. To test this hypothesis, Wood and Rowe (2011) surveyed consumers about several attributes of potential ISP-based security services, including imposing software defenses and quarantines following a compromise. "They find that the most respondents would pay for lots of security and little obligation was around $7.25 each month. This suggests that market demand is present, but may not be sufficient to pay for the customer support costs of retail security services. On the fraud side, financial and credit institutions serve both as a vector of fraud and a means to extract value from fraud. When a criminal seeks to open a new line of credit with a victim's identity credentials, these credentials are verified by credit agencies that also have access to the details of the credit application. This data can be scrutinized more closely to make fraud more difficult and costly to the attacker. A recent study of fraudulent credit applications showed that the impostors supplied obviously fake information, which was accepted by the credit grantors (Hoofnagle, 2010).

While closer scrutiny would raise the price of managing personal credit ratings, the responsible agencies are in an ideal position to serve as a strong line of defense.

"Financial institutions are also critical for value extraction at the other end of the fraud food chain. The spam economy, for example, is built around networks of botnets sending out diverse spam messages which drive gullible internet marks to a bevy of fake pharmacy websites run by a set of affiliate networks. The spam is hard to detect centrally, hosting can be protected, and the members of the affiliate networks work hard to hide themselves. At some point, however, the victim must pay the network through the pharmacy. For a credit card purchase, the merchant must have a merchant relationship with an acquiring bank to process the credit card information. Levchenko et al (2011) find that just 13 banks handled almost all of the 76 trial purchases they made through spam networks, with three of them handling the majority. "This hints at the ability to directly intervene at the financial level, by either pressuring the acquiring banks directly or allowing consumer credit card banks to refuse settlement of funds for suspicious purchases.

Finally, focusing on the intermediaries aligns incentives for understanding the risk of tipping points in online crime. Up to a point, crime represents a simple cost tradeoff for the organizations that bear some cost of victimization. These costs can be seen as part of doing business, or a margin of error. "However, above a certain level, these costs threaten the basic business model of the organization responsible, introducing a new class of risk: that the providers of the infrastructure will remove functionality or reduce functionality of the infrastructure. This risk of a tipping point represents a genuine public interest, but requires transparency and cooperation from the banks and other intermediaries in question.

1.5 Global cyber-threats from Africa

Cyber attacks originated from African economies have a worldwide effect. Gady (2010) has put it most strongly in his argument that Africa's "Cyber [weapon of mass destruction] WMD" potentially poses a direct threat to the world. For instance, in 2010, 80% PCs used in Africa were infected with viruses and malware (Gady, 2010). According to a report from Interpol, cybercrime is a growing problem in Africa with "sophisticated and well-organized" criminal groups operating in countries such as South Africa, Nigeria, and Morocco (Interpol, 2018). These groups often target financial institutions and individuals for cyber extortion, phishing scams, and malware attacks.

One notable example of a cybercriminal in Africa is "Mike," a Nigerian man who was arrested in 2018 for his role in a cybercrime ring that targeted U.S. businesses and individuals with phishing scams and ransomware attacks (FBI, 2018). Mike and his accomplices are believed to have stolen millions of dollars from their victims. An annual survey of CyberSource released in 2006 ranked Nigeria as the world's riskiest country for online transactions. CyberSource's 2008 similar survey showed that 76% of the North American merchants rejected orders from Nigeria and 58% did so for Ghana (Kshetri, 2013). Likewise, due to a large number of fraudulent clicks from Africa on Internet pay per click advertising, paid-search companies such as Overture have implemented

“continental cut-off” services, which reportedly disregard clicks on adverting originated from Africa (Kshetri, 2010).

1.5.1 Key cyber threats in Africa

a. Online scams

An online scam is a fraudulent scheme that is carried out using the internet. It is designed to trick people into giving away personal information, money, or other resources. Online scams can take many forms, such as phishing scams, romance scams, investment scams, and more.

According to the Federal Bureau of Investigation (FBI), "an online scam is an attempt by an individual or group to trick individuals into giving away personal or financial information for illegal purposes." The FBI goes on to say that online scams are becoming more sophisticated and difficult to detect, and that people should be cautious when providing personal information or sending money online..

According to Kaspersky (2020), phishing emails may leverage scenarios such as delivery, postal, financial and HR services, convincing victims to open malicious attachments or click on malicious links. According to a 2019 report by the Africa Cyber Security Association (ACSA), online scams in Africa often involve the use of fake websites, phishing attacks, and social media scams to trick individuals into giving out sensitive personal or financial information or paying money to fraudulent entities (ACSA, 2019).

One common method used by online scammers in Africa is the creation of fake websites that appear to be legitimate, but are actually designed to steal personal or financial information from visitors. These scams often target individuals seeking employment or business opportunities, and may require them to provide personal information or pay a fee in order to access the supposed opportunity (ACSA, 2019). Coupled with the COVID-19 pandemic and its impact on the cybercrime landscape, Africa saw a sustained increase in the volume of cyber attacks, including the 238% rise in cyber-attacks on online banking platforms in 2020 (Reva, 2020).

b. Digital extortion

“Digital extortion, also known as ransomware, is a form of cybercrime in which perpetrators use malicious software to block access to a computer system or its data until a sum of money is paid (Zetter, 2019). The ransom is typically demanded in a digital currency, such as Bitcoin, to make it more difficult for authorities to trace the transaction (Zetter, 2019). Digital extortion often involves the use of technology to gain access to someone's computer or other digital devices, and can be carried out remotely from anywhere in the world. It is a serious and growing threat that can have serious consequences for both individuals and organizations. While such claims are often mass-produced, sextortion activities have also been detected in apps, where threat actors will trick unsuspecting victims, who are usually male, to pre-record or send videos of themselves performing sex acts to what they believe are females, with the threat actors then threatening to release the footage unless the victim pays a financial sum (Trend Micro and Interpol, 2017).

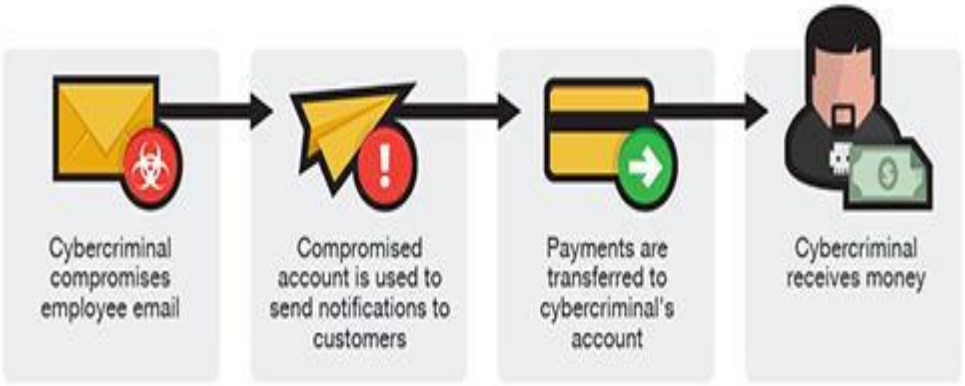
c. Business email compromise (BEC)

The FBI defines Business Email Compromise as a sophisticated email scam that targets businesses working with foreign partners that regularly perform wire transfer payments. Formerly known as the Man-in-the-Email scam. Trend Micro (2016).

"Fraudulent emails are then sent from these email accounts with an established level of trust to other employees or related individuals, asking them to transfer funds or data to a specific bank account". The three types of BEC scam are illustrated in the diagrams below, developed by Trend Micro (2017).

Bogus Invoice Scheme

The Bogus Invoice Scheme usually involves a business that has an established relationship with a supplier. The fraudster asks for invoice payment monies to be wired to an alternative, fraudulent account via a spoofed email, telephone, or fax message.



.

Figure 1: Bogus Invoice Scheme (developed by Trend Micro, 2017)

CEO Fraud

In CEO Fraud, the fraudsters identify themselves as high-level executives (CFO, CEO, CTO, etc.), lawyers, or other types of legal representative, and purport to be handling confidential or time-sensitive matters and initiate a wire transfer to an account they control. In some cases, the fraudulent request for wire transfer is sent directly to the financial institution with instructions to urgently send funds to a bank. This scam is also known as "CEO Fraud", "Business Executive Scam", "Masquerading", and "Financial Industry Wire Fraud".

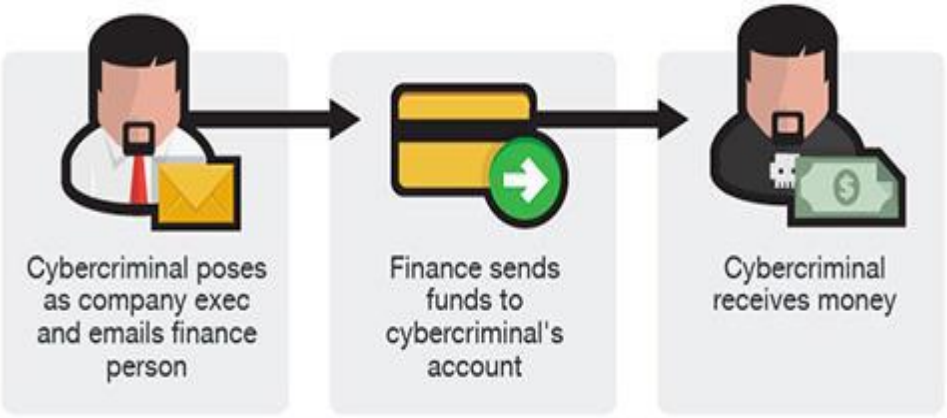


Figure 2: CEO Fraud (developed by Trend Micro, 2017)

Account Compromise

In Account Compromise cases, an employee's email account is hacked and then used to make requests for invoice payments to fraudster-controlled bank accounts. Messages are sent to multiple vendors identified from the employee's contact list. The business may not become aware of the scheme until their vendors follow up to check the status of the invoice payment.

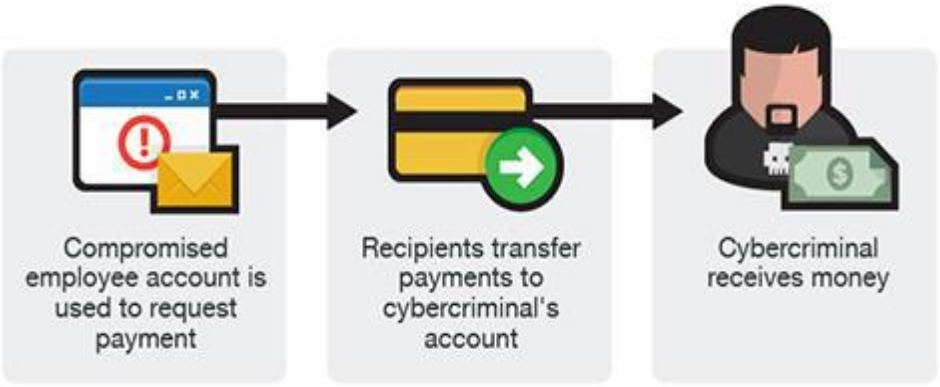


Figure 3: Account Compromise (developed by Trend Micro, 2017)

According to Trend Micro, the proportion of BEC attempts on victims in Africa from 2020 to April 2021 was less than 1% of global BEC attempts. "Based on the submission of Trend Micro findings it was argues that top BEC attempts are in English-speaking countries such as the United States, Australia and the UK. Cybercriminals typically target larger corporations because they offer the potential for larger payouts. However, there is a lower proportion of BEC (business email compromise) attempts in Africa due to the smaller concentration of large businesses and corporations there. The COVID-19 pandemic has contributed to an increase in BEC in Africa, particularly in countries like South Africa, Tunisia, Morocco, Mauritius, Nigeria, Cameroon, and Kenya. These countries have a high number of offshore companies that rely heavily on wire transfer transactions, which makes them vulnerable to BEC attempts.

d. Botnets

A Botnets is a network of compromised computers that are controlled by a single entity without the knowledge or consent of the computer's owner. These computers, known as bots, can be used to carry out malicious activities such as spamming, denial of service attacks, and other cybercrimes. Botnets are often created by hackers who exploit vulnerabilities in computer systems to gain control over the devices. According to Kaspersky (2020), there are three stages to building a botnet:

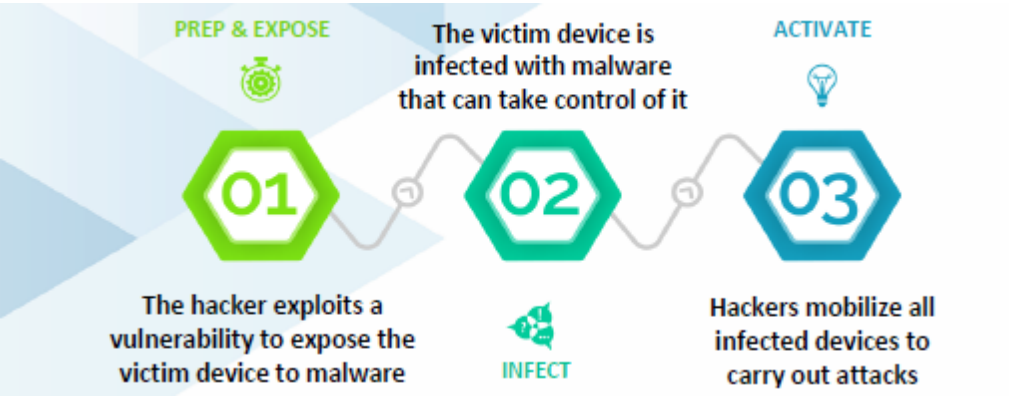


Figure 4: Three Stages to Building a Botnet (adopted by Kaspersky (2020)

Upon activation, hackers send commands and control the botnet from a main server, known as the Command & Control (C&C) server. According to Trend Micro (2017), the victims of botnets in Africa average 3,900 detections monthly, with roughly 50,000 detections in total.

e. Ransomware

Ransomware is a type of malware that encrypts a victim's data and demands a ransom payment in exchange for the decryption key.This type of cyber attack has been on the rise in recent years, with victims ranging from individual users to large businesses and government agencies. Liptak .A (2017). In 2017, a ransomware attack known as "WannaCry" infected over 200,000 computers in 150 countries (Budiness Insider, 2017). This highlights the potential impact of ransomware and the need for individuals and organizations to take appropriate measures to protect against such attacks capable of bringing governments, business and supply chains to a grinding halt, the impact of ransomware attacks also has a reputational impact on victims alongside the economic impact, with the latter evidenced in research from INTERPOL's private partner, Palo Alto Networks (2021), showing that the average ransomware payment has accelerated to more than 300,000 USD. Although the ratio of overall ransomware detections within Africa ranked in the bottom 10% compared to all other regions, research from Check Point Software Technologies (2021) reported that African organizations have seen the "highest increase in attacks, at 34%", from January to April 2021. One example is the notorious ransomware Nefilim, where it affects banking and government sectors (Allen, 2021).

1.5.2 Increasing cyber-victimization in Africa

Cyber-victimization, also known as cyberbullying, refers to the use of technology, such as the internet, social media, and mobile phones, to harass, intimidate, or otherwise harm individuals. According to Hamadoun Toure, an ex-secretary-general of the International Telecommunications Union (ITU) said "At the moment, cybercriminals see Africa as a safe haven to operate illegally with impunity". Symantec (2016) report that 24 million malware incidents that targeted, Ghana's financial institutions were reported to experience more than 400,000 incidents related to malware, 44 million related to spam emails and 280,000 related to botnets. The advent of the digital nourishment in Africa has brought about cybercrimes, although, cybersecurity is still perceive as a luxury rather than necessity which makes it seems the level of awareness is low. For instance, 86% of South Africans regularly use online banking services" Nir Kshetri (2019). This is quite huge compare to Middle East.

Cyber security budgets in many organizations are reported to be less than 1% and many organizations had a zero-budget allocated to cyber security (Kshetri, 2013).

Many financial organization in Africa are still very behind about the importance of cybersecuirty, only few of the organization have a safe and secured databases. According to a 2011

Deloitte study, only 40% of banks in Kenya, Uganda and Tanzania were prepared against cyber threats (Karambu, 2011).

Africa is faced with shortage of human capital in the area of cybersecurity. It is estimated that Africa will have a shortage of 100,000 cyber security personnel by 2020.5 Just like in the BRICS countries (Brazil, Russia, India, China, and South Africa) (Kshetri, 2015), African

According to a report African Union Commission (AUC) in November (2016) and the cyber security firm Symantec, out of the 54 countries of Africa, 30 lacked specific legal provisions to fight cybercrime and deal with electronic evidence.

Some elected high-level State officials were also reportedly involved in cybercrimes. In 2003, Nigeria's Economic and Financial Crimes Commission (EFCC) arrested Maurice Ibekwe, a member of Nigeria's House of Representatives for his alleged engagement in cybercrime-related activities (Kshetri, 2013). Cybercriminals also benefit from inter-jurisdictional and intra-jurisdictional arbitrage (Kshetri, 2019).

1.5.3 Situation of cybercrime in Sub-Saharan African countries: (Nigeria and Cameroon)

Sub-Saharan countries (Nigeria and Cameroon), fall among the list of countries worst affected by cybercrime in Africa.

A. Situation of cybercrime in Nigeria

Until 2001, the phenomenon of Internet criminal fraud was not globally associated with Nigeria. The arrival of internet in Nigeria has enabled criminals and their activities to increase the number of their unsuspecting victims and this invariably makes it difficult to track them down (Aghatise, 2006). Cybercrime is now a serious problem in Nigeria ranks third of the top ten cyber crime hot spots in the world by a 2009 Internet Crime Report (National White-Collar Crime Centre and the Federal Bureau of Investigation, 2010). Four years in a roll (2006, 2007, 2008 and 2009) Nigeria

ranks world cyber crime perpetrator countries (National White-Collar Crime Centre and the Federal Bureau of Investigation, 2010).

Emerging evidence shows that cybercrime criminals in Nigeria focus exclusively on cyber-fraud (Ojedokun & Eraye, 2012; Smith, 2008; Tade & Aliyu, 2011; Adogame, 2007; Doyon-Martin, 2015; Chawki et al., 2015b; Akpome, 2015; Ellis, 2016; Ibrahim, 2016).

According to Ellen (2009)'s survey of 113 financial services firms, mass compromise of merchant networks and card processors is viewed as the main cause of payment-card fraud.

Today, the technology is ubiquitous and increasingly easy to use, ensuring its availability to both offenders and victims (Clough, 2010). Commonly known as "Yahoo Boys", refers to the name given to every Nigeria Cyber Criminal. Even the name '419' was adopted (to refer to cyber criminals) after Section 419 of the Nigerian Criminal Code (Capp 777 of 1990) that prohibits advance fee fraud. Advanced technology within the financial institution sectors in Nigeria have generated automated Teller Machines (ATM). These machines provide innovative service delivery mode that offers diversified financial services like cash withdrawal, funds transfer, cash deposits, payment of utility and credit card bills, cheque book requests, and other financial enquiries (Muhammad, 2009).

In Nigeria today, the Presidency through the Office of the National Security Adviser (ONSA) has taken it as a course to tackle cybercrime head-on. According to the Office of the Nigerian National Security Adviser (2014), "National Cyber Security Strategy (NCSS) was created to be the nation's readiness strategy to provide cohesive measures and strategic actions towards assuring security and protection of the country's presence in cyberspace, safeguarding critical information infrastructure, building and nurturing trusted cyber-community".

Between the years 2013 and 2014, fraud on e-payment platform of the Nigerian banking sector increased by 183 per cent (2014 Annual report of the Nigeria Deposit Insurance Corporation). The estimated cost of cybercrime to Nigeria was at about 0.08 per cent of their GDP, representing about N127 billion (2014 report by the Centre for Strategic and International Studies, UK).

According to the Office of the National Security Adviser (ONSA) Nigeria, over N159 billion was lost by Nigerians through online scam and identity theft between 2000 and 2013 with 2,175 websites defaced within the same period. "Cyber espionage and stealing individuals" personal information was estimated to have affected more than 800 million people during 2013. Report revealed that 25% of the cybercrimes in Nigeria are unresolved and that 7.5% of the world's hackers are Nigerians (Information Security Society of Nigeria, 2015).

B. Situation of cybercrime in Cameroon

The advent of the internet in Cameroon has had a significant impact on the country's social and economic development. It has brought about a new era of connectivity and information sharing, enabling people to access a wealth of knowledge and resources online.

One of the major benefits of the internet in Cameroon has been the ability to connect with people around the world, facilitating communication and collaboration across borders. This has had a

positive impact on businesses, particularly those in the tech and communication sectors, as they have been able to expand their reach and access new markets. Despite the arrival and the steadily growing Internet penetration rate (which averaged 14 percent growth per year between 2007 and 2011), Cameroon remained the least connected country in the world with only 5.5% of its population online in 2013.

Even though, the internet has also played a vital role in improving education in Cameroon, as students and educators have been able to access a wide range of online resources and educational materials. This has helped to enhance the learning experience and increase access to education for many students in the country. Cameroon has faced a significant increase in cybercrime in recent years. The country has seen an increase in cyber-attacks targeting government institutions, businesses, and individuals.

One of the most common forms of cybercrime in Cameroon is cyber fraud, which includes phishing scams and online scams targeting individuals and businesses. These scams often involve the use of fake websites, emails, and social media accounts to trick people into giving away personal information or money.

Another major issue in Cameroon is the proliferation of malware, which can be used to steal sensitive information, disrupt systems, and spread malicious content. This has led to significant financial losses for businesses and individuals in the country.

The government has taken steps to address the issue of cybercrime, including the establishment of a cybercrime unit within the police force and the development of a national cyber security strategy. However, a lack of resources and trained personnel has hindered efforts to effectively tackle the problem.

Overall, the cybercrime situation in Cameroon remains a significant concern for businesses, individuals, and the government. It is important for individuals and organizations to be aware of the risks and take steps to protect themselves from cyber-attacks.

1.6 The nature of cyber security

Cybersecurity is an important concern for individuals, organizations, and governments, as the increasing reliance on technology has made it easier for hackers to gain access to sensitive information and systems. Ensuring the security and integrity of data and systems is essential to protect against cyber threats and maintain trust in the digital world. Funds are stolen, vital information are hacked, critical infrastructures are attacked and rendered incapacitated and individuals are vulnerable and at risk of being targeted withier private communication and information by the criminals (Mowbray, 2013).

“The world today survives on digital or internet communication where a large amount of information is stored and transferred. But, this practice is done at a greater risk because an unwanted target or fraudsters can access such data and used it negatively as against the ethics of the government, private organizations or a breach of personal privacy” (Mat, Darwinda, Pero, Wahid, Sule, 2019 P :215).

Cyber security is not only an issue of protecting criminals from hacking government and business information but it is also the need to protect and secure the digital environment from risks and threats of vulnerabilities which may affect government functions, private business and particularly digital economy (Meeuwisse, 2015).

Cybercrime is borderless and can be perpetrated by criminals from within, outside, terrorists, organizations and even enemy government (Meeuwisse, 2015). To mitigate these threats, organizations and individuals implement various cybersecurity measures, such as installing and regularly updating antivirus software, using strong passwords, applying security patches and updates, and educating employees about safe online practices.

It also includes the state of being protected from such threats and the broad field of endeavour including research and analysis aimed at implementing and improving those activities and quality. The major weaknesses in Cyber security consist of service disruption, theft of assets and control (Fischer, 2009).

It is viewed as a holistic set of activities that are focused on protecting an organization's vital information. Cyber security includes the technologies employed to protect information (Norwood & Catwell, 2009).

At the governmental level, it may include spy from other states, attacks on critical infrastructures, hacking vital governmental information and data and preventing normal functions of governmental assets (Rittinghouse & Hancock, 2003).

Cyber security evolves to protect the stakeholders from any form of vulnerabilities in information to both individual, organizational, and governmental. These vulnerabilities can include risks in hardware, software, people, computers, and cyberspace, as well as risks in cyber insurance. At the individual level, vulnerabilities may involve trust, ethics, communication, intelligence, courage, and limitations. At the organizational level, vulnerabilities may include human factors, security services, external technologies, wireless networks, and cloud computing. At the governmental level, vulnerabilities may include organized criminals, nation-states, critical infrastructures, and classified data. It is important to develop means of defense against these vulnerabilities. Cyber defense can occur through file protection application, PC performance applications, protection tools and email protection as well as cybercrime laws and policies (Kostopoulos, 2013).

1.6.1 Trends changing cyber security

Below are some of the trends that are having a huge impact on cyber security.

1. **Web servers:** A web server is a computer system that hosts websites and provides access to web content over the internet. Web servers are typically connected to the internet and serve up web pages in response to requests from clients (O'Reilly, 2018).
2. **Cloud computing and its services:** Cloud computing is the delivery of computing services such as storage, processing, networking, and analytics over the internet. These services are typically provided on a subscription basis and can be accessed from any device with an internet connection (Jerry Luftman, 2014).

3. **APT's and targeted attacks:** APT stands for Advanced Persistent Threat, which refers to a type of cyber-attack in which an attacker gains access to a network or system and remains there for an extended period of time, often undetected. These attacks are typically well-funded and highly organized, and the attackers may have specific goals or targets in mind. APTs are often used to steal sensitive data or disrupt operations, and they may be carried out by nation-states, criminal organizations, or other groups
4. **Mobile networks:** Mobile network has faced with major threat this days, as the usage of Mobile phone, Ipad and other gadgets increased rapidly across the globe. Hence, the need for mobile network security is paramount.
5. **IPv6: New internet protocol:** IPv6 is a new internet protocol that was developed to replace the older IPv4 protocol. IPv6 uses a 128-bit address system, which allows for a much larger number of unique IP addresses compared to the 32-bit address system used in IPv4. This allows for the continued growth and expansion of the internet, as the number of devices and users continues to increase. IPv6 also includes new features and improvements, such as improved security and support for new technologies such as mobile networks and the Internet of Things.
6. **Encryption of the code:** Encryption is the process of converting plain, unencrypted data into a coded, encrypted form that can only be accessed or decrypted by someone who has the correct key or password. This process is used to protect sensitive information and ensure that only authorized individuals can access it. Encryption is commonly used in online communication, data storage, and financial transactions to keep information secure.

1.6.2 Cyber security techniques

Cyber-attack is one of the hard task to prevent. Dion (2010) said that cyber-criminals are often difficult to identify since they committed their crimes at the very long distance from their victims. Sometimes, the country in which they live and/or have their criminal activities does not have strong criminal laws against cyber-criminality. Despite of these challenges, the following measures can be taken to account as the way of combating these cyber criminals' activities:

1. **Encryption**: Encrypting data ensures that it is only readable by those who have the proper decryption key. This can protect data from being accessed by unauthorized individuals, even if it is intercepted during transmission.
2. **Firewalls:** Firewalls are devices or software programs that block unauthorized access to a network or computer system. They can be configured to allow or block specific types of traffic, helping to prevent cyber-attacks.
3. **Two-factor authentication:** Two-factor authentication (2FA) requires users to provide two forms of identification in order to log into a system. This can include something the user knows (such as a password) and something the user has (such as a security token or phone).

4. **Virus scanning:** Virus scanners are software programs that scan a computer or network for known viruses or malware. They can help to prevent infections by alerting the user to any potential threats and allowing them to take action. Then all the traffic sent through the tunnel is encrypted (Isack & Mohammed, 2007).
5. **Network segmentation:** Network segmentation involves dividing a network into smaller, isolated segments in order to protect sensitive data. This can help to limit the impact of a cyber-attack and make it more difficult for attackers to access critical systems.
6. **Password management:** Strong passwords and password management practices are essential for protecting against cyber-attacks. This includes using unique passwords for each account, regularly updating passwords, and using a password manager to securely store them.). Password should be changed with regular interval of time and it should be alpha numeric and should be difficult to judge (Kumar, 2008).
7. **Security awareness training:** Providing security awareness training to employees can help to educate them on best practices for protecting company data and systems. This can include things like avoiding phishing scams and using secure networks when accessing sensitive data.
8. **Using open source for security:** Cybercrimes can also be prevent using of Open source software. Hoepman & Jacobs (2007) wrote that; open source enables users to evaluate the security by themselves, or to hire a party of their choice to evaluate the security for them.

1.6.3 Investment in cyber security

One of the best defensive action, is for organizations to invest in security, failure to do this might lead to negative impact on the organization in a situation of disruption by attackers. The problem of most organizations is they tends to focus on immediate attacks or threat by investing in data loss prevention rather than been proactive in preventing high risk of exposure to threat.
Grossklags, Christin, and Chuang (2008) argue that this approach can be rational and even socially optimal. They frame it as a question of self-insurance, and show that it is sometimes advantageous. Returning to the question of data loss, there is evidence that suffering a breach has a small but significant impact on a company's share price (Acquisti, Friedman, and Telang, 2006).
Rowe and Galleher (2006) neatly frame the contrasts between prophylactic investment and responsive investment as two complementary investment functions.

1.6.4 Policies and regulations on cyber security and empirical reviews

The need for policies on cyber security are important because they help ensure the confidentiality, integrity, and availability of information and systems. Without these policies and regulations, it would be difficult for individuals and organizations to protect themselves and their assets from cyber threats such as hacking, malware, and ransomware. The 2009 cyber attacks on South Korea and United States present a good case for concern in this regard (Andreason 2012). According to Pelton and Singh (2015), cyber security laws should target four major areas. protecting sensitive

information from unauthorized access, use, disclosure, disruption, modification, or destruction. This includes measures to prevent cyber-attacks, data breaches, and other security incidents, as well as efforts to educate individuals and organizations about the importance of cyber security.

A leader in this respect, the International Telecommunications Union (ITU) launched the Global Security Agenda in 2007 and formed a High-Level Expert Group to investigate the issues and develop proposals for long term strategies (Shalhoub & Al Qasimi 2010). The ITU in particular promulgates laws under its auspices that have some applicability to information warfare attacks that use the electromagnetic spectrum or international telecommunications network (Greenberg, Goodman, & Hoo 1998). On the state level, governments have adopted anti-hacking laws to help promote cyber security and attempted to approach the issue within the framework of the internationally recognized right of nation-states' rights to defend themselves when attacked, in accordance with article 51 of the UN Charter (Guiora 2017).

The Convention on Cybercrime, also known as the Budapest Convention, is a multilateral treaty of the Council of Europe that aims to harmonize national laws and improve cooperation among nations in order to effectively combat cybercrime. The Convention was adopted by the Council of Europe in 2001 and has been signed and ratified by a number of countries, including many in Europe. However, some critics argue that these laws are outdated and have failed to help effectively protect either private or government computers (Kosseff 2017). Further, as observed by Maurushat (2013), the challenges of laws related to cybercrime are many, including but not limited to the issues of freedom of expression/freedom of speech, copyright, tort of negligence, defamation, illegal telecommunications interception (surveillance), privacy law, data protection, and data breach notification.

A number of studies have investigated related topics to cyber security management and digital economy across sub-Saharan Africa countries and have come up with varying results. Some of these studies were conducted from different parts of the world including Nigeria. Branley-Bell et al (2021) conducted a study on developing and validating a behavioural model of cyber insurance adoption.

Yakubu (2017) examined cyber security issues in Nigeria and challenges. This study attempted to provide an overview of Cybercrime and Cyber-security. It defined the concept of cybercrime; identified reasons for cyber-crime and its eradication. It looked at those involved and the reasons for their involvement. Methods of stepping up cyber security and the recommendations that would help in checking the increasing rate of cyber-crimes were highlighted. The study also attempted to name some challenges of cybercrime and present practical and logical solutions to these threats.

Eric, Isaac and Chanika (2011) conducted a study on combating cyber crime in Sub-Sahara Africa. The study sought to address questions by examining three principal issues: First, it identified the various stakeholders involved in the fight against cybercrime in SSA. Second, it examined the existing laws, policies and practices employed by stakeholders to combat this malaise. Third, it discussed the impediments that these stakeholder structures and institutions face in countering cybercrime. A sound knowledge of these principal issues provided policy makers and stakeholders

with an in-depth understanding of the various structures and their existing efforts to combat cyber crime.

Ekoa and Mungwe (2018) conducted a review of Cybercrime in Sub-Saharan Africa. The authors discussed different crimes perpetrated in the society and point out the magnitude of this crimes on all the stakeholders. Also, explained that the continents is lacking the expertise and tools to combat these menace of cybercrime.

Aslam et al (2020) examined innovation in the era of IoT and industry 5.0: Absolute Innovation Management (AIM) Framework. The study proposed a new innovation management framework labeled as "Absolute Innovation Management (AIM)" to make innovation more understandable, implementable, and part of the organization's everyday routine by synergizing the innovation ecosystem, design thinking, and corporate strategy to achieve competitive advantage and economic growth. The study used an integrative literature review methodology to develop the "Absolute Innovation Management" framework. The absolute innovation management framework linked the innovation ecosystem with the corporate strategy of the firm by adopting innovation management as a strategy through design thinking. Thus, making innovation more user/human-centered that is desirable by the customer, viable for business and technically feasible, creating both entrepreneurial and customer value, and boosting corporate venturing and corporate entrepreneurship to achieve competitive advantage and economic growth while addressing the needs of IoT and Industry 5.0 era. In summary, it synergized innovation, design thinking, and strategy to make businesses future-ready for IoT and industry 5.0 revolution. The study was significant, as it not only make considerable contributions to the existing literature on innovation management by developing a new framework but also makes the concept more practical, implementable and part of an organization's everyday routine.

Mshana (2021) carried out an empirical study on cybercrime and it's Impact in the society. The aim of the research was to examine the negative impact cybercrimes pose to the society. Results from this study show that, there were many negative impacts which the society suffers from the cybercrimes and why the computer or networking are tools target for the crimes. The discussions were made from the findings and finally the paper addressed different measures which can be taken to combat these cybercrimes so that people still enjoy using the technology rather than stop them to use it.

Chooi and Ahmad (2017) sought to gain insights on the relationship between the development of the NCSS and the success of digital economy of the nation based on literature from journal articles, global reports, current industry happenings and market trends. NCSS of nine nations were analyzed centered on digital economy success. Interestingly, it was found that the readiness of nation to reap digital economy is not correlated to the development and publication of the nation's NCSS. In order for digital economy to thrive, the digital confidence of the stakeholders should be high. Nations with high digital confidence depend less on the national level NCSS to strengthen the trust and confidence in digital space. Nevertheless, the NCSS is still a need as a foundation for long term strategy to cement the cyber security of the nation, as cyber threats and risks keep evolving and will remain a challenge. A country like Singapore is intensifying its efforts and commitment

in national cyber security. The existing top ten nations in digital economy have NCSS providing the necessary foundation for digital economy to flourish further. Though a NCSS is not a requirement for nation to begin digital economy, NCSS is a requirement for a nation to continuously develop and to be successful in digital economy.

Bakri, Siti, Ratnaria and Babayo (2019) examined the impact of a secured cyberspace or the role of cyber security in promoting digital economy in Malaysia through a trusted law for customers and enterprise. The result shows that Malaysians are not vulnerable but there are still existence of threat which needs to be combacted.

Babayo, Bakri, Usman, Mohammed and Muhammad (2021) examined the implications of cybercrime and weak cyber security defense for Nigeria's national security and digital economy from the perspective of nontraditional discourse within international security debates. The study suggested that Nigeria take steps to improve its online security and digital infrastructure in order to reduce crime and enhance national security and economic growth in the digital sector.

Mario and Alen (2018) examined cyber security challenges in digital economy. In this the authors discussed about the shift from information to cyber security, mainly as the change of paradigm in protection from ongoing attacks. While in information security era it was enough to conduct basic protection from 'common' attacks, in cyber security era organizations need to implement smart, innovative and efficient controls to detect and prevent advanced and emerging cyber attacks. The authors affirmed that cyber security activities should no longer be solely the responsibility of IT departments or assigned individuals (CISOs or similar), but institution-wide efforts with all employees engaged. As digital technologies are strategically aligned with business strategy, the same should be done with cyber security. The authors conducted a preliminary research on how mature are security controls in large companies in Croatia related to important or critical national infrastructure. The authors came out to conclusion that basic protection is efficient, but there are still rooms for improvements in taking a collective ambition towards holistic cyber security governance and applying more advanced controls.

Kshetri (2013) examined cybercrime and cyber-security issues associated with China. China is linked to cybercrimes of diverse types, scales, motivations and objectives. The Chinese cyberspace thus provided an interesting setting for the study of cybercrimes. In this study, the author first develop typology, classification and characterization of cybercrimes associated with China, which helped in understanding modus operandi, structures, profiles and personal characteristics of cybercrime organizations and potential perpetrators, the signature aspects and goals of cybercrimes, the nature and backgrounds of the criminal groups involved, characteristics of potential targets for criminal activities, the nature and extent of the damage inflicted on the victims and the implications to and responses elicited from various actors. The author then examined the issue from developmental and international political economy angles. Specifically, the study delineated salient features of China's politics, culture, human capital and technological issues from the standpoint of cyber-security and analyzes emerging international relations and international trade issues associated with this phenomenon. Findings indicated that China's global ambition, the

shift in the base of regime legitimacy from Marx Leninism to economic growth, the strong state and weak civil society explain the distinctive pattern of the country's cyber-attack and cyber-security landscapes.

1.7 Uncertain times, unsettled lives: Shaping our future in a transforming world we live in a world of worry.

Covid-19 pandemic has shown a driven reversals in human development in almost every country, continues to spin off variants unpredictably. War in Ukraine and elsewhere has created more human suffering. Record-breaking temperatures, fires, storms and floods sound the alarm of planetary systems increasingly out of whack". Together, they are fuelling a cost-of-living crisis felt around the world, painting a picture of uncertain times and unsettled lives. Uncertainty is not new, but its dimensions are taking ominous new forms today. A new "uncertainty complex" is emerging, never before seen in human history. Constituting it are three volatile and interacting strands: the destabilizing planetary pressures and inequalities of the Anthropocene, the pursuit of sweeping societal transformations to ease those pressures and the widespread and intensifying polarization.

This new uncertainty complex and each new crisis it spawns are impeding human development and unsettling lives the world over. In the wake of the pandemic, and for the first time ever, the global Human Development Index (HDI) value declined—for two years straight. Many countries experienced ongoing declines on the HDI in 2021. Even before the pandemic, feelings of insecurity were on the rise nearly everywhere. Many people feel alienated from their political systems, and in another reversal, democratic backsliding has worsened. There is peril in new uncertainties, in the insecurity, polarization and demagoguery that grip many countries. But there is promise; too an opportunity to re-imagine our futures, to renew and adapt our institutions and to craft new stories about who we are and what we value. This is the hopeful path forward, the path to follow if we wish to thrive in a world in flux

1.7.1 Digital technologies and threats to human Security

"Digital technologies are increasingly central in people's lives as consumers, citizens, workers and entrepreneurs and even in their personal relationships. Digital technologies can do much to expand capabilities and promote human security. They can expand human freedoms, boost productivity and facilitate humanity's response to current challenges such as tackling Anthropocene risks and tracking pandemics". Digital technologies can also be enablers. Take mobile phones, which can enhance freedom and expand people's capabilities to communicate and acquire information, leading to, for instance, access to better health care services. Digital technologies co-evolve with values and social practices and thus have an indirect bearing on people's agency (Special Report on Human Security, 2022).

Digital technologies can also affect agency directly for example, increasing opportunities for community participation and mobilization. As digital technologies become more widely used in commerce, governance and social life, they pose new challenges for human security. Indeed,

respondents to a World Economic Forum survey cited technological risks such as digital inequality, cyber attacks, data fraud and theft, and concentrated digital power, among the most imminent threats. The security implications of digital technologies are often assessed through a national security lens (applying a human security approach re-centers the focus on implications for people (SRHS, 2022).

For instance, cyber attacks on communication networks affect not only national security but also people's access to information and freedom of association. Digital technologies can facilitate harm to people, such as bullying, harassment, fraud and misinformation. Other technology-related threats to human security can be associated with responses to the uncertainty generated by technology discussion. For instance, concentrations of control by technology providers or governments can dis-empower or abuse users. In considering how new technologies may serve as digital public goods, policymakers must go beyond technical solutions alone and also consider questions of values and ethics. For instance, over advancing equality and minimizing harm (SRHS, 2022).

1.7.2 Cyber insecurity and unintended consequences of technology

Given global interconnectivity and the large numbers of technology users, systems and network components involved, cyber attacks can generate harm through many pathways. With people relying on digital technologies more than ever during the Covid-19 pandemic, digital threats have intensified. Cyber harm is the direct or indirect result of cyber threats on individuals, organizations, communities or states by numerous bad actors, among them nation-states, terrorist groups, corporate spies, organized crime syndicates, hackers and hack activists, as well as accidental actions of authorized users. Cyber threats have varying reach and motivations that require multiple risk mitigation and control techniques. With increasing digitalization and many more stakeholders potentially affected, assessing the impact of cyber events criminal, political or developmental is complex (SRHS, 2022).

Cybercrime's damage in 2021 is estimated at about $6 trillion, up 600 percent since the beginning of the Covid-19 pandemic in 2020. More than half of breaches involve identity theft (65 percent), followed by account access (17 percent) and financial access (13 percent). With increasing digitalization and many more stakeholders potentially affected, assessing the impact of cyber events criminal, political or developmental is complex. For instance, attackers use malware programs to compromise the networks of large corporations and public institutions in supply chain attacks. An abundance of marketable material can be accessed as a by-product of the primary attack, which supports a growing market in stolen personal information. Cyber harm can be especially damaging for developing countries and regions (SRHS, 2022).

"Most digital products, services and technologies are produced or designed outside developing countries, limiting those countries' inputs into security standards. And capacity to detect cyber attacks varies widely across regions. In 2020 the global median time taken to detect attacks was 24 days (In the Americas it was 17 days, compared with 66 days in Europe, the Middle\ East and Africa and 76 days in the Asia-Pacific region. Users in many African countries are

disproportionately affected by most forms of malicious activity, including malware, cyber attacks and social media scams) Of the 50 countries with the fewest secure servers per million people in 2020, 36 were in Sub- Saharan Africa, where values ranged from 0.8 in Eritrea to 264 in Botswana. Sub- Saharan Africa's average of 799 secure servers per million people is well below the global average of 11,516. In 2017 an estimated 95 percent of African companies were unable to protect themselves from losses". Cyber attacks can generate substantial human and economic losses, especially in countries with high cyber insecurity (SRHS, 2022).

Despite campaigns such as Stop Killer Robots and the call by UN Secretary-General António Guterres to ban them, such weapons mushroom. (Some digital technologies can have unintended negative consequences. Many of the social consequences of new technologies appear only as those technologies mature. For instance, quantum computers have considerable computing power and can revolutionize whole fields that require such power. But they could also be used to crack encryption algorithms of internet sites) or to attack financial systems and institutions (for instance, compromising the security of mobile banking and e-commerce). Crypto currencies such as Bitcoin were designed to facilitate financial transactions by cutting out intermediaries and instead using a decentralized network of users to validate transactions (SRHS, 2022).

But validating crypto currency transactions requires vast computing power and uses a lot of electricity as a result. It also generates considerable e-waste by some estimates more than that of many midsize countries in 2021 Other negative social consequences have emerged thefts from exchanges, illegal drug trade and ransomware, as well as bubbles and Ponzi schemes that profit from price volatility. Country responses have been mixed. El Salvador was the worst nation to officially adopt Bitcoin as legal tender in September 2021.Some countries have explicitly banned trading or using crypto currencies; others have imposed an implicit ban. From a human security perspective, it is important to support people's freedom to use and participate in social media, while protecting them from harm (SRHS, 2022).

1.7.3 Technological innovation opens new possibilities

Technological innovation allows us to explore new ideas, solve complex problems, and create solutions that were previously unimaginable. It has the potential to improve our daily lives, make us more efficient and productive, and help us to better understand and interact with the world around us.

Through technological innovation, we can develop new technologies and applications that can improve our health and wellbeing, enhance communication and collaboration, and enable us to access and share information more easily and effectively.

Innovation in technology also has the power to drive economic growth and create new job opportunities, as well as improve the quality of life for individuals and communities around the world.

As we continue to advance and innovate in technology, the possibilities for what we can achieve are limitless. From advancing medical research to exploring new frontiers in space, technological innovation has the potential to change the world in countless ways. “Technological changes affect human capabilities in multiple ways: they not only expand people’s ability to do more things (as an enabler), but they also affect our social context and people’s agency. Innovation is more than new inventions or machines; it is about new ideas for doing things and taking advantage of existing resources to make those ideas come to fruition. In this respect innovation is linked to agency—people’s ability to act on their values, ideas and priorities. It is a broad process of transformation, where human initiative and creativity interact with social, economic and political choices” (Human Development Report, 2021-22, P: 161).

1.7.4 Technological advances are offering transformative potential

Technology is transforming various industries and applications through the use of self-driving cars, artificial intelligence, and the internet of things (IoT). The IoT allows for interconnected devices to communicate and exchange data without human intervention, improving industries such as manufacturing, agriculture, and healthcare. Robotics are also becoming more advanced and able to perform tasks in manufacturing, agriculture, and healthcare. In healthcare, technology is improving patient care and efficiency through electronic health records, telemedicine, and wearable devices. Overall, technology has the potential to improve efficiency, reduce costs, and enhance the quality of products and services in various industries. There have been major

In this context, it can be stated that by identifying the menace of cybercrime, how it affects people and how it can be eradicated. It is important to harness the existing laws, policies and practices employed by stakeholders to combat cybercrime coupled with structures and institutions in countering cybercrime.

1.7.5 Cyber ethics

Cyber ethics also involves considering the impact of technology on society and the environment, and taking action to ensure that its use is beneficial to all. It is important for individuals to practice good cyber ethics in order to create a safe and respectful online community. The below are a few of them:

- Privacy: Respect the privacy of others and protect personal information from unauthorized access or misuse.
- Security: Protect computer systems, networks, and data from unauthorized access or attacks.
- Confidentiality: Keep sensitive information, such as passwords or financial data, secure and confidential.
- Responsibility: Accept responsibility for your actions online, including any consequences that may result from them.

- Transparency: Be honest and open about your online activities, including any personal or professional relationships.
- Fairness: Do not engage in activities that are dishonest or deceptive, such as phishing or spamming.
- Respect: Treat others online with the same respect and dignity you would in person.
- Inclusivity: Respect diversity and do not discriminate against others based on their race, gender, sexual orientation, or other personal characteristics.
- Legal compliance: Follow all laws and regulations related to online activity, including copyright and intellectual property laws.
- Professionalism: Maintain a professional online presence and conduct yourself in a manner that reflects positively on your organization or profession.

In summary, this chapter has critically reviewed the concept of digital economy within the context of cybercrime and security management. It considered the different types of cybercrimes of perpetrated and the problems associated with it. Also, the chapter considered the motives initiating such attacks e.g., incentives. The chapter attempted to model the series of attacks and defense against the subject matter. It reviewed the nature behind cyber crime and it intermediaries, it global effects and menace to Africa and it sub countries. Also, the chapter considered the key cybercrime (mostly perpetrated) in Africa, it increasing cyber-victimization in Africa (e.g., those affected). Also, in a bid to drive home our discussion the situation of cybercrime in Sub-Saharan African countries such as Nigeria and Cameroon specified as case study were reviewed it terms of the types, nature and trends cyber attacks perpetrated and cyber security techniques adopted by it established and existing cyber protocols, it levels of investment in cyber security management, it policies and regulations on cyber security within the countries. In addition, the chapter also emphasized on the uncertain times, unsettled lives on how it shapes cyber ethics for the future in a transforming world we live in a world of worry as it gives credence to digital technologies and threats to human security. Finally, the chapter reviewed the tendencies of cyber insecurity and its unintended consequences of technology, its' technological innovation with new open possibilities, advances and transformative potentialities.
Thus, in the following section, the research methodology, the theoretical framework of research methodology construction and the research design were outlined.

CHAPTER TWO

METHODOLOGY OF RESEARCH

The aspect of this study focuses on the theoretical framework which helps to construct the conceptual background of the research methodology, also the methodology used in generating data for the study. It consists of research design, population of the study, sample and sampling technique, research instrument, method for data collection, other data sources, and criteria for informants' selection and method of data analysis

2.1 Theoretical framework for research methodology construction

This social phenomenon was anchored on the theory of planned behaviour (TPB), protection motivation theory (PMT) and Alagappa theory on national security of developing countries. These theories were chosen because of its permeability, comprehensiveness, and wider horizon in embracing all the elements and variables discussed in the study, such as cyber security, cyber crime, national security, digital economy, policy responses, and collective security in general.

There are three key theoretical models often applied in this field: the Theory of Planned Behaviour (TPB), Protection Motivation Theory (PMT) and General Deterrence Theory (GDT) (Lebek et al, 2014; Nasir, 2018). The Technology Acceptance Model (TAM) is also applied, but arguably not as often as the aforementioned (Nasir, 2018).

In the context of **ISP, TPB** suggests a comprehensive approach to cybersecurity that considers both technical measures and the psychological factors that influence individual behaviour. By understanding how individuals within an organization perceive the importance of information security and their ability to follow protocols, organizations can design effective strategies to protect their sensitive data and system

PMT is a psychological theory that explains how individuals respond to perceived threats. In the context of information security, this theory can be applied to understand how individuals respond to the threat of cyber-attacks and the measures they take to protect themselves and their information. Individuals go through a process when faced with a perceived threat. First, they assess the severity of the threat and the likelihood that it will occur. If the threat is perceived as severe and likely to occur, the individual will experience anxiety and fear. This anxiety and fear then leads to a motivational state where the individual seeks out ways to reduce the threat and protect themselves.

GDT suggests that individuals are less likely to engage in undesirable behavior if they believe that the consequences of doing so will be severe and that the likelihood of being caught is high. Information security protocols that are designed to deter cybercrime and data breaches should therefore include measures that make it easy to detect and trace illegal activities, as well as strict penalties for those who are caught.

TAM In the context of information security, the TAM model can be used to understand how individuals perceive and accept new security protocols. Within this field, published reviews consistently show the TPB is the most widely applied of the four models (Lebek et al, 2014; Nasir, 2018). Described by Nasir et al (2018), as "the most dominant theory" with "the most significant main constructs in predicting and explaining employees' ISP compliance behavior" (p. 740). For example, Ifinedo (2012) widely cited study demonstrates that the inclusion of PMT constructs to the TPB model can increase explained variance in ISP compliance from 0.60 to 0.70. Ifinedo (2012) suggests that "the fusion of both theoretical frameworks permits a better understanding of

the sorts of factors that affect employees' ISP behavioural compliance as opposed to when each is used alone to investigate the theme" (p. 90).
Similarly, Sommestad et al. (2014) asked whether the TPB and/or PMT are sufficient to account for cybersecurity policy compliance in employees. "They concluded that both models do a "fairly good job at prediction intentions and behaviour" but also noted that the regression model of the TPB could be improved by the addition of threat appraisal constructs from PMT.
(Sommestad et al. 2014, pp. 14-15)". For this reason, and to keep within the scope of this research, TPB and PMT were chosen as the two models to be applied. Branley-Bell, et al (2021) described these two models below, outlining their putative relationship to cyber insurance uptake and then go on to a more careful critique of the predictive power of their constituting factors.

2.1.1 Protection motivation theory

PMT was originally designed to explain engagement in protective actions in relation to health-related behaviours (Figure 5) (Nasir, 2018). However, as noted earlier, the theory has since been applied to the explanation of other protective actions, including uptake of insurance (Rogers, 1975; Dittrich et al, 2016; Beck, 1984; Grahn, 2019) and the adoption of secure online behaviours (van Bavel et al 2019; Tsai et al, 2016). PMT to cybersecurity was conducted by Kim, Song, and Kim (2014). They found that the perception of the severity of the consequences of a cyber attack (such as financial loss or identity theft) and the perceived efficacy of protective measures (such as antivirus software or cyber insurance policy) were significant predictors of an individual's intention to engage in protective behaviors. The coping appraisal refers to the individual's belief in the effectiveness of cyber insurance and their own ability to follow the necessary guidelines for obtaining a policy. It assesses their perceived self-efficacy and the perceived efficacy of the recommended protective behavior.To explain: an individual considering whether to invest in cyber insurance may firstly weigh up the likelihood that they will receive a cyber attack of a particular severity against (a) the cost of taking out cyber insurance (finances, time, effort) and (b) how effective they believe that insurance will be (response efficacy) and/or how much confidence they have in their own ability to put insurance measures into place (self-efficacy)

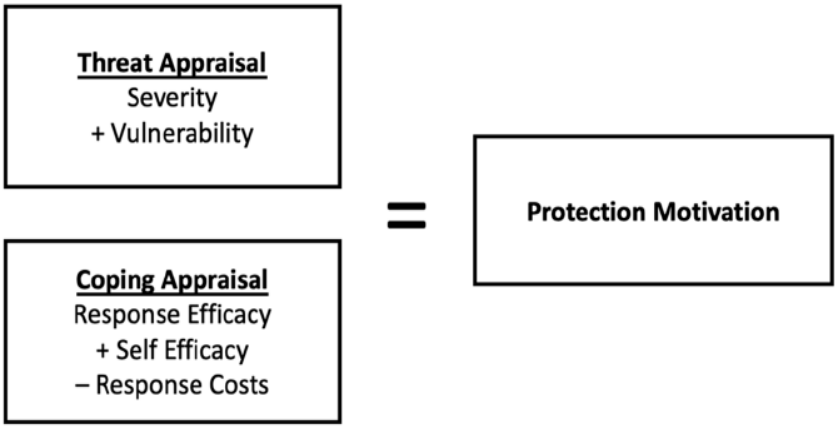


Figure 5: Protection motivation theory (Source: Branley-Bell et al, 2021)

2.1.2 Theory of planned behaviour

TPB highlights additional factors which may influence insurance purchase decisions. TPB states that intention to perform a behaviour is the most immediate and important determinator of behaviour (although perceived control has also been shown to influence behaviour directly, as represented by the dashed line in Figure 6) (Ajzen, 1985; Brahmana et al, 2019). Intention is influenced by the individual's attitude(s) towards the behaviour, subjective norm(s) and perceived control over the situation. Brahmana et al. Brahmana et al (2019) applied the TPB to explore intention to purchase health insurance. Perceived self-efficacy from PMT and perceived behavioural control from TPB are thought to measure the same construct (Ifinedo, 2012).

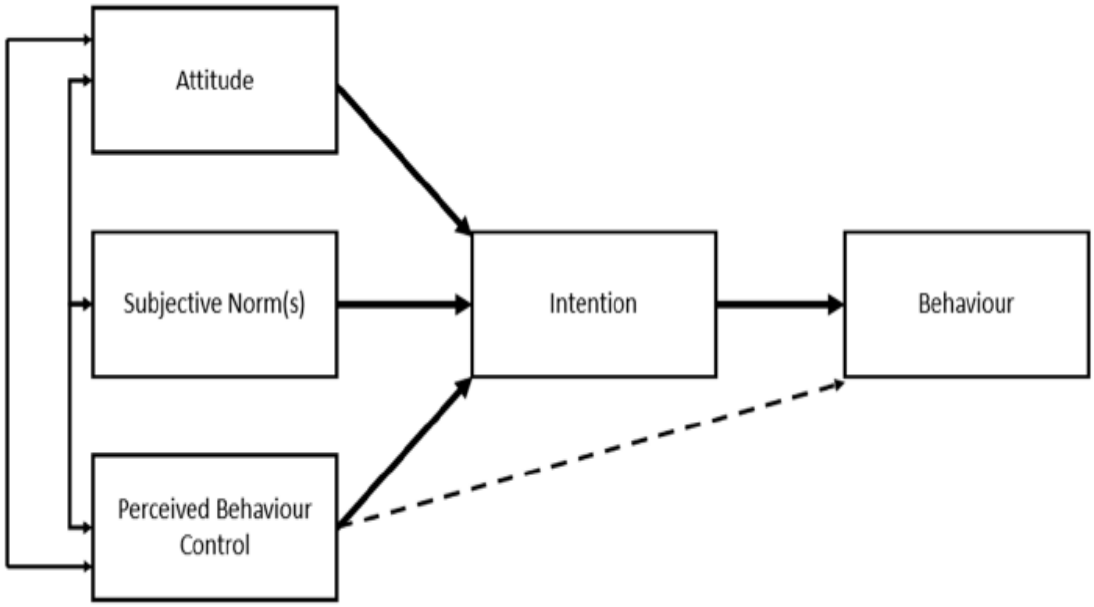


Figure 6: Theory of Planned Behaviour (Source: Branley-Bell et al, 2021)

Although widely used, these models are not without criticism. A systematic review by ENISA (2018) found that the coping elements of PMT and the TPB were useful (p. 11), but questioned the predictive value of threat models, including PMT's threat appraisal. This is curious when we consider that Sommestad et al (2014) found added predictive value in the threat component, and concluded that no single PMT variable was able to explain more than a small portion of the variance within the studied populations.. That said, other recent work has also suggested that coping elements offer greater value than threat elements when trying to predict or improve online security behaviour (van Bavel, 2014).

2.1.3 National security of developing countries model by Alagappa (1987)

This work adopts and expands the on the "National Security of Developing States" model postulated by Muthiah Alagappa (1987), presented and discussed below. This theoretical concepts chosen was based on the following reasons. This theory discusses the value and innovation of a study that presents a framework for understanding national security and vulnerabilities. The

diagram in the study provides clear illustrations to help understand the concepts involved. Previous studies have used different theories, but this study is unique and proposes new ideas. The theory also leaves room for future theory building, as it was originally developed in 1987 to identify threats to national security in developing countries. However, it also allows for exploration of threats in various areas, including political, social, economic, and environmental, which allows for further development of knowledge in the field of social sciences.

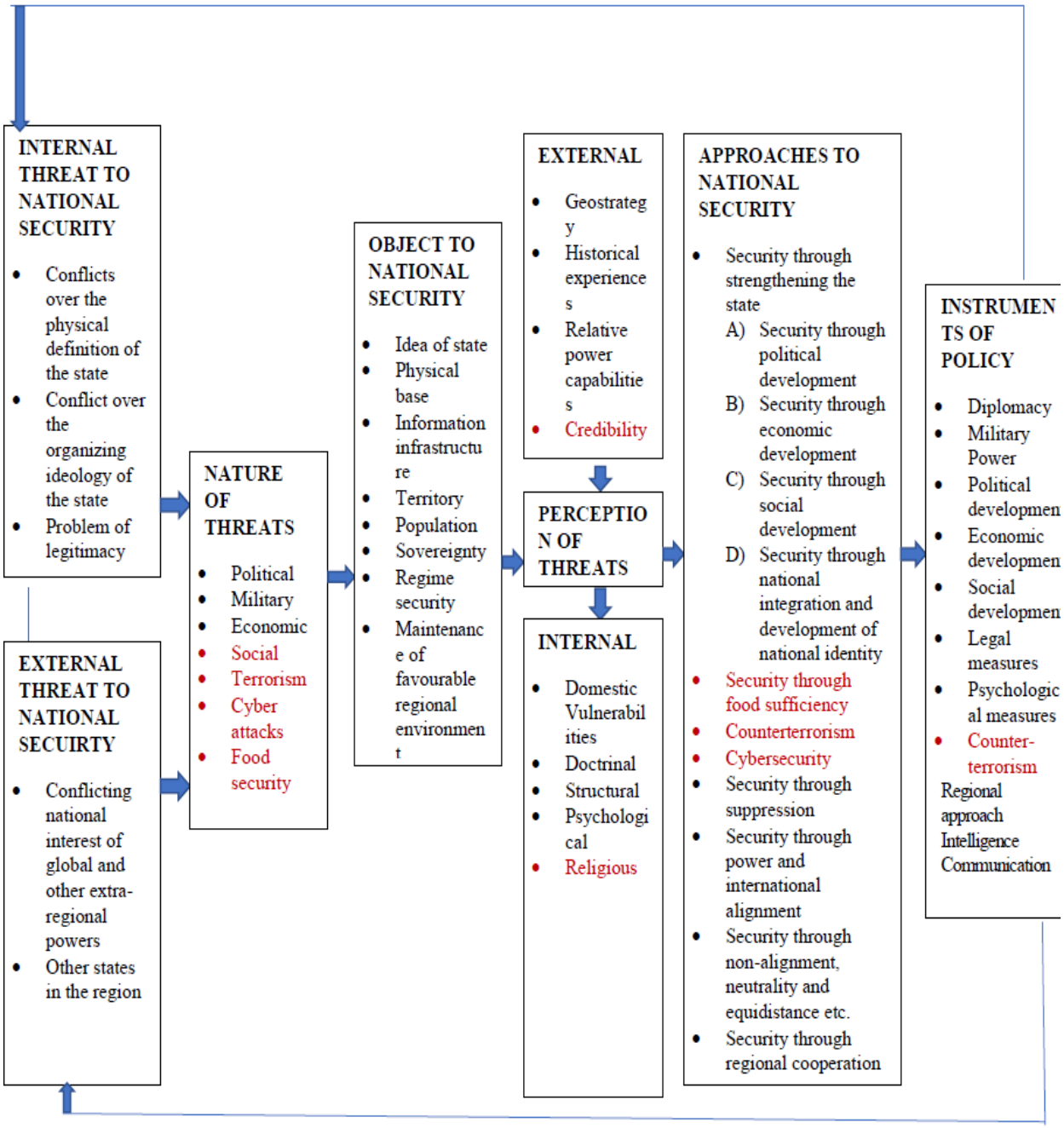


Figure 7: The National Security of Developing States: A Framework of Analysis
Source: Muthiah Alagappa (1987). Expanded by the researchers

According to Sule et al, (2021). There are two main types of threats to national security: internal and external. These threats can be traditional, such as armed groups or military conflict, or nontraditional, such as economic issues or social settings. These threats can affect developing states like Nigeria and Cameroon, and can include traditional and nontraditional threats such as terrorism, food insecurity, or cyber attacks.

Thus, as identified by Alagappa (1987), any serious developing country that seeks absolute national security must pay attention to both internal and external security and also must give consideration utmostly to both the trational and nontraditional military threats. The framework advanced by Alagappa (1987) is suitable for this study because it has the leverage of providing an all-round explanation of national security of countries like Nigeria and Cameroon, which is, accounting for both traditional and nontraditional threats. Other theoretical frameworks discussed in the above section can explain either the political angle or the economic perspective of cyber security and cybercrime.

However, Sule et al (2021) posit that theory is all-encompassing in terms of both theoretical and empirical analysis. For instance, the high numbers of mobile phone and internet users in Nigeria and Cameroon, coupled with the significant loss of billions of dollars due to cybercrime, suggests that these phenomena pose a threat to national security. The large amounts of money deposited in the Treasury Single Account and spent on salaries through the Integrated Personnel Payroll Information System in Nigeria make these systems vulnerable to cyber-attacks. This study relies heavily on empirical facts related to criminals and terrorists using cyber communication. In essence, this research agrees with the empirical findings of Sule et al (2021). which strongly support the theory's suggestion that nontraditional security threats to countries like Nigeria and Cameroon can be as strong as traditional ones. This study is inspired, certainly, by that of others. For instance, Cavelty & Wenger (2019) opined that there is a great deal of effort within the international relations discipline aimed at situating its analytical discourse toward an inclusive focus on cyber security as a part of global security concerns.

Cavelty et al. (2019) stress that cyber security is connected to political security because state actors are dealing with state and non-state actors on the international scene whenever there are threats and vulnerabilities of attacks from a perceived hostile enemy. Cavelty et al. (2019) presented three key drivers that influence cyber security politics and research in the field. They include politics (divided into domestic politics and international politics), science (consisting of academic debates and institutionalization), and technology (involving key events and development and use).

One of the areas that this research is interested in is domestic and international politics of Nigeria with regard to cyber security, and of particular relevance to us is that Cavelty et al. (2019) found it expedient to expand the rationale behind why research of this nature is undertaken from the theoretical perspective. There are other studies (Koops 2016; Aniekan & Afolabi 2017; Diogenes & Ozkaya 2018; Kremling & Parker 2018; and Kshetri 2019) similar to that of Cavelty et al. (2019) on the nature and necessity of undertaking cyber security research and cybercrime protection from the perspective of politics. These studies suggest strongly that any serious country and indeed other

organizations as well as individuals today must have a serious provision and concern for securing their personal belongings, data, and environment against political attacks via cyber warfare.
The theoretical and empirical contribution of this research supports the conclusion that the assumptions and strategies presented by the likes of Alagappa (1987), Cavelty et al. (2019), and Kshetri (2019) for identification of cyber security as a nontraditional political security threat that requires counteraction should be analyzed and digested by researchers and policymakers in the area of study.

2.2 Research design and methods development

The research design adopted for this study is descriptive research design. This design is considered suitable, because it makes use of primary sources of data as it key and first hand evidence. This method of research design affords the researcher to maintain a cordial interaction with the focus group in the identified study population. The research is constructed on ***mixed research strategy*** (*quantitativ*e and *qualitative methods*; *primary and secondary data collection and analyzing*). Hence, this study will be centered on sub-Saharan African countries using *Nigeria and Cameroon as a case study*. As Bryman (2006), explained the method of mixed strategy in the context of triangulation as traditional view where quantitative and qualitative researchers are combined to triangulate findings in other to be mutually corroborated. The researcher will make use of both the qualitative and quantitative method of research in order to be able to draw a valid and reliable result.

2.3 Population and area of the study

The population of this study comprises of *a host of military and paramilitary security personnel* in Nigeria and Cameroon; *researchers* of research institutes and *agencies handling security issues* in Nigeria and Cameroon; *academicians* (professors) of recognized universities in Nigeria and Cameroon; and as well as *personnel(s) in private setups such as banks*, telecommunication industries etc, in Nigeria and Cameroon.

2.4 Sample size and sampling technique

The study will use a diverse range of sources, including categories within the study, the Nigerian and Cameroonian government's cyber security policy document, and reports from relevant agencies. A total number of **sixty participants** will be selected, to be sorted in ***four categories coded as category A, B, C, and D through non probability sampling type, the purposive sampling technique.*** This technique is considered suitable because it affords the target audience the equal chances of being selected during the survey exercise which does not require any randomization techniques. Purposive sampling is used when a diverse sample is necessary or opinion of experts in a particular field is the topic of interest. Interviewing field professionals is a unique opportunity to gather information where it is not available elsewhere.
In category A, sixteen military or paramilitary security personnel will be selected from different agencies directly dealing with security issues (N = 16). Two senior security officers in Nigerian and Cameroonian military selection was based on the ease of access to the data and the presence

of high-quality data related to the subject being studied; another two senior officers from the Nigerian and Cameroonian Police Force selection was based on the ease of access to the data and the presence of high-quality data related to the subject being studied. Other interviewees in this category included two senior officers from the Department of State Security, two senior officers from both Nigerian and Cameroonian Immigration Services, two senior officers from the Nigerian and Cameroonian Prison Services, two senior officers from the Nigerian and Cameroonian Security and Civil Defense Corps, two senior officers from the Nigerian and Cameroonian Custom Services, and two senior officers from the Nigerian and Cameroonian Federal Road Safety Corps.

In category B, twenty senior officials will be chosen from institutes and agencies handling security issues in Nigeria and Cameroon (N = 20), including four senior officials from the Institute for Policy and Strategic Studies, four senior officials in the Defense Academy, four senior officials from the Police College, four senior officials from the Ministry of Defense, and four senior officials from the War Institute.

For its part, **category C** There will be a group of academics scholars, consisting of twelve professors chosen from three universities, based on the proximity to the target audience (N = 12). Four professors from reputable national universities that specializes in political science with a focus on security and strategic studies. Four professors from reputable national universities that specializes in computer science with a focus on cyber security and the digital environment. The remaining four professors from reputable national universities that specializies in sociology with a focus on criminology

In category D, twelve members of private institutions that deal with cyber activities will be selected randomly and interviewed (N = 12). These comprises of two senior bank officials in two commercial banks, four senior officers from the telecommunications companies operating in Nigeria and Cameroonian, two senior officials in the Communication Commission, two senior officials from the Technology Development Agencies, and two senior officials from the Federal Ministry of Communication. All the participants will be selected and interviewed directly online.

Furthermore, to answer the proposed research question (1-2) a semi-structured interview will be conducted. In accordance with the ethical standards, the research would anonymize the names of the participants; informants are not personally identified, but instead codified as (I) informants.

The interview is expected to last from a half to one hour. After analyzing the collected data, the informants were asked to review the findings and to provide comments.

Thus, the author emphasize that the main dimensions of the interview focuses on the areas of informants' personal demographic variables such as gender, name of organization, cadre, position/designation and years of work experience (all contained in the Section A of the semi interview checklist); also the semi interview checklist contains raised questions centered amidst the current situation of cybercrimes and threats ravaging the digital space with reference to the selected sub-Saharan African countries specified in the study i.e., Nigeria and Cameroon, here the informants gives their personal assessment on cyber security protocols and already established laws in combating cyber crimes in the digital economy peculiar to their country (all the raised questions are contained in the Section B of the interview checklist); and lastly, the semi interview

checklist also contains raised questions on the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes as in the case of trust in this evolving complex digitalized economy as both corporate and individual users hands-off/outsource their cyber assurance in terms of monitoring, managing and safeguarding highly sensitive information internally to cyber security protocols regarded as "third party" peculiar to the informants country (all the raised questions are contained in the Section C of the interview checklist). Informants' could give their responses/feedbacks either through written modes in the provided space or documented in an audio format.

After analyzing the collected data, the informants will be asked to review the findings and to provide comments. Also, the transcribed interviews would be read repeatedly in order to capture the key points as well as identify meaningful elements in the area of study. The content analysis would be applied to analyze the qualitative data collected in the course of performing the interviews with the informants specified in the study area. The researcher would analyze the data using a modified version of content analysis. The qualitative content analysis distinguishes the following categories: subcategories, interview quotes etc.

Finally, the semi interview checklist was developed and generalized upon two fundamental constructs with motive to identify the nature and types of cyber security protocols and already established laws in combating cyber crimes in the digital economy of the selected sub-Saharan African countries; and the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes in the digital economy of the selected sub-Saharan African countries.

2.5 Research instrument and method of data collection

The primary research involves interviews and analysis of the opinion provided by the primary respondents. The research instrument to be used in this research work will be interview method: a semi-structured interview guide/questionnaire would be employed as research tools. This instrument is developed by the researcher. The research will ask specific questions to each group, but also some general questions to all interviewees. The interview method will involve semi-structured written questionnaires, which can be adapted for different groups. Some interviews will be conducted over the phone, email, or WhatsApp. The goal is to allow for flexibility and a free flow of information from the informants. Previous literatures, as well as digital resources and closed questionnaire (survey) will be used for the quantitative research strategy.

2.6 Other data sources

As mentioned, the *other* primary sources (strategies and policy documents) The study will use a diverse range of sources, including categories within the study, the Nigerian and Cameroonian government's cyber security policy document, and reports from relevant agencies. While those of ***secondary sources***, consists secondary statistical data, journals, and internet sources relevant to the topic at hand.

2.7 Criteria for informants' selection

There are **three criteria used in identifying informants** to be interviewed in this study.

i. ***The first*** is the *identification of stakeholders who are closely linked and related to the subject matter of cyber security, and cyber crime, digital economy and national security.* The researcher will be instructed by various agencies and ministries to consult staff or units on cyber security in security parastatals and other ministries. The researcher will be instructed by higher-level officials at the unit to seek guidance from the most knowledgeable individuals on the topic of cyber security. The chosen sources will be interviewed under the condition of anonymity and confidentiality.

ii. ***The second*** *selection was based on the ease of access to the data and the presence of high-quality data related to the subject being studied same for some government ministries and agencies.*

iii. ***The third*** *the members of private institutions that deal with cyber activities will be used as criteria.*

In summary, based on Sharan's postulate (2009) that the minimum number of interviewees for a qualitative research project should be either four or five and that the maximum should not be more sixty, depending on the availability of the resources and informants with quality information.

2.8 Method of data analysis

The collected data will be organized distinctly and analyzed through content analysis. This process will involve comparing the findings of this research to prior literature and using the established theoretical framework to draw conclusions and present the results.

In summary, this chapter has made an appraisal of the theoretical tenets (framework) validating the construct of this research methodology. Amongst the proposed theoretical tenets were those of protection motivation theory and the planned behaviour theory. Also the model of Alagappa (1987) on national security of developing countries was considered. Furthermore, the research methodology outlined for the thesis such as the research design, population of the study, sample and sampling technique, research instrument, method for data collection, other data sources, and criteria for informants' selection and method of data analysis were all considered, determined and substantiated for the research.

CHAPTER THREE

EMPIRICAL ANALYSIS: DATA ANALYSIS AND RESULTS

This chapter gives the empirical analysis of data generated by the researcher and also discusses the results obtained from the analysis.

3.1 Data analysis

For the purpose of this research, a total of 60 sample size was selected from the study population and were administered copies of the semi-structured interview questionnaire. However, only 54 copies of the semi-structured interview questionnaire were correctly and completely responded to by the sampled respondents and were returned and collated by the researcher for data analysis. The analysis is presented in three categories as follows:

The first category entails the presentation and distribution of respondents' demographic characteristics which shows the relationship among others; respondents' gender, cadre, position and experience as indicated in the research instrument.

Also, second category of the analysis presents and analyzes the respondents' views on the subject matter (**security impact of cyber security management on digital economy across sub-Saharan African countries using Nigeria and Cameroon as a case study**) in relations to the hypothesized research questions as responded and collated in the semi-structured interview questionnaire.

Finally, of the analysis makes a general discussion from the findings thereof in relations to the empirical outcomes and findings of previous scholars on cyber security management and digital economies of advanced, developing and emerging countries (Nigeria and Cameroon) as indicated in the study case of this research.

3.2 Presentation and distribution of respondents' demographic characteristics

Table 3.2 Distribution of respondents' demographic characteristics

VARIABLE	OPTIONS	FREQUENCY	VALID PERCENTAGE %	CUMM PERCENTAGE %
GENDER	**MALE**	**44**	**81.5**	**81.5**
	FEMALE	10	18.5	100.0
			100.0	
CADRE	**TOP**	**20**	**37.0**	**37.0**
	MIDDLE	26	48.2	85.2
	LOWER	8	14.8	100.0
			100.0	
POSITION	**SYSTEM ANALYST**	**18**	**33.4**	**33.4**
	DATA ANALYST	12	22.2	55.6
	PROGRAMMER	16	29.6	85.2
	SYS ADMINISTRATOR	8	14.8	100.0
			100.0	
EXPERIENCE	**5-10YRS**	**30**	**55.5**	**55.5**
	11-20YRS	14	26.0	81.5
	21YRS AND ABOVE	10	18.5	100.0
			100.0	

Source: Researcher's Field Report (2022)

From the table 3.2 above, it was evident that 44(81.5%) of the respondents were male, while the remaining 10(18.5%) were female respondents. This implies that majority of the respondents that took part in the research exercise were male. Also, it was evident from the table that 20(37.0%) of the respondents were at the top cadre of their organizations, 26(48.2%) were at the middle cadre, while the remaining 8(14.8%) were at the lower of their organizations respectively. This implies that majority of the respondents that took part in the research exercise were at the middle cadre of their organizations.

Furthermore, it was also evident from the table that 18(33.4%) of the respondents were employed as system analyst in their organizations, 12(22.2%) were employed as data analyst, 16(29.6%) were employed as programmer while the remaining 8(14.8%) were employed as system administrators in their organizations respectively. This implies that majority of the respondents

that took part in the research exercise were employed as system programmer in their respective organizations.
Lastly, it was also evident from the table that 30(55.5%) of the respondents had at least 5-10yrs of work experience on the job, 14(26.0%) also had at least 11-20yrs of work experience on the job, while the remaining 10(18.5%) of the respondents had well over 21yrs and above work experience on the job respectively. This implies that majority of the respondents that took part in the research exercise had at least 5-10yrs of work experience on cyber security management as it relates to their job description in their respective organizations.

3.3 Test of hypothesized research questions

To support this thesis, ***three fundamental hypotheses are formulated as follows (H_1; H_2; H_3).*** The testing/verification of the above-outlined hypotheses explained the interaction of cyber security management and its impact on the digital economy in Sub-African countries.

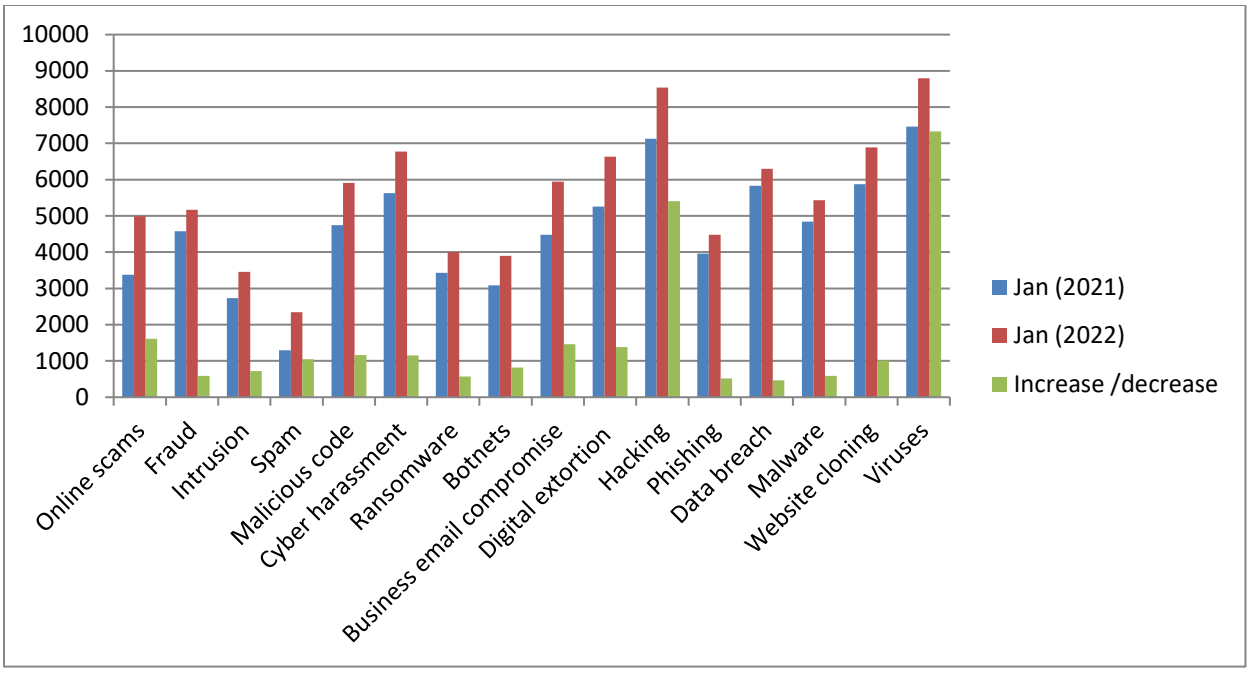
Here, the hypothesized research questions are tested in relations to respondents' views as portrayed in the semi-structured interview checklist) (see attached interview transcripts: Annex No 1)

Hypothesized Research Question One:

H_1 *What is the past and current trend of cyber crimes perpetrated in the digital economy of the selected sub-Saharan African countries?*

In a bid to provide answer to the hypothesized research question stated above, the researcher conducted an assessment on the collated responses of the sampled respondents on the sub questions surrounding "***based on the previous and current trend of cybercrime perpetrated in the digital economy of your country within 2020 and 2021"*** as indicated in **Section B** (*Number 2*) of the semi-structured interview questionnaire.

Table 3.3: Analysis on the past and current trend of cyber crimes perpetrated in the digital economy of the selected sub-Saharan African countries



Graphical illustration of the past and current trend of cybercrime perpetrated in the digital economy of the selected sub-Saharan African countries

From the above graphical presentation (table 3.3), it was evident that majority of the sampled respondents purported the series of cybercrimes perpetrated in their digital economy of the selected sub Sahara African countries within in January 2021 and January 2022 to be those of online scams, fraud, intrusion, spam, malicious code, cyber harassment, ransomware, botnets, business email compromise, digital extortion, hacking, phishing, data breach, malware, website cloning and viruses. However, based on the outcome of graphical illustration, the cybercrimes relating to those of viruses and hacking as at January 2021 and January 2022, were revealed to be the mostly perpetrated cybercrimes by cyber offenders within the digital axis of the selected sub Sahara African countries (Nigeria and Cameroon) and these further showed an absurd increase in the trend of viruses and hacking cyber-vices.

Hypothesized Research Question Two:

H_2 *What is the nature and types of cyber security protocols and already established laws in combating cyber crimes in the digital economy of the selected sub-Saharan African countries?*

In a bid to provide answer to the hypothesized research question stated above, the researcher conducted an assessment on the collated responses of the sampled respondents on the sub questions surrounding "***Amidst the current situation of cybercrimes and threats ravaging the digital space particularly most sub-Saharan African countries with reference to your country what is your assessment on cyber security protocols and already established laws in combating cyber crimes in the digital economy of your country***…" as indicated in **Section B** (*Numbers 1-16*) of the semi-structured interview questionnaire.

Table 3.4 Analysis on the nature and types of cyber security protocols and already established laws in combating cyber crimes in the digital economy of the selected sub-Saharan African countries

S/N	STATEMENTS	RESPONSES	REMARKS
1	Situation of cybercrime and attacks <...>"	Worst and decaying	Very true
2	Nature, types and trend of cybercrimes <...>"	Viruses and hacking	Very true
3	Major perpetrators and victims of the cybercrimes	Youths and unemployed	Very true
4	Major motive behind cybercrimes <...>"	Poverty and idleness	Very true
5	Presence of CSPs managing cyber activities <...>"	Present and established	Very true
6	Mention CSPs already established and in <...>"	EFCC,ICPC, Police, CCB etc	Very true
7	CSPs have legal backing to checkmate <...>"	Legal backing to prosecute	Very true
8	Position of laws of CSPs on cyber offenders in <...>"	Right to arrest/prosecute	Very true
9	Established laws that serve as deterrents <...>"	Provision of Criminal Acts	Very true
10	CSPs engage tracking devices to checkmate users <...>"	Do engage tracking devices	Very true
11	CSPs perform periodic drills to ensure that <...>"	Perform periodic drills	Very true
12	CSPs grant preferential access to certain users to <...>"	Depends on purpose/usage	Very true
13	CSPs restrict application access to users operating <...>"	Depends on the users	Very true
14	The percentage of users' who secure their devices <...>"	60-86 percent	Very true
15	CSPs keep users informed on threats and best <...>"	Massive awareness	Very true
16	CSPs enable usage of external devices based on <...>"	Depends on purpose/usage	Very true

Source: Researcher's Field Report (2022)

From the table 3.4 above it was evident that majority of the sampled respondents described the situation of cybercrime and attacks as very worst which has brought about societal and economic decadence in Nigeria and Cameroon. Also, majority sampled respondents acclaimed the most commonly perpetrated cybercrimes as that of viruses and hacking and also pointed an alarming rise in cyber-attacks within the periods of 2021 and 2022 in Nigeria and Cameroon. Also, majority of the sampled respondents affirmed that youths and unemployed as major perpetrators of cybercrimes in the selected sub-Saharan African countries (Nigeria and Cameroon). Also, majority of the sampled respondents among other factors attested poverty, idleness and get rich quick syndrome to be the motives behind why youths and those who fall within the unemployed bracket to engage in cybercrimes in Nigeria and Cameroon. Also, majority of the sampled respondents affirmed that there are cyber security protocols (CSPs) monitoring and checking all forms of illicit cyber activities in the selected sub-Saharan African countries.

Furthermore, majority of the sampled respondents also listed a few of the presence of already established CSPs monitoring illicit cyber activities such EFCC, ICPC, CCB and Police-force in Nigeria and Cameroon. Also, majority of the sampled respondents admitted that the established CSPs combating illicit cyber activities have the full backing and authorization of the law to prosecute cyber offenders in the selected sub-Saharan African countries. Also, majority of the sampled respondents pointed out that the already established CSPs have the right and the backing of the law (Criminal Act) to make arrest, prosecute and arraign suspects of illicit cyber activities before any presiding court law to ensure adequate verdicts and sentences are served to alleged offenders in the selected sub-Saharan African countries.

More so, majority of the sampled respondents also mentioned that CSPs acts within the provisions of the Criminal Acts to administer punishments as deterrents to cyber offenders in the selected sub-Saharan African countries. Also, majority of the sampled respondents admitted that the CSPs most cases engage the timely and adequate usage of tracking devices to monitor and checking users operating corporate owned and self-managed devices in the selected sub-Saharan African countries. Also, majority of the sampled respondents admitted that CSPs in the selected sub-Saharan African countries often undergo and conduct series of periodic drills to ensure that users are well prepared and informed so as to mitigate the adversity of cyber attacks.

In addition, majority of the sampled respondents also attested that CSPs in the selected sub-Saharan African countries barely grants preferential and unfettered access to classified applications to users, except such usage is governmentally and economically defined. Also, majority of the sampled respondents unanimously admitted that CSPs in the selected sub-Saharan African countries places restriction on access to classified applications to users operating either corporate owned and/or self-managed devices. Also, majority of the sampled respondents attested the percentage of users' who secure their devices are adequately password as 60-86 percent in the selected sub-Saharan African countries. Also, majority of the sampled respondents admitted that CSPs in the selected sub-Saharan African countries embarks on massive awareness in keeping users informed on threats and best practices safeguard and protect their cyber assets (vital data and information).

Lastly, majority of the sampled respondents also submitted that CSPs in the selected sub-Saharan African countries often discourage the usage of external devices either by corporate or personal users, except the purpose is defined before usage can be granted.

Hypothesized Research Question Three:

H_3 *What are the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes in the digital economy of the selected sub-Saharan African countries?*

Furthermore, in a bid to provide answer to the hypothesized research question stated above, the researcher also conducted an assessment on the collated responses of the sampled respondents on the sub questions surrounding "**What are your responses to the following sub questions to the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes as in the case of trust in this evolving complex digitalized economy as both corporate and individual users hands-off/outsource their cyber assurance in terms of monitoring, managing and safeguarding highly sensitive information internally to cyber security protocols regarded as "third party" in your country**…" as indicated in **Section C** (*Numbers 1-8*) of the semi-structured interview questionnaire.

Table 3.5 Analysis on the perceived roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes in the digital economy of the selected sub-Saharan African countries

S/N	STATEMENTS	YES	F	NO	F	NOT SURE	F
1	As a matter of urgency a vast pop <…>"	46	85.2	6	11.1	2	3.7
2	A vast percentage of users <…>"	18	33.4	24	44.4	12	22.2
3	More than forty-five percent users <…>"	36	66.7	8	14.8	10	18.5
4	Not less than twenty five percent <…>"	25	22.2	12	46.3	17	31.5
5	Users (corporate and individuals) <…>"	35	64.8	5	9.2	14	26.0
6	Users (corporate and individuals) <…>"	50	92.6	0	0	4	7.4
7	Due to the fast evolving digital <…>"	24	44.4	14	26.0	16	29.6
8	Only very few users would use <…>"	4	7.4	40	74.1	10	18.5

Source: Researcher's Field Report (2022)

From the table 3.5 above it was evident that majority of the sampled respondents with 46(85.2%) believes that as a matter of urgency a vast population of users (corporate and individuals) outsource and manage their IT and security infrastructure through service partners, 6(11.1%) responded no, while the remaining 2(3.7%) were not sure. Also, majority of respondents with 24(44.4%) doesn't believe that the vast percentage of users (corporate and individuals) security needs were well protected and managed effectively by existing service partners, 18(33.4%) believes that the vast percentage of users (corporate and individuals) security needs were well protected and managed effectively by existing service partners, while the remaining 12(22.2%) were not sure.

Furthermore, majority of respondents with 36(66.7%) believes that more than forty-five percent users (corporate and individuals) outsource less than 20 percent of their security functions to a third party, 8(14.8%) responded no, while the remaining 10(18.5%) were not sure. Also, majority of respondents with 12(46.3%) believes that not less than twenty five percent users (corporate and individuals) handle the bulk of their IT security internally and also enlist the help of consultants for support, 25(22.2%) responded no, while the remaining 17(31.5%) were not sure.

More so, majority of respondents with 35(64.8%) believes that users (corporate and individuals) seek outside help to fill in resource and knowledge gaps in their security resources and meet critical compliance and security demands, 5(9.2%) responded no, while the remaining 14(26.0%) were not sure.

Also, majority of respondents with 50(92.6)% believes that users (corporate and individuals) turn to external managed security service providers for a fairly broad spectrum of needs, ranging from tactical device monitoring to more strategic areas where they may lack the institutional knowledge, while the remaining 4(7.4%) were not sure.

In addition, majority of respondents with 24(44.4%) believes that due to the fast evolving digital economy and mitigate any damage following cyber attacks most users (corporate and individuals) would prefer to manage their compliance needs in-house, 14(26.0%) responded no, while the remaining 16(29.6%) were not sure.

Lastly, majority of respondents with 40(74.1%) don't believes that only very few users would use third parties for governance, risk and compliance management support, 4(7.4%) believes only very few users would use third parties for governance, risk and compliance management support, while the remaining 10(18.5%) were not sure.

In this study the aim of the Interviews was to triangulate the empirical data: the researcher gathered Qualitative data from field professionals and use it as supporting data for Quantitative data. This data helped to explain Quantitative data if specific details and elaborate the results.

Main requirements for the Interviews were:

1. To make sure the research question is clear.
2. Line of the questioning prepared in unbiased and clear manner.
3. Interviewees had clear information prior the Interview about conducted research and the purpose of the interviews.

Interview method is the best used when we want to learn detailed information from an experts. And particularly useful if it is the experts of the studied field and learn their opinions.
To approach the project, aim and objectives of the study, Interview was conducted and questions were asked to answer posed research questions and prove hypotheses.

Interview ***"Funnel method"*** was chosen to conduct the interviews. This particular method aims to collect a lot of information by starting with general questions, then narrowing the gap by asking open-ended questions and slowly getting to the point with directed questions. So, semi-structured interviews were conducted. This type of interview is proper when collecting attitudinal information on a large scale or when it is not possible to draw up a list of possible pre-codes because little is known about the subject area. With semi-structured interviewing, the open-ended nature of the question defines the topic under investigation but also provides opportunities for the interviewer and interviewee to discuss some issues in more detail (Mathers and all, 2000).

Content analysis for the ***semi-structured interview questionnaire*** was applied. Interviews transcripts were analyzed to quantify patterns and trends and coded and summarized to provide interpretation of Qualitative data and make a conclusion. In this case, direct quotations were used to support analysis and to bring gathered information to the reader as it is in reality. *The coding method was based on the research questions. Mixed methods research also allows the use of both inductive and deductive approaches for reasoning the data.*

Table 3.6 Triangulation findings of the semi-structured experts interview content analysis

Research criteria I-II-III	Categories Subcategories reflect survey indicators	Repetition rate	Interview quotes
I. The past and current trend of cyber crimes perpetrated in the digital economy of the selected	(a) Current situation of cyber attacks in the countries under survey	7	'<...>''very alarming and disturbing phenomenon;
		5	'<...> a demeaning and shameful act on the rise ;
		4	'<...> so disheartening and a totally lost of goodwill and national resources;
	(b) Assessment of most common perpetrated cyber attacks in the	6	'<...>viruses and hacking ;
		3	'<...> digital extortion and cyber harassment;

sub-Saharan African countries	countries under survey		
	(c) Factors behind perpetration of cybercrimes and the age bracket of it perpetrators in the countries under survey	8	'<...>the high state of unemployment, poverty and get rich quick syndrome and it major perpetrators are mostly the youths;
II. The nature and types of cyber security protocols and already established laws in combating cyber crimes in the digital economy of the selected sub-Saharan African countries.	(a) Forms and existence of cyber security protocols in the countries under survey	7	'<...> Independent Corrupt Practices Commission, Economic and Financial Crimes Commission, Code of Conduct Bureau, Public Complaints Commission (Ombudsman) , Police and other Security Agencies etc;
	(b) Systems of prosecuting and punishment metered to cyber offenders in the countries under survey	6	'<...>have the full backing and support of the Nigeria legal system as enshrined within the jurisdiction of the Nigerian Criminal Acts as amended;
		5	'<...>anyone found guilty of cyber offense by the law guiding against cybercrime is officially arrested by any of the anti-cyber protocol (agencies) and arraigned before the magistrate for prosecution and jailed/sentenced with or with bail depending on the count charges and extent of the cyber offence;
		6	'<...>arresting and arraign of cyber offenders for persecution before an accredited court of law in Nigeria';
	(c) Position of existing laws in the management of cybercrimes in the countries under survey	4	'<...> conduct swift fact check on cyber offenders;
		5	'<...> arrest, prosecute, arraigned before a judge and sentenced to jail based on the weight of the offense;

III. The roles of economy stakeholders in the repositioning and enforcement of cyber security	(a) Creation of tracking devices in checkmating cybercrimes in the countries under survey	6	'<...> security agencies are equipped with tracking devices and modules in detecting, checkmating and monitoring users operating corporate and self owned devices;
		4	'<...> extremely detective and effective;
		4	'<...> highly innovative and efficient;
	(b) Engagement of periodic security drills on specific and general cyber users	7	'<...> yes, there are concerted levels of periodic security drills and awareness by cyber security agencies to citizens towards the unanimous fight against cybercrimes adversities;
	(c) Preference to access on classified	6	'<...>well, it all depends on the nature and purpose of the classified applicant or user;

protocols in effectively combating cyber crimes in the digital economy of the selected sub-Saharan African countries.	information and applications among specific and general cyber users	5	'<...> preference should be accorded on the nature, type and purpose of the kind of information accessed by the classified applicant;
	(d) Percentage of users that secure devices with passwords or security codes	5	'<...> rating in percentage of users' who secure their cyber devices with a password is 55 to 65 percent ;
		4	'<...>who secure their cyber devices with a password, my rating will be 55 to 60percent;

The content analysis allowed for the researcher to be unassuming regarding qualitative data collection and analysis, and was not influencing the results.

3.4 Discussion of the research results

Here, ***significant findings of this study are discussed*** in this section as it relates to the focus of this study on cyber security management: security impact on digital economy across sub- Saharan Africa countries. Also, ***the empirical findings are discussed comparing with the results of other researchers.***

Based on the outcome of the tested research question on the past and current trend of cyber crimes perpetrated in the digital economy of the selected sub-Saharan African countries, *findings revealed that majority of the sampled respondents attested that among the commonly perpetrated cybercrimes in digital economy of the selected sub-Sahara African countries (Nigeria and Cameroon) as at January 2021 and January 2022 were those of viruses and hacking cybercrimes and these further showed an absurd increase in the trend of viruses and hacking cyber-vices perpetrated in digital economy of the selected sub-Sahara African countries.*

The outcome was in line with empirical views of Aghatise (2006) who also submitted that the arrival of internet in Nigeria has enabled criminals and their activities to increase the number of their unsuspecting victims and this invariably makes it difficult to track them down (Aghatise, 2006). Cybercrime is now a serious problem in Nigeria ranks third of the top ten cyber crime hot spots in the world by a 2009 Internet Crime Report (National White-Collar Crime Centre and the Federal Bureau of Investigation, 2010). Four years in a roll (2006, 2007, 2008 and 2009) Nigeria ranks world cyber crime perpetrator countries (National White-Collar Crime Centre and the Federal Bureau of Investigation, 2010). Also Ibrahim (2016) confirmed that cybercrime criminals in Nigeria focus exclusively on hacking as a means to perpetrate cyber-fraud. Furthermore, CIA

World Factbook (2020) supported that internet arrival in Cameroon has not just provided an opportunity for development but has also presented a ground for exploitation for criminal activities. According to Munbela Mungwe (2018). There has been a significant transition from traditional criminology to the study of cybercrime. Based on the outcome of *the tested research question on the nature and types of cyber security protocols and already established laws in combating cyber crimes in the digital economy of the selected sub-Saharan African countries, findings revealed that majority of the sampled respondents described the situation of cybercrime and attacks as very worst which has brought about societal and economic decadence in Nigeria and Cameroon.* Also, majority acclaimed the most commonly perpetrated cybercrimes as that of viruses and hacking and also pointed an alarming rise in cyber-attacks within the periods of 2021 and 2022 in Nigeria and Cameroon. *Also, majority affirmed that youths and unemployed as major perpetrators of cybercrimes in the selected sub-Saharan African countries (Nigeria and Cameroon). Also, majority among other factors attested poverty, idleness and get rich quick syndrome to be the motives behind why youths and those who fall within the unemployed bracket to engage in cybercrimes in Nigeria and Cameroon. Also, majority affirmed that there are cyber security protocols (CSPs) monitoring and checking all forms of illicit cyber activities in the selected sub-Saharan African countries.*

Furthermore, *majority listed a few of the presence of already established CSPs monitoring illicit cyber activities such EFCC, ICPC, CCB and Police-force in Nigeria and Cameroon. Also, majority admitted that the established CSPs combating illicit cyber activities have the full backing and authorization of the law to prosecute cyber offenders in the selected sub-Saharan African countries.* Also, majority pointed out that the already established CSPs have the right and the backing of the law (Criminal Act) to make arrest, prosecute and arraign suspects of illicit cyber activities before any presiding court law to ensure adequate verdicts and sentences are served to alleged offenders in the selected sub-Saharan African countries.

More so, majority of mentioned that CSPs acts within the provisions of the Criminal Acts to administer punishments as deterrents to cyber offenders in the selected sub-Saharan African countries. Also, majority admitted that the CSPs most cases engage the timely and adequate usage of tracking devices to monitor and checking users operating corporate owned and self-managed devices in the selected sub-Saharan African countries. Also, majority admitted that CSPs in the selected sub-Saharan African countries often undergo and conduct series of periodic drills to ensure that users are well prepared and informed so as to mitigate the adversity of cyber attacks. Also, majority attested that CSPs in the selected sub-Saharan African countries barely **grants** preferential and unfettered access to classified applications to users, except such usage is governmentally and economically defined. Also, majority admitted that CSPs in the selected sub-Saharan African countries places restriction on access to classified applications to users operating either corporate owned and/or self-managed devices. Also, majority attested the percentage of users' who secure their devices are adequately password as **60-86** percent in the selected sub-Saharan African countries. Also, *majority admitted that CSPs in the selected sub-Saharan African countries embarks on massive awareness in keeping users informed on threats and best practices*

safeguard and protect their cyber assets (vital data and information). And lastly, majority submitted that CSPs in the selected sub-Saharan African countries often discourage the usage of external devices either by corporate or personal users, except the purpose is defined before usage can be granted.

The outcome was in line with empirical views of Babayo et al (2021) who also confirmed that just like other sub-Saharan African countries (Cameroon, Ghana Malaysia) cybercrime is flourishing in Nigeria undetected like other sub, affecting its critical national infrastructure, causing prolonged terrorism affecting national security and the safety of national environment due to weak cyber security capability. Thus, Nigeria should adopt measures toward strengthening its cyberspace and digital environment to prevent crimes and promote national security and the digital economy. Also, Bakri et al (2019) submitted that cyber attacks in Cameroon and Malaysia is on the high side and its threats and vulnerabilities has great consequences on the nations digital trust, digital identity and digital business. It is therefore, expedient that laws on digital trust and cyber security should be consolidated and public awareness should be intensified to minimize the risk and to prepare for future unforeseen. Also, Mario et al (2018) affirmed that cyber security activities should no longer be solely the responsibility of IT departments or assigned individuals (CISOs or similar), but institution-wide efforts with all employees engaged. As digital technologies are strategically aligned with business strategy, the same should be done with cyber security. Hence, basic protection is efficient and needful, but there are still rooms for improvements in taking a collective ambition towards holistic cyber security governance and applying more advanced controls.

It can be stated, *based on the outcome of the tested research question on the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes in the digital economy of the selected sub-Saharan African countries, findings revealed that majority of the sampled respondents described with 46(85.2%) believes that as a matter of urgency a vast population of users (corporate and individuals) outsource and manage their IT and security infrastructure through service partners. Also, majority with 24(44.4%) doesn't believe that the vast percentage of users (corporate and individuals) security needs were well protected and managed effectively by existing service partners. Also, majority with 36(66.7%) believes that more than forty-five percent users (corporate and individuals) outsource less than 20 percent of their security functions to a third party. Also, majority of with 12(46.3%) believes that not less than twenty five percent users (corporate and individuals) handle the bulk of their IT security internally and also enlist the help of consultants for support. Also, majority 35(64.8%) believes that users (corporate and individuals) seek outside help to fill in resource and knowledge gaps in their security resources and meet critical compliance and security demands. Also, majority with 50(92.6)% believes that users (corporate and individuals) turn to external managed security service providers for a fairly broad spectrum of needs, ranging from tactical device monitoring to more strategic areas where they may lack the institutional knowledge, while the remaining. Also, majority with 24(44.4%) believes that due to the fast evolving digital economy and mitigate any damage following cyber attacks most users (corporate and individuals) would prefer to manage their compliance needs in-house. And Lastly, majority*

with 40(74.1%) don't believes that only very few users would use third parties for governance, risk and compliance management support.

The outcome was in line with empirical views of Branley-Bell et al (2021) who supported the need to consider the larger cyber security ecosystem when designing interventions to increase adoption of cyber insurance and/or promote more secure online behaviour. Eric, et al (2011) affirmed the need for a sound knowledge among policy makers and economic stakeholders on cyber security management with an in-depth understanding of the various structures and their existing efforts to combat cyber crime. Ekoa and Mungwe (2018) attested that with the existence of Internet Technology as internet users increases, there is every tendency for cybercrime to also be on the increase. Mshana (nd) supported that in a bid to consciously combat cybercrimes, there is need for governments of nations to design and come up with practical to combat cybercrimes so that people still enjoy using the technology rather than stop them to use it. Chooi and Ahmad (2017) also supported that in order for digital economy to thrive, the digital confidence of the stakeholders should be high. Nations with high digital confidence depend less on the national level NCSS to strengthen the trust and confidence in digital space. Nevertheless, the NCSS is still a need as a foundation for long term strategy to cement the cyber security of the nation, as cyber threats and risks keep evolving and will remain a challenge. Though a NCSS is not a requirement for nation to begin digital economy, NCSS is a requirement for a nation to continuously develop and to be successful in digital economy. Chooi and Ahmad (2017)

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

This study (by applying theoretical and empirical results) has thoroughly considered security impact of cyber security management on digital economy across sub-Saharan African countries using Nigeria and Cameroon.

The analysis of the significance of cyber security management intensity in the context of the Nigeria and Cameroon countries sustainability based on scientific sources, revealed *four important findings.*

1. From theoretical finding, it was very evident that from the outcome of the first hypothesized research question which to determine the past and current trend of cyber crimes perpetrated in the digital economy of the selected sub-Saharan African countries, it was evidently discovered that majority of the interviewed respondents concluded that among the commonly perpetrated cybercrimes were those of viruses and hacking cybercrimes within the digital economy of the selected sub-Sahara African countries (Nigeria and Cameroon) as at January 2021 and January 2022; and these has subsequently led to the absurd increase in the trend of viruses and hacking cyber-vices perpetrated in digital economy of the selected sub-Sahara African countries. A number of scholars such as Aghatise (2006); Ibrahim (2016); CIA World Factbook (2020); and National White-Collar Crime Centre and the Federal Bureau of Investigation (2010), all confirmed that the arrival of internet in sub-Saharan African countries under study has enabled criminals and their activities to increase the number of their unsuspecting victims and this invariably

makes it difficult to track them down. Cybercrime is now a serious problem in sub-Saharan African countries as many cyber perpetrators consider hacking as a means to perpetrate cyber-fraud and as a ground for exploitation for cyber criminal activities.

2. Furthermore, it was also evident that from the outcome of the second hypothesized research question which to determine the nature and types of cyber security protocols and already established laws in combating cyber crimes in the digital economy of the selected sub-Saharan African countries, it was also evidently discovered that majority of the interviewed respondents described the situation of cybercrime and attacks as very worst which has brought about societal and economic decadence in Nigeria and Cameroon. Majority also acclaimed the most commonly perpetrated cybercrimes as that of viruses and hacking and also pointed an alarming rise in cyber-attacks within the periods of 2021 and 2022 in Nigeria and Cameroon. Also, majority listed a few of the presence of already established CSPs monitoring illicit cyber activities such EFCC, ICPC, CCB and Police-force in Nigeria and Cameroon. Also, majority admitted that the established CSPs combating illicit cyber activities have the full backing and authorization of the law to prosecute cyber offenders in the selected sub-Saharan African countries. The outcome was supported by a number of scholars also Babayo et al (2021); Marioet al (2018); and Bakri et al (2019), concluding that like other sub-Saharan African, cybercrime is flourishing in Nigeria and Cameroon undetected, affecting its critical national infrastructure, causing prolonged terrorism affecting national security and the safety of national environment due to weak cyber security capability. Thus, the sub-Saharan African should adopt measures toward strengthening its cyberspace and digital environment to prevent crimes and promote national security and the digital economy. Also adding that cyber security activities should no longer be solely the responsibility of IT departments or assigned individuals (CISOs or similar), but institution-wide efforts with all employees engaged. As digital technologies are strategically aligned with business strategy, the same should be done with cyber security.
3. Also, it was evident that from the outcome of the third hypothesized research question which to determine the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes in the digital economy of the selected sub-Saharan African countries, it was also evidently discovered that majority of the interviewed respondents believes that as a matter of urgency a vast population of users (corporate and individuals) outsource and manage their IT and security infrastructure through service partners. Majority doesn't believe that the vast percentage of users (corporate and individuals) security needs were well protected and managed effectively by existing service partners. Also, majority believes that more than forty-five percent users (corporate and individuals) outsource less than 20 percent of their security functions to a third party. Finally, majority believes that not less than twenty five percent users (corporate and individuals) handle the bulk of their IT security internally and also enlist the help of consultants for support and that users (corporate and individuals) seek

outside help to fill in resource and knowledge gaps in their security resources and meet critical compliance and security demands. These outcomes were supported by some scholars Branley-Bell et al (2021); Eric, et al (2011); Ekoa and Mungwe (2018); and Chooi and Ahmad (2017), affirming that the need to consider the larger cyber security ecosystem when designing interventions to increase adoption of cyber insurance and/or promote more secure online behaviour and the need for a sound knowledge among policy makers and economic stakeholders on cyber security management with an in-depth understanding of the various structures and their existing efforts to combat cyber crime. Also noting that with the existence of Internet Technology as internet users increases, there is every tendency for cybercrime to also be on the increase. Hence, For the digital economy to be successful, stakeholders must have a high level of trust and confidence in digital technology

4. **Finally,** the situation of cybercrime and attacks in the selected sub Saharan African countries under study (Nigeria and Cameroon) demonstrates a very worst and these have led to societal and economic decadence. The most commonly perpetrated cybercrimes in Nigeria and Cameroon are those of viruses and hacking and as such has led to a surge in the rise of cyber-attacks within the periods of 2021 and 2022 in Nigeria and Cameroon. The main perpetrators of cybercrimes in Nigeria and Cameroon are the youths and unemployed; as this is more of an economical problem. Among other factors responsible for cybercrimes are those of poverty, idleness and get rich quick syndrome among youths and unemployed in Nigeria and Cameroon. Although, there are presence of existing cyber security protocols (CSPs) monitoring and checking all forms of illicit cyber activities in Nigeria and Cameroon there is need for more practical and logical solutions to tackle the threats and menace of cybercrime. Thus there is an urgency for a vast population of users (corporate and individuals) to outsource and manage their IT and security infrastructure through service partners and there is need for users security needs to be well protected and managed effectively by existing service partners; as an average user has a sound and an in-depth understanding on cyber security management as well as various structures combating cyber crime.

Recommendations

Based on the findings of this study the following recommendations were made *to the stakeholders*, especially *the Government and private institutions* which would be effective as a public-private partnership in:

a) Monitoring - In order to improve cooperation among different stakeholders in the field of cyber security, it is suggested that governments create a mechanism within their cyber security protocols (CSPs) structure to gather information about various projects and initiatives and disseminate it widely. It is also recommended that this mechanism utilize the resources and relationships already established within CSPs. At a minimum, CSPs should be monitoring these initiatives and projects by various organizations as a means of promoting cooperation. This can be done with minimal

resources and does not require the consent of the organizations, although their cooperation is preferable. Making this information available to stakeholders will encourage them to coordinate their activities.

b) Coordination - The government and economic stakeholders in the cyber security field should consider the possibility of creating a network to coordinate activities, initiatives, and projects in order to increase efficiency and better utilize resources. However, this initiative should be voluntary in order to avoid negative reactions from those who may see it as a loss of sovereignty. If there is sufficient support and resources, CSPs (cyber security providers) should take the lead in coordinating the work of various organizations to prevent duplication. The extent of control and resources available will determine the scale at which this coordination can take place.

c) Harmonizing – it is recommended that to tackle cyber-attacks, it would be to harmonize the cyber security strategies and protocols among different departments and agencies within an organization and government level. By aligning and standardizing these approaches, the organization can better defend against cyber threats and more effectively respond to any attacks that may occur. Additionally, working with external partners and stakeholders to harmonise cybersecurity efforts can also help to strengthen the organization's overall defenses against cyber attacks

d) Advocacy - tackle cyber-attacks is to increase advocacy for cyber security awareness and education. This can be achieved through promoting the importance of cyber security to individuals, businesses, and governments, and providing resources and training on how to protect against cyber threats. This can also involve working with policy makers to implement laws and regulations that promote cyber security and hold those who engage in cyber-attacks accountable for their actions. By increasing advocacy for cyber security, we can work towards building a more secure and resilient digital landscape. Thus, in order to bring about a culture of cyber security, it is important that CSPs undertakes the primary role in advocacy.

REFERENCES

Acquisti, A., Allan, F., & Rahul T (2006). Is there a cost to privacy breaches? An event study, International Conference on Information Systems (ICIS).

Ajzen, I. (1985) From intentions to actions: A theory of planned behavior. In action control; Springer: Berlin/Heidelberg, Germany.

Ajzen, I. (1991). *The theory of planned behavior*. Organ. Behav. Hum. Decis. Process, 50, 179–211.

Alagappa, M. (1987). *The national security of developing states: Lessons from Thailand*. Dover, MA: Auburn House.

Al-Khouri, A.M., (2012). *Emerging markets and digital economy. International Journal of Innovation in the Digital Economy*. 3(2), 57-69.

Allen, N. (2021) Africa center for strategic studies, Africa's evolving cyber threats. Available at: [https://Africacenter.org/spotlight/Africa-evolving-cyber-threats/]

Andreason, K. (2012). *Cyber security: Public Sector Threats and Responses*. London: Taylor & Francis.

Aniekan, M. N., & Afolabi, M. B. (2017). Introduction to cyber security and cyber crime. In Aniekan & Afolabi (Eds.) *Intelligence and Security Studies Programme*. Lagos, Nigeria: Spectrum.

Aslam, F., Aimin, W., Li, M., & Rehman, K.U (2020). Innovation in the era of IoT and industry 5.0: Absolute Innovation Management (AIM) Framework, Information, 11 (124), 1-24; doi:10.3390/info11020124 www.mdpi.com/journal/information

Babayo S., Bakri, M., Usman, S., Mohammed, K.T., & Muhammad, A.Y. (2021). Cyber security and Cybercrime in Nigeria: The implications on national. *Journal of Intelligence and Cyber Security*, 4(1), 27-61.

Bakri M., Siti, D.M.P., Ratnaria, W., & Babayo S (2019). Cyber security and digital economy in Malaysia: Trusted law for customer and enterprise protection. *International Journal of Innovative Technology and Exploring Engineering*, 8(8), 214-220.

Baller, S., S. Dutta, & B. Lanvin, (2016). The global information technology report: innovation in the digital economy, World Economic Forum: Geneva.

Barsky, R.B., Juster, F.T., Kimball, M.S., & Shapiro, M.D (1997) Preference parameters and behavioral heterogeneity: An experimental approach in the health and retirement study. *Q. J. Econ*, 112, 537–579.

Bax, S. (2011). Digital education: Beyond the "wow" factor. In Thomas, M. (Ed.), *Digital education. Opportunities for social collaboration* (pp. 239–256). New York: Palgrave Macmillan.

Beck, K.H. (1984). The effects of risk probability, outcome severity, efficacy of protection and access to protection on decision making: A further test of protection motivation theory. *Soc. Behav. Personal. Int. J*, 12, 121–125.

Black , G.P., & Hawk, K.R. (2010) Computer and internet crimes, San Francisco, California [Online] available from http://www.fd.org/pdf_ lib/WS2010/WS2010_Computer_Crimes.pdf.

Bohme, R., & Tyler, M. (2010). The iterated weakest link, *IEEE Security and Privacy*, 8(1), 53-55.

Bouwman, H. (1999, April). E-commerce: cyber and physical environments. *Electronic Markets, 9*(1).

Bowen, J.P., & Giannini, T. (2014). *Digitalism: The new realism?* EVA London 2014 Conference Proceedings. Electronic Workshops in Computing (eWiC), pp. 324–331. https://doi.org/10.14236/ewic/eva2014.38.

Brahmana, R., Brahmana, R.K., & Memarista, G. (2018). Planned behaviour in purchasing health insurance. *South East Asian J. Manag*.

Branley-Bell, D., Gómez, Y., Coventry, L., Vila, J., & Briggs, P. (2021). Developing and Validating a Behavioural Model of Cyber insurance Adoption. Sustainability, 13, 9528.

Brennen, S., & Kreiss, D. (2014). Digitalization and digitization. *Culture Digitally*, 8. Retrieved from: http://culturedigitally.org.digitalization-and-digitization.

Bryman, A. (2006). Integrating quantitative and qualitative research: How is it done? *Qualitative Research*, *6*(1), 97–113. https://doi.org/10.1177/1468794106058877

Brynjolfsson, E., & Kahin, B. (Eds.) (2002). *Understanding the digital economy: Data, tools, and research*. Cambridge: Massachusetts Institute of Technology.

Campbell, J. (2019). Council on Foreign Relations, Last Month, Over Half-a-Billion Africans Accessed the Internet. Available at: [https://www.cfr.org/blog/last-month-over-half-billion-Africans-accessed-internet]

Cavelty, M. D., & Wenger, A. (2019). Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science. *Contemporary Security Policy* 41(1): 1–28.

CGTN, Rights group launches tool to stem cybercrime in Africa, Odonkor, A, 27 October 2020. Available at: [https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html.]

Chawki, M. (2005) *Cybercrime in France: An overview* [Online] available from<http://www.crime-research.org/articles/cybercrime-in-france-overview/>.

Checkpoint, The new ransomware threat: Triple extortion, (2020). Available at: [https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/]

Chooi, S.T, & Ahmad K.M (2017). National cyber security strategies for digital economy, *Journal of Theoretical and Applied Information Technology*, 95(23), 1-4.

Cision, (2020). Africa Leads World in Digital Financial Services Deployments with Prepaid Cards an Important Part of Mix, Says Axiom Prepaid Holdings Reps. Available at: [https://www.prweb.com/releases/Africa_leads_world_in_digital_financial_services_deployments_with_prepaid_cards_an_important_part_of_mix_says_axiom_prepaid_holdings_reps/prweb17214821.htm]

Clayton, R. (2009). How much did shutting down McColo help? Sixth Conference on Email and AntiSpam.

Cybercrime Magazine, Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Morgan, S., 13 November 2020. Available at: [https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021]

Cybercrime and Money Laundering - Eurasiangroup.org. eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014_English.pdf.

DDoS Attacks in the United Kingdom. 4a7efb2d53317100f611-1d7064c4f7b6de25658a4199efb34975.ssl.cf1.rackcdn.com/ddos-lessons-from-uk-attacks-eresource-1-p-1524.pdf.

Detica. (2011). The cost of cyber crime, Cabinet Office, http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime

Diogenes, I., & Ozkaya, E. (2018). *Cyber security Attacks and Defense Strategy*. Birmingham, UK: Packt Publishers.

Dion, Michael (2010) *Advance fee fraud letters as machiavellian/narcissistic narratives*, *International Journal of Cyber criminology*,4(1and2), 630–642 [Online] available from http://www.cybercrimejournal.com/ micheldion2010ijcc.pdf/.

Dittrich, R., Wreford, A., Butler, A., & Moran, D. (2016). The impact of flood action groups on the uptake of flood management measures. Clim. Chang. 138, 471–489.

Druică, E. (2012). *Digital economy. Innovations and impacts on society*. Hershey: Information Science Reference.

Ekoa, R., & Mungwe, M. (2018). A review of Cybercrime in Sub-Saharan Africa: A Study Cameroon and Nigeria. *International Journal of Scientific & Engineering Research*, 9(5), 211-228.

ENISA. (2018) Cyber security culture guidelines: Behavioural aspects of cyber security; ENISA: Attiki, Greece.

Eric, A.A, Isaac, M.O., & Chanika, R.J. (2011). Combating cyber crime in Sub-Sahara Africa; A discourse on law, policy and practice. *Journal of Peace, Gender and Development Studies*, 1(4), 129-137.

Fassassi, A., (2016). Scidenet, Cybercrime in Africa: Facts and figures., July 2016. Available at: [https://www.scidev.net/sub-saharan-Africa/features/cybercrime-Africa-facts-figures/]

Fischer, E.A. (2009). Creating a National Framework for Cyber security. An Analysis of Issues And Options. New York: Nova Science Publishers.

Friedman, A. (2011). Economic and policy frameworks for cyber security risks. Center for Technology Innovation at Brookings, p. 1-24

Frizell, S. (2018). How Kenya's new data privacy bill could hurt its economy, Accessed November 8, 2018. https://www. cfr.org/blog/how-kenyas-new-data-privacy-bill-could-hurt-its-economy.

Gady, F.S. (2010). Africa's cyber WMD. http://www.foreignpolicy.com/articles/2010/03/24/ africas_cyber_wmd?page=0,0.

Gärdin, O. (2002). The New Economy New challenges for the statistical system. *The International Association for Official Statisticians Conference*, London 2002.

Garcia, D., et al. (2018). The exponential age of technology. Science, 342(6157), 668-671.

Goldfarb, A., & Tucker, C. (2019). Digital economics. *Journal of Economic Literature*, 57(1), 3–43. https://doi.org/10.1257/jel.20171452.

Goliński, M. (2018). Gospodarka cyfrowa, gospodarka informacyjna, gospodarka oparta na wiedzy – rożne określenia tych samych zjawisk czy podobne pojęcia określające rożne zjawiska? *Roczniki Kolegium Analiz Ekonomicznych SGH*, No. 49.

Grahn, T & Jaldell, H. (2019). Households (un)willingness to perform private flood risk reduction—Results from a Swedish survey. *Saf. Sci*, 116, 127–136.

Granrath, L. (2017). *Japan industry news*. Retrieved from: https://www.japanindus trynews.com/2017/08/japans-society-5-0-going-beyond-industry-4-0.

Greenberg, L. T., Goodman, S. E., & Soo Hoo, K. J. (1998). *Information warfare and* international *law*. Washington, DC: National Defense University Press.

Grossklags, J., Nicolas, C., & John, C (2008). Secure or insure?: A game-theoretic analysis of information security games, Proceeding of the 17th international conference on World Wide Web.

Guiora, A. M. (2017). *Cyber security, geopolitics and law*. London: Routledge. Heintze, H., & Thielborger, P. (2016). "From Cold War to Cyber War: The Evolution.

Gunter, W., Higgins, G. & Gealt, R. (2010) *Pirating youth: Examining the correlates of digital music piracy among adolescents*, *International Journal of Cyber Criminology* 4(1and2), 657–671 [Online] available from http://www.cybercrimejournal.com/whitneyetal2010ijcc.pdf/.

Hathaway, M.E., (2013). *Cyber Readiness Index 1.0*. Hathaway Global Strategies LLC: Great Falls, VA.

Helbing, D. (2015). *Thinking ahead – essays on big data, digital revolution, and participatory market society*. Cham: Springer.

Hinduja, Sameer & Schafer, Joseph A. (2009) "US cybercrime units on the world wide web", Policing: An International Journal of Police Strategies and Management, 32(2), 278 – 296 Available from < http://www. emeraldinsight.com/journals.htm?issn=1363-951Xandvolume=32andissue= 2andPHPSESSID=9b6iln802cqem26pgpbll0pme0>.

Hoepman, J., & Jacobs, B. (2007). Increased security through open Source: *Communications of the ACM*, Jan2007, Vol. 50 Issue 1, p79-83, 5p [Online] available from http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid =7a28b26e-60d2-4ee8-a9ff-d0f7f9f6cdef%40sessionmgr104andvid=1andhid=105.

Hoofnagle, C.J. (2010). Internalizing identity theft, *UCLA Journal of Law and Technology*, pg 1.

Human Development Report (2021-22). Uncertain times, unsettled lives: shaping our future in a transforming world. New York. Human Development Report 2021-22 | Human Development Reports (undp.org)

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Comput. Secur, 31, 83–95.

International Finance Corporation, Digital Access: The Future of Financial Inclusion in Africa, 2018. Available at: [https://www.ifc.org/wps/wcm/connect/region__ext_content/ifc_external_corporate_site/sub-saharan+africa/resources/201805_report_digital-access-africa]

Internet Security Threat Report- Symantec 2013.

Issac, Biju., & Mohammed, L.A. (2007) War driving and WLAN security issues - Attacks, security design and remedies*: The Journal of Information Systems Management*, 24(4), 289-298, 10p, [Online] available from < http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=7andhid= 105andsid=d9b6cd7d-57dd-42f8-89f2-dcf2f83440ea%40sessionmgr110>.

Johansson, B., Karlsson, Ch., & Stough, R. (2006). Entrepreneurship, clusters and policy in the emerging digital economy. In Johansson, B., Karlsson, Ch., & Stough, R. (Eds.), *The emerging digital economy: Entrepreneurship, clusters, and policy* (pp. 1–19). Berlin: Springer.

Kanich, Chris et al. (2008). Spamalytics: An empirical analysis of spam marketing conversion, proceedings of the 15th ACM conference on computer and communications security.

Kaspersky, (2020) The year of social distancing or social engineering? Phishing goes targeted and diversifies during COVID-19 outbreak. Available at: [https://www.kaspersky.com/about/press-releases/2020_the-year-of-social-distancing-or-social-engineering]

Kauffman, R.J. & Walden, E.A. (2001). Economics and e-commerce: survey and research directions. *International Journal of Electronic Commerce*, *5*(4), 4-115.

Kehal, H.S. & Singh, V.P. (2005). *Digital economy: Impacts, influences, and challenges*. Idea Group Pub.

Kirwan, Gráinne, and Andrew Power. "The Psychology of Cyber Crime." *Advances in Digital Crime, Forensics, and Cyber Terrorism*, 2012, doi:10.4018/978-1-61350-350-8.

Kleiman, M., & Beau K (2009). The dynamics of deterrence, proceedings of the national academy of sciences of the United States of America, 106(34).

Knickrehm, M., B. Berthon, & P. Daugherty, (2016) *Digital disruption: The growth multiplier.* accenture strategy.

Koops, B. (2016). Megatrends and grand challenges of cybercrime and cyber terrorism policy and research. In Akhgar, B., & Brewster, B. (Eds.) *Combating Cybercrime and Cyber terrorism: Challenges, Trends and Priorities*. Geneva: Springer.

Kosseff, J. (2017). *Cyber security law*. Hoboken, NJ: John Wiley & Sons.

Kostopoulos, G.K. (2013). Cyber space and cyber security. London: Taylor & Francis.

Kremling, J., & Parker, A. M. S. (2018). *Cyber space, cyber security and cyber crime*. London: Sage.

Kshetri, N. (2010). The economics of click fraud. IEEE Security & Privacy Magazine, 8(3), 45–53. doi:10.1109/ MSP.2010.88

Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: Some economic and institutional considerations. *Electronic Commerce Research,* 13 (1), 41-69.

Kshetri, N. (2015). Cybercrime and cyber security issues in the BRICS economies. Journal of Global Information Technology Management, 18(4), 1–5. doi:10.1080/1097198X.2015.1108093

Kshetri, N. (2019). Cybercrime and cyber security in Africa. *Journal of Global Information Technology Management* 22(2): 77–81.

Kumar, V. S (2008) cyber crime prevention, detection [online] available from http://www.cidap.gov.in/documents/Cyber%20Crime.pdf.

Kunz, M., & Wilson, P. (2004) Computer crime and computer fraud, university of maryland department of criminology and criminal justice [online] available from http://www.montgomerycountymd.gov/content/ CJCC/pdf/computer_crime_study.pdf.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M.H. (2014) Information security awareness and behavior: A theory-based literature review. *Manag. Res. Rev*, 37, 1049–1092.

Liptak, Andrew. "The WannaCry Ransomware Attack Has Spread to 150 Countries." *The Verge*, The Verge, 14 May 2017, www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries.

Luftman, Jerry. "Strategic Alignment Maturity." *Computing Handbook, Third Edition*, 2014, doi:10.1201/b16768-75.

Lovelock, P. (2018), *Framing policies for the digital economy towards policy frameworks in the Asia-Pacific.* Singapore: UNDP Global Centre for Public Service Excellence.

Lynn, William, (2010).Defending a new domain: The pentagon's cyber strategy, *Foreign Affairs*. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

Mario S., & Alen, Š (2018). Cyber security challenges in digital economy. Proceedings of the world congress on engineering 2018, I(4-6), London, U.K.

Martellozzo, E., Nehring, D., & Taylor, H. (2010) *Online child sexual abuse by female offenders-An Exploratory study*, International Journal of Cyber criminology Vol 4 Iss 1and2, pp 592–609 [Online] available from http://www.cybercrimejournal.com/elenaetal2010ijcc.pdf/.

Maurushat, A. (2013). *Disclosure of security vulnerabilities: Legal and ethical issues*. Berlin: Springer.

McAfee, Net losses: Estimating the global cost of cybercrime. 2014.

Meeuwisse, R. (2015). Cyber security for Beginners. Canterbury: Icutrain Ltd.

Moore, Tyler et al. (2011). The economics of online crime," *Journal of Economic Perspectives*, 2009.

Mowbray, T.J. (2013). Cyber security: Managing systems, Conducting testing, and investigating intrusions. Indianapolis: John Wiley & Sons.

Mshana, J.A (nd). Cybercrime: An Empirical Study of its Impact in the Society- A Case Study of Tanzania.

Mulligan, C., (2017). Cyber security: cornerstone of the digital economy, in Imperial College Business School London, Imperial College London: London.

Nasir, A., Arshah, R.A., & Ab Hamid, M.R. (2018). The Significance of main constructs of theory of planned behavior in recent information security policy compliance behavior study: A comparison among top three behavioral theories. Int. J. Eng. Technol,7, 737–741.

Norwood, H.T. & Catwell, S.P. (2009). Cyber security, Cyber analysis and warning. New York: Nova Science Publishers.

Nowicka, K. (2019). *Technologie cyfrowe jako determinanta transformacji łańcuchow dostaw*. Warszawa: Oficyna Wydawnicza SGH.

Nuestar-insights DDoS attacks survey q1-2012.

OECD, (2019). *Going digital: Shaping policies, improving lives*. Paris: OECD Publishing. https://doi.org/10.1787/9789264312012-en.

Palo Alto Networks (2021), Extortion Payments Hit New Records as Ransomware Crisis Intensifies, Baylor, Brown and Martineau. Available at: [https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/]

Pelton, J. N., & Singh, I. B. (2015). *Digital Defense: A Cyber security Primer*. Cham: Springer.

Persaud, A. (2001). The knowledge gap. *Foreign Affairs, 80*(2), 107-117.

Reddy, G.N., & Reddy G.J.U (2017). Study of cyber security challenges and its emerging trends on latest technologies.

Reva, D. (2020) Institute for security studies, Africa can't risk a major maritime cyber attack,. Available at: [https://issAfrica.org/iss-today/Africa-cant-risk-a-major-maritime-cyberattack]

Rittinghouse, J.W. & Hancock, W.M. (2003). Cyber security operations handbook. Amsterdam: Elsevier.

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *J. Psychol*, 91, 93–114.

Rowe, B.R. & Michael, P.G., (2006). Private sector cyber security investment strategies: An Empirical analysis, presented at the fifth Workshop on the Economics of Information security (WEIS).

Saban, K.A., McGivern, E., & Saykiewicz, J.N. (2002); A critical look at the impact of cybercrime on consumer behaviour: *Journal of Marketing Theory and Practice*, 10(2), 29, 9p [Online] available from < http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?sid=e59a071fc629- 476c-97e0-283aa772d4d2%40sessionmgr112andvid=1andhid=105>

Salminen, M., & Zojer, G. (2020). A human security perspective on cyber security in the European High North. In Salminen, M., Zojer, G., Hossain, K. (Eds.), *Digitalization and human security: A multi-disciplinary approach to cyber security in the European High North* (pp. 3–17). London: Palgrave-Macmillan.

Schachtman, N. (2011). Pirates of the ISPs: Tactics for turning online crooks into international pariahs. Brookings Institution 21st Century Defense Initiative, Forthcoming.

Schwab, K. (2016), *Fourth Industrial Revolution*, World Economic Forum.

Serpa, S., Ferreira, C.M, Sa, M.S., & Santos, A.I. (2020). *Digital society and social dynamics*. https://doi.org/10.14738/eb.17.2020.

Shalhoub, Z. K., & Al Qasimi, S. L. (2010). *Cyber law and cyber security in developing and* emerging *economies*. Northampton, UK: Edward Elgar.

Sharan, M.P. (2009). *Qualitative research method*. San Francisco: John Wiley & Sons.

Sharma, S. K., Wickramansinghe, N. & Gupta, J.N.D. (2004). What should SMEs Do To succeed in today's knowledge-based economy? In N. Al-Qirim (Ed.), *(forthcoming).* Hershey, PA: Idea Group Publishing.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance. Inf. Manag. Comput. Secur, 22, 42–75.

Special Report on Human Security (2022). Special report on human security | Human development reports (undp.org).

Symantec Intelligence Report 2013.

Symantec Internet Security Threat Report: Trends for 2010, Symantec.

Symantec, Cybercrime and Cyber Security Trends in Africa. November 2016. Available at: [https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf]

Szelągowska, A & Pluta-Zaremba, A (2021). The economics of sustainable transformation; transformation of the economy towards era 5.0 (ebk) (CC BY-NC-ND 4.0). Routlegde

Taylor & Francis Group, London and New York. https://www.researchgate.net/publication/355412085

Tapscott, D. (1995). *The digital economy: Promise and peril in the age of networked intelligence*. New York: McGraw-Hill.

Trend Micro & INTERPOL (2017), Cybercrime in West Africa; Poised for an underground market. Available at: [https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-Africa.pdf]

Tsai, H.-Y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., & Cotten, S.R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Comput. Secur*, 59, 138–150.

UBM Tech (2014). The state of cyber security economy. Balancing flexibility with effective risk management.

United Nations, (2019). *Digital economy report 2019. Value creation and capture: Implications for developing countries*. Geneva: United Nations Publications.

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *Int. J. Hum. Comput. Stud*, 123, 29–39.

Wall, David S. (2005) The internet as a conduit for criminal activity, In A. Pattavina (Ed.), Information technology and the criminal justice system (pp.78-94) Thousand Oaks, CA: Sage..

Wang, Q & Seung H.K (2009). Cyber attacks: does physical boundary matter? Proceedings of the International Conference on Information Systems (ICIS).

Weill, P. & S.L. Woerner, (2013). The Future of the CIO in a Digital Economy. MIS Quarterly Executive. 12(2).

Welcome to Fbi.gov." *FBI*, FBI, 31 Mar. 2022, www.fbi.gov/scams-safety/fraud/internet_fraud.

Wienclaw, R.A. (2008) *Internet security -- Research starters business* [online] available from < http://web.ebscohost.com/ehost/pdfviewer/pdfviewer?hid= 105 andsid=56be29d8-2da9-4ecd-9429-c3b87bbdd88a%40sessionmgr114andvid =1>.

Woodall, P. (2000). Survey: The new economy: Knowledge is power. *The Economist*, *356*(8189), 27-32.

Xu, Y., Wang, H., & Zhang, Y. (2019). A review of machine learning techniques applied in cyber security. IEEE Access, 7, 122124-122142.

Yadav, Hetram, and Shashant Gour. "Cyber Attacks: An Impact on Economy to an Organization.'" *International Journal of Information & Computation Technology.*, Volume 4, no. 0974, ser. 2239, 2014. *2239*, doi:http://www. irphouse.com.

Yakubu, A.M. (2017). Cyber security issues in nigeria and challenges. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(4), 315-32.

ANNEXES

ANNEXE No1.

INTERVIEW CHECKLIST

ODEJAYI, Rasheed Olalekan
raodejayi@stud.mruni.eu
MYKOLAS ROMERIS UNIVERSITY, LITHUANIA
(Ateities st. 20, LT-08303 Vilnius)

I am a final student of the above named university. I am currently conducting my master's thesis (research) on **Cyber Security Management: Security Impact on Digital Economy across Sub- Saharan African Countries** in partial fulfillment for the award in Masters (MSc) in Cyber Security Management.

I will appreciate it if you can schedule a few minutes of your precious time to help provide your views to the raised questions in this interview checklist.

The information provided will be confidentially treated solely for the purpose of research.

Your co-operation is highly needed and appreciated.

Thanks

SECTION A

1. Gender: ……
2. Name of Organization:……...
3. Cadre:……..
4. Position/Designation:…….
5. Years of Work Experience:……..yrs

SECTION B

Amidst the current situation of cybercrimes and threats ravaging the digital space particularly most sub-Saharan African countries with reference to your country what is your assessment on cyber security protocols and already established laws in combating cyber crimes in the digital economy of your country with reference to the following questions **(please note that responses can be written in the provided space or documented in an audio format):**

1. What is the situation of cybercrime and attacks in your country?
   ……
   ……

……
……
……

2. What would be your assessment on the nature, types and trend of cybercrimes often perpetuated in your country within 2020 and 2021 (Here the informant is meant to provide the figures the previous and current years)

Incidents	Jan (2021)	Jan (2022)	Increase /decrease
Online scams			
Fraud			
Intrusion			
Spam			
Malicious code			
Cyber harassment			
Ransomware			
Botnets			
Business email compromise			
Digital extortion			
Hacking			
Phishing			
Data breach			
Malware			
Website cloning			
Viruses			

3. Who do you think are major perpetrators and victims of the cybercrimes?
……
……
……
……
……

4. What do you think is the major motive behind cybercrimes (is it political or economical)?
……
……
……
……
……

5. Are there cyber security protocols monitoring and managing cyber activities and/or crimes in your country?
……
……
……
……
……

6. Can you mention the cyber security protocols already established and in operation in your country?

   ……
   ……
   ……
   ……
   ……

7. Do cyber security protocols in your country have direct control and authorized backing to checkmate, prosecute and punish cyber offenders?

   ……
   ……
   ……
   ……
   ……

8. What is the position of the established laws of cyber security protocols on cyber offenders in your country?

   ……
   ……
   ……
   ……
   ……

9. Are the established laws strong enough to serve as deterrents to combat cybercrimes in your country?

   ……
   ……
   ……
   ……
   ……

10. Do cyber security protocols in your country engage tracking devices to checkmate and monitor users operating corporate owned and self-managed devices?

    ……
    ……
    ……
    ……
    ……

11. Do cyber security protocols in your country perform security drills on a periodic basis to make sure that users are prepared to mitigate the impact of cyber attacks?

    ……
    ……
    ……
    ……
    ……

12. Do cyber security protocols in your country grant preferential and unfettered access to certain users to classified applications while others only have access to general-issued devices?
    ……
    ……
    ……
    ……
13. Do cyber security protocols in your country restrict application access to users operating corporate owned and self-managed devices?
    ……
    ……
    ……
    ……
    ……
14. In your personal opinion, what's the percentage of users' who secure their cyber devices with a password?
    ……
    ……
    ……
    ……
15. Do cyber security protocols in your country engage and keep users informed on communicating information both about potential threats and about best practices with which to protect their assets?
    ……
    ……
    ……
16. Do cyber security protocols in your country enable external devices based on the role of the user?
    ……
    ……
    ……

SECTION C

What are your responses to the following sub questions to the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes as in the case of trust in this evolving complex digitalized economy as both corporate and individual users hands-off/outsource their cyber assurance in terms of monitoring, managing and safeguarding highly sensitive information internally to cyber security protocols regarded as "third party" in your country?

Please respond to sub-questions in the provided space by ticking (√). Key: Y (YES) =3; NS (NOT SURE) =2; and N (NO) =1.

Questions	Yes	No	Not sure

Do you think as a matter of urgency a vast population of users (corporate and individuals) outsource and manage their IT and security infrastructure through service partners?			
Do you think a vast percentage of users (corporate and individuals) security needs are well protected and managed effectively by existing service partners?			
Do you think more than forty-five percent users (corporate and individuals) outsource less than 20 percent of their security functions to a third party?			
Do you think not less than twenty five percent users (corporate and individuals) handle the bulk of their IT security internally but do enlist the help of consultants for support?			
Do you think users (corporate and individuals) seek outside help to fill in resource and knowledge gaps in their security resources and meet critical compliance and security demands?			
Do you think users (corporate and individuals) turn to external managed security service providers for a fairly broad spectrum of needs, ranging from tactical device monitoring to more strategic areas where they may lack the institutional knowledge?			
Do you think due to the fast evolving digital economy and mitigate any damage following cyber attacks most users (corporate and individuals) would prefer to manage their compliance needs in-house?			
Do you think only very few users would use third parties for governance, risk and compliance management support?			

I SINCERELY APPRECIATE YOUR TIME AND OPINIONS SO PROVIDED. I ASSURE YOU THAT EVERY RESPONSE GIVEN WOULD BE KEPT CONFIDENTIAL

ANNEX NO1-4. SEMI STRUCTURED INTERVIEW CHECKLIST

ANNEXE No2.

INTERVIEWS TRANSCRIPT

Interviewee No1

Date of the interview: 3. 4. 2022
Interviewee name: Undisclosed.
The researcher: Rasheed Odejayi
Location: Ateitiesst. 20, LT-08303 Vilnius
Interview type: e-mail

Researcher:

Could you please provide as much information as possible about yourself concerning the topic of the study? Cadre, experience (can be general information only, such as job position and type of company, no name indicated)
How much experience do you have in cyber security?

Interviewee:

I have ten years experience in cyber security. I was employed initially as a system analyst; however, due to my quest for additional knowledge in cyber management, I was promoted to intermediate cyber analyst to manage and safeguard relevant and official data for the greater good my organization.

Researcher:

What is the situation of cybercrime and attacks in your country?

Interviewee:

Sincerely, issues regarding cybercrimes have totally become a stronghold menace in Nigeria and since inception, this demeaning act has been launched to sabotage the goodwill, resources and efforts of well meaning individuals, business startups, corporate organizations, as well as the government of the day.

Researcher:

Given the informant below, based on the previous and current nature, types and trend of cybercrime in your country, what would be your assessment within 2020 and 2021?

Interviewee:

Incidents	Jan (2021)	Jan (2022)	Increase /decrease
Online scams	3378	4994	**1616**
Fraud	4573	5165	**592**
Intrusion	2733	3455	**722**
Spam	1292	2341	**1049**

Malicious code	4744	5909	**1165**
Cyber harassment	5624	6772	**1153**
Ransomware	3433	4002	**569**
Botnets	3082	3899	**817**
Business email compromise	4476	5943	**1464**
Digital extortion	5254	6637	**1383**
Hacking	7131	8542	**1411**
Phishing	3961	4476	**515**
Data breach	5832	6299	**467**
Malware	4845	5432	**587**
Website cloning	5877	6888	**1011**
Viruses	7463	8793	**1330**

Researcher:

Who do you think are major perpetrators and victims of the cybercrimes?

Interviewee:

I believe most perpetrators of cybercrimes are fondly the so called 'Yahoo-Boys" or some time referred as "G-Boys" and I equally believe most of the time there are case of insiders (staff) who act as informants that sell-out vital information of the company to the G-Boys, aiding smooth and successful perpetrated cybercrimes.

Researcher:

What do you think is the major motive behind cybercrimes (is it political or economical)?

Interviewee:

Honestly, among other important factors that could be responsible for the motive behind engagement in cybercrime in Nigeria is accountable to the state of poverty and unemployment in the country. However, regardless of these factors, I believe these factors should be sufficient for any patriotic citizen to engage in cybercrime.

Researcher:

Are there cyber security protocols monitoring and managing cyber activities and/or crimes in your country?

Interviewee:

Yeah, there are a number of well renowned cyber security protocols (agencies) monitoring and managing cyber activities and/or crimes in the Nigerian.

Researcher:

Can you mention the cyber security protocols already established and in operation in your country?

Interviewee:

Among the already established protocols are those of Independent Corrupt Practices Commission (ICPC), Economic and Financial Crimes Commission (EFCC), Code of Conduct Bureau (CCB), Public Complaints Commission (Ombudsman) (PCC), Police and other Security Agencies etc.

Researcher:

Do cyber security protocols in your country have direct control and authorized backing to checkmate, prosecute and punish cyber offenders?

Interviewee:

Yeah, to a large extent the cyber security protocols in Nigeria all have direct control and authorized backing of the law to checkmate, prosecute and punish cyber offenders. As I speak there are countless of cases of cyber offenders whose fate had already been determined and are currently facing the full weight of the law.

Researcher:

What is the position of the established laws of cyber security protocols on cyber offenders in your country?

Interviewee:

Anyone found guilty of cyber offense by the law guiding against cybercrime is officially arrested by any of the anti-cyber protocol (agencies) and arraigned before the magistrate for prosecution and jailed/sentenced with or with bail depending on the count charges and extent of the cyber offence.

Researcher:

Are the established laws strong enough to serve as deterrents to combat cybercrimes in your country?

Interviewee:

At least, with the presence of the established law guiding against cybercrimes, a large number of persons has been deterred from perpetrating cybercrimes due to the kind of sentences metered on offenders and the rate of stigmatization (public disgrace) that comes with it.

Researcher:

Do cyber security protocols in your country engage tracking devices to checkmate and monitor users operating corporate owned and self-managed devices?

Interviewee:

Yeah, at least, to a reasonable degree the cyber security agencies in Nigeria are equipped with tracking devices and modules in detecting, checkmating and monitoring users operating corporate and self owned devices. However, based on the dynamic changes that come with technology there's need for the government to further equip the cyber security agencies for sake of effectiveness in detecting and tracking offenders for adequate prosecution of the law.

Researcher:

Do cyber security protocols in your country perform security drills on a periodic basis to make sure that users are prepared to mitigate the impact of cyber attacks?

Interviewee:

Yeah, to a reasonable degree there are concerted levels of periodic security drills and awareness by cyber security agencies in Nigeria to citizens towards the unanimous fight against cybercrimes adversities. However, I'm of the opinion that more effort should be geared at training the more cyber security agencies with modern approaches in the use of sophisticated technologies in upgrading their searches and findings as it relates to cyber security management in the country.

Researcher:

Do cyber security protocols in your country grant preferential and unfettered access to certain users to classified applications while others only have access to general-issued devices?

Interviewee:

Well, it all depends on the nature and purpose of the classified applicant or user. I believe, there are certain information that can't just be generalized or made accessible by every tom dick and harry but only made accessible by classified individuals. Based on these, preference is accorded on the nature,

type and purpose of the kind of information accessed by the classified applicant.

Researcher:

Do cyber security protocols in your country restrict application access to users operating corporate owned and self-managed devices?

Interviewee:

Well, as earlier pointed it all depends on the nature and purpose of the application. Every application comes with a definite purpose and what it stands to achieve. It is not every application that should be made available to every person be it corporate owned and/or self owned. Otherwise, in ability to theme or place restrictions on certain classified application may lead to unprecedented rise in cybercrime.

Researcher:

In your personal opinion, what's the percentage of users' who secure their cyber devices with a password?

Interviewee:

Virtually, with the constant rise in cybercrime in today's Nigerian digital economy, I believe there is barely any corporate and self managed device that is not under password. Almost every as we speak is aware of the menace of cybercrime and the damage cost it comes with.

Researcher:

Do cyber security protocols in your country engage and keep users informed on communicating information both about potential threats and about best practices with which to protect their assets?

Interviewee:

Yeah, in Nigeria there are efforts puts in place by cyber security agencies to engage and keep users informed on cyber threats and best practices to protect users' interest. Many anti-cyber security agencies e.g., EFCC and ICPC has a number of programs aired on TV and radio stations to create more levels of awareness and in some cases short text messages are sent to users handsets on steps to takes to prevent loss of vital information and guide against cyber perpetrators.

Researcher:

Do cyber security protocols in your country enable external devices based on the role of the user?

Interviewee:

Well, it all depends too on the nature of the external device in possession of the user. In my candid opinion, I believe the cyber security agencies must be aware of the existence of such device and the purpose for which such device is to be used and if possible, such device should be registered and granted users permission before accessed by the user.

Researcher:

What are your responses to the following sub questions to the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes as in the case of trust in this evolving complex digitalized economy as both corporate and individual users hands-off/outsource their cyber assurance in terms of monitoring, managing and safeguarding highly sensitive information internally to cyber security protocols regarded as "third party" in your country?

Interviewee:

Roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes

Questions	Yes	No	Not sure
Do you think as a matter of urgency a vast population of users (corporate and individuals) outsource and manage their IT and security infrastructure through service partners?	√		
Do you think a vast percentage of users (corporate and individuals) security needs are well protected and managed effectively by existing service partners?			√
Do you think more than forty-five percent users (corporate and individuals) outsource less than 20 percent of their security functions to a third party?	√		
Do you think not less than twenty five percent users (corporate and individuals) handle the bulk of their IT security internally but do enlist the help of consultants for support?	√		
Do you think users (corporate and individuals) seek outside help to fill in resource and knowledge gaps in their security resources and meet critical compliance and security demands?	√		
Do you think users (corporate and individuals) turn to external managed security service providers for a fairly broad spectrum of needs, ranging from tactical device monitoring to more strategic areas where they may lack the institutional knowledge?	√		
Do you think due to the fast evolving digital economy and mitigate any damage following cyber attacks most users (corporate and individuals) would prefer to manage their compliance needs in-house?			√
Do you think only very few users would use third parties for governance, risk and compliance management support?			√

ANNEXE No3.

INTERVIEWS TRANSCRIPT

Interviewee No2

Date of the interview: 5. 4. 2022
Interviewee name: Undisclosed.
The researcher: Rasheed Odejayi
Location: Ateitiesst. 20, LT-08303 Vilnius
Interview type: e-mail

Researcher:

Could you please provide as much information as possible about yourself concerning the topic of the study? Cadre, experience (can be general information only, such as job position and type of company, no name indicated)
How much experience do you have in cyber security?

Interviewee:

I have well over six years experience in cyber management. From the very onset of my employment, I was employed as a system programmer to manage the programming highly sensitive information of my organization; and over the years have acquired a number of knowledge in cyber security.

Researcher:

What is the situation of cybercrime and attacks in your country?

Interviewee:

At present, the circumstances surrounding the cybercrime in Nigeria is unequivocally alarming and very unprecedented as almost every potential youth the country is suspected to be cyber perpetrator.

Researcher:

Given the informant below, based on the previous and current nature, types and trend of cybercrime in your country, what would be your assessment within 2020 and 2021?

Interviewee:

Incidents	Jan (2021)	Jan (2022)	Increase /decrease
Online scams	3452	4321	869
Fraud	2633	3553	920
Intrusion	1423	2488	1065
Spam	1234	3222	1988
Malicious code	3452	4581	1129
Cyber harassment	3213	4532	1319
Ransomware	3411	4343	932
Botnets	2314	3321	1007
Business email compromise	2343	3355	1012
Digital extortion	2423	3349	926
Hacking	4534	6587	2053
Phishing	1236	2635	1399
Data breach	1343	2512	1169
Malware	2742	3442	700
Website cloning	3002	5534	2532
Viruses	3271	5656	2385

Researcher:

Who do you think are major perpetrators and victims of the cybercrimes?

Interviewee:

I strong believe that majority of the cybercrime perpetrators are the unemployed youths and anyone who wants to be rich over night. And the victims are individuals, households, business corporations and the society at large.

Researcher:

What do you think is the major motive behind cybercrimes (is it political or economical)?

Interviewee:

Basically, I believe state of poverty in the Nigeria and laziness backed with get rich quick syndromes are the major motives behind anyone engaging in cybercrimes.

Researcher:

Are there cyber security protocols monitoring and managing cyber activities and/or crimes in your country?

Interviewee:

Yes to a reasonable extent, there are a number of cyber security protocols monitoring and managing cyber activities in Nigeria.

Researcher:

Can you mention the cyber security protocols already established and in operation in your country?

Interviewee:

To my best of knowledge in Nigeria we the Economic and Financial Crimes Commission (EFCC) Independent Corrupt Practices Commission (ICPC), Public Complaints Commission (Ombudsman) (PCC) and so many others.

Researcher:

Do cyber security protocols in your country have direct control and authorized backing to checkmate, prosecute and punish cyber offenders?

Interviewee:

Yes with 100 percent backing of the law, the already established cyber security protocols in Nigeria have adequate authorization and full control to checkmate, monitor, prosecute and arraign before the court of law anyone persons suspected and/or found guilty of cyber offense.

Researcher:

What is the position of the established laws of cyber security protocols on cyber offenders in your country?

Interviewee:

Anyone found or suspected to be guilty of cybercrime is arrested by any of acclaimed cyber security protocol: and arraign and prosecuted in the court of law where adequate judgment in form of punishment is be delivered on alleged offender.

Researcher:

Are the established laws strong enough to serve as deterrents to combat cybercrimes in your country?

Interviewee:

Although, to an extent I will admit yes, however, there need for more stringent measures as means to effectively deter cybercrime and offenders in the country (Nigeria) can't be overemphasized; because despite all of the established laws

and delivered justice on the fight against cybercrime, the surge in cybercrime and offenders has consistently being on the increase.

Researcher:

Do cyber security protocols in your country engage tracking devices to checkmate and monitor users operating corporate owned and self-managed devices?

Interviewee:

Yes, to a reasonable extent, the cyber security protocols in Nigeria oftentimes engage the use of tracking device to checkmate and monitor users operating corporate owned and self-managed devices.

Researcher:

Do cyber security protocols in your country perform security drills on a periodic basis to make sure that users are prepared to mitigate the impact of cyber attacks?

Interviewee:

Yes, on a regular basis, the cyber security protocols in my country do perform security drill exercise to mitigate the impact of cyber attacks; through these medium a number of illicit cyber offenders have been caught and arraigned before the court of law.

Researcher:

Do cyber security protocols in your country grant preferential and unfettered access to certain users to classified applications while others only have access to general-issued devices?

Interviewee:

Yes, however, such preferential grants and unfettered access to certain users to classified applications by cyber security protocols only happens on special cases; particularly, where such access to classified applications is consequential at aiding further investigations into nabbing cyber offenders.

Researcher:

Do cyber security protocols in your country restrict application access to users operating corporate owned and self-managed devices?

Interviewee:

Yes, based on discretion, cyber security protocols in my country oftentimes restrict application access to users operating corporate owned and self-managed devices; these has help to safeguard undue access to highly classified and

verified data by unauthorized and un-trusted users be it corporate owned and self-managed devices.

Researcher:

In your personal opinion, what's the percentage of users' who secure their cyber devices with a password?

Interviewee:

Well, in my personal views, my rating in percentage of users' who secure their cyber devices with a password is 55 to 65 percent.

Researcher:

Do cyber security protocols in your country engage and keep users informed on communicating information both about potential threats and about best practices with which to protect their assets?

Interviewee:

Yes, the cyber security protocols in my country often engage a number of measures and efforts in educating, informing and creating more awareness to corporate and individual users on best possible ways to guide against externalities informs of cyber threat and also maximize their cyber security within the digital space.

Researcher:

Do cyber security protocols in your country enable external devices based on the role of the user?

Interviewee:

Well, I am not so sure about that, however, I believe such grant on the use of any external devices by cyber security protocols to a user for whatsoever purpose would go through a series of scrutiny and assessment before permission is granted.

Researcher:

What are your responses to the following sub questions to the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes as in the case of trust in this evolving complex digitalized economy as both corporate and individual users hands-off/outsource their cyber assurance in terms of monitoring, managing and safeguarding highly sensitive information internally to cyber security protocols regarded as "third party" in your country?

Interviewee:

Roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes

Questions	Yes	No	Not sure
Do you think as a matter of urgency a vast population of users (corporate and individuals) outsource and manage their IT and security infrastructure through service partners?	√		
Do you think a vast percentage of users (corporate and individuals) security needs are well protected and managed effectively by existing service partners?			√
Do you think more than forty-five percent users (corporate and individuals) outsource less than 20 percent of their security functions to a third party?	√		
Do you think not less than twenty five percent users (corporate and individuals) handle the bulk of their IT security internally but do enlist the help of consultants for support?			√
Do you think users (corporate and individuals) seek outside help to fill in resource and knowledge gaps in their security resources and meet critical compliance and security demands?	√		
Do you think users (corporate and individuals) turn to external managed security service providers for a fairly broad spectrum of needs, ranging from tactical device monitoring to more strategic areas where they may lack the institutional knowledge?	√		
Do you think due to the fast evolving digital economy and mitigate any damage following cyber attacks most users (corporate and individuals) would prefer to manage their compliance needs in-house?			√
Do you think only very few users would use third parties for governance, risk and compliance management support?			√

ANNEXE No4.

INTERVIEWS TRANSCRIPT

Interviewee No3

Date of the interview: 6. 4. 2022
Interviewee name: Undisclosed.
The researcher: Rasheed Odejayi
Location: Ateitiesst. 20, LT-08303 Vilnius
Interview type: e-mail

Researcher:

Could you please provide as much information as possible about yourself concerning the topic of the study? Cadre, experience (can be general information only, such as job position and type of company, no name indicated)
How much experience do you have in cyber security?

Interviewee:

I have been on this job as a system and hub administrator for the past eight years and with my wealth of experience have been able to safeguard, manage and protect classified data in the interest of my organization and clientele relations.

Researcher:

What is the situation of cybercrime and attacks in your country?

Interviewee:

Currently, I would describe the state of cybercrime and attacks to be on the increase and many perpetrators conceives it as the most brilliant way to conveniently fraud individuals, firms and governmental resources.

Researcher:

Given the informant below, based on the previous and current nature, types and trend of cybercrime in your country, what would be your assessment within 2020 and 2021?

Interviewee:

Incidents	Jan (2021)	Jan (2022)	Increase /decrease
Online scams	1324	2273	949
Fraud	2533	3565	1032
Intrusion	1109	2874	1765
Spam	980	1634	654
Malicious code	2123	3334	1211
Cyber harassment	2251	3289	1038
Ransomware	2114	2674	560
Botnets	1532	2388	856
Business email compromise	1299	2652	1353
Digital extortion	1879	3423	1544
Hacking	3427	5662	2235
Phishing	2091	3444	1353
Data breach	1523	3721	2198
Malware	2874	4338	1464
Website cloning	2374	4445	2071
Viruses	3435	5432	1997

Researcher:

Who do you think are major perpetrators and victims of the cybercrimes?

Interviewee:

I believe everyone who possesses sound knowledge and skills in the use of computer; one who seeks easy way to be wealthy and probably unemployed or underemployed in the society.

Researcher:

What do you think is the major motive behind cybercrimes (is it political or economical)?

Interviewee:

I would admit the motive behind cybercrime in Nigeria is basically economical; and to a great extent it reflects on the state of poverty in the country and the state of weak orientation as presumed to be in circulation particularly among today's youths who by all means want to break out of the poverty line and become rich quick at any cost.

Researcher:

Are there cyber security protocols monitoring and managing cyber activities and/or crimes in your country?

Interviewee:

Of a truth, yes, there are a number of well established and efficient cyber security protocols monitoring and managing cyber activities and crimes in Nigeria.

Researcher:

Can you mention the cyber security protocols already established and in operation in your country?

Interviewee:

Currently, among the already existing ones that I am conversant with is the EFCC (Economic and Financial Crimes Commission), ICPC (Independent Corrupt Practices Commission), CCB (Code of Conduct Bureau), CBN (central bank of Nigeria) and PCC (Public Complaints Commission)

Researcher:

Do cyber security protocols in your country have direct control and authorized backing to checkmate, prosecute and punish cyber offenders?

Interviewee:

Yes, the mention cyber security protocols operating in Nigeria have the direct legal backing and authorization of the law to interfere, checkmate, arraign and prosecute cyber offenders before the court of law.

Researcher:

What is the position of the established laws of cyber security protocols on cyber offenders in your country?

Interviewee:

At the instance of concrete evidence by the cyber security protocols, offenders suspected to be engaged in cybercrimes are arrested forthwith, arraigned before the court of law and prosecuted accordingly to the provisions of the Nigerian Criminal Acts.

Researcher:

Are the established laws strong enough to serve as deterrents to combat cybercrimes in your country?

Interviewee:

From past verdicts on cases according to the provisions of the Nigerian Criminal Acts, I will admit that the established laws are solidly serving as deterrents to

combat cybercrimes in the country. However, there's need to establish more severe deterrents to totally discourage cybercrimes in the country.

Researcher:

Do cyber security protocols in your country engage tracking devices to checkmate and monitor users operating corporate owned and self-managed devices?

Interviewee:

True, several measures have been put in place by emerging cyber security protocols in Nigeria to combat cybercrimes in the country. The agencies have been able to design and adopt tracking measures (devices) that pitch red alert on illicit cyber acts regardless of the users' consent. This over the while has been able to effectively checkmate users' intention on the cyberspace.

Researcher:

Do cyber security protocols in your country perform security drills on a periodic basis to make sure that users are prepared to mitigate the impact of cyber attacks?

Interviewee:

Yes, I have been opportune to see a number of programs put in place by the cyber security protocols in sensitizing, informing and educating the users on the menace and consequences of cybercrime; and also proffering possible measure to overcome it once detected.

Researcher:

Do cyber security protocols in your country grant preferential and unfettered access to certain users to classified applications while others only have access to general-issued devices?

Interviewee:

I am not sure about that, but I think if such grant and access to classified applications would given to a user, then it should be at the agencies discretion being fully aware of the intent and purpose for such request to be granted.

Researcher:

Do cyber security protocols in your country restrict application access to users operating corporate owned and self-managed devices?

Interviewee:

Yes, I believe not all applications are made accessible by users operating either a corporate owned or self-managed devices because not data can be accessed. There should be a kind of restriction placed on data or applications that are classified as highly sensitive data.

Researcher:

In your personal opinion, what's the percentage of users' who secure their cyber devices with a password?

Interviewee:

In my personal views of users' who secure their cyber devices with a password, my rating will be 55 to 60percent.

Researcher:

Do cyber security protocols in your country engage and keep users informed on communicating information both about potential threats and about best practices with which to protect their assets?

Interviewee:

Yes, cyber security protocols often engage series of communication channels to create a level of awareness to keep users informed about potential threats and possible practices to protect their data and classified information.

Researcher:

Do cyber security protocols in your country enable external devices based on the role of the user?

Interviewee:

I am not so sure about that, but if there be need for such I believe there must have been some sort of communication and negotiation between the user of the external device and the security protocols before such permission would be granted.

Researcher:

What are your responses to the following sub questions to the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes as in the case of trust in this evolving complex digitalized economy as both corporate and individual users hands-off/outsource their cyber assurance in terms of monitoring, managing and safeguarding highly sensitive information internally to cyber security protocols regarded as "third party" in your country?

Interviewee:

Roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes

Questions	Yes	No	Not sure
Do you think as a matter of urgency a vast population of users (corporate and individuals) outsource and manage their IT and security infrastructure through service partners?	√		
Do you think a vast percentage of users (corporate and individuals) security needs are well protected and managed effectively by existing service partners?			√
Do you think more than forty-five percent users (corporate and individuals) outsource less than 20 percent of their security functions to a third party?			√
Do you think not less than twenty five percent users (corporate and individuals) handle the bulk of their IT security internally but do enlist the help of consultants for support?			√
Do you think users (corporate and individuals) seek outside help to fill in resource and knowledge gaps in their security resources and meet critical compliance and security demands?	√		
Do you think users (corporate and individuals) turn to external managed security service providers for a fairly broad spectrum of needs, ranging from tactical device monitoring to more strategic areas where they may lack the institutional knowledge?	√		
Do you think due to the fast evolving digital economy and mitigate any damage following cyber attacks most users (corporate and individuals) would prefer to manage their compliance needs in-house?	√		
Do you think only very few users would use third parties for governance, risk and compliance management support?	√		

ANNEXE No5.

INTERVIEWS TRANSCRIPT

Interviewee No4

Date of the interview: 8. 4. 2022
Interviewee name: Undisclosed.
The researcher: Rasheed Odejayi
Location: Ateitiesst. 20, LT-08303 Vilnius
Interview type: e-mail

Researcher:

Could you please provide as much information as possible about yourself concerning the topic of the study? Cadre, experience (can be general information only, such as job position and type of company, no name indicated)
How much experience do you have in cyber security?

Interviewee:

I'm employed on this job as a data and system analyst and with my acquired skills, I have consistently been able to process, protect and manage the inflow and out flow data base for effective decision making purpose in my organization.

Researcher:

What is the situation of cybercrime and attacks in your country?

Interviewee:

The state of cybercrime in Nigeria is worst, very disserting and I am of the candid opinion that it should be out rightly discouraged.

Researcher:

Given the informant below, based on the previous and current nature, types and trend of cybercrime in your country, what would be your assessment within 2020 and 2021?

Interviewee:

Incidents	Jan (2021)	Jan (2022)	Increase /decrease
Online scams	2342	4453	2111
Fraud	3254	5343	2089
Intrusion	1226	3211	1985

Spam	1028	2382	1354
Malicious code	2411	3172	761
Cyber harassment	3442	5452	2010
Ransomware	1083	2338	1255
Botnets	1192	2874	1682
Business email compromise	2488	3612	1124
Digital extortion	2309	3234	925
Hacking	3249	5783	2534
Phishing	2854	4776	1922
Data breach	2932	3437	505
Malware	1092	2333	1241
Website cloning	2763	3499	736
Viruses	3523	5734	2211

Researcher:

Who do you think are major perpetrators and victims of the cybercrimes?

Interviewee:

In my own point of view, I believe youths are the major perpetrators of cybercrime and they should be held accountable for these malicious acts.

Researcher:

What do you think is the major motive behind cybercrimes (is it political or economical)?

Interviewee:

I strongly believe laziness, covetousness, greed coupled with the state of unemployment are the major motives fostering cybercrimes in Nigeria. To me, I believe it is more of economical problem than the political.

Researcher:

Are there cyber security protocols monitoring and managing cyber activities and/or crimes in your country?

Interviewee:

Sure, there are a number of cyber security protocols managing and prosecuting cyber offenders in Nigeria.

Researcher:

Can you mention the cyber security protocols already established and in operation in your country?

Interviewee:

Among the existing ones in Nigeria, are majorly the Economic and Financial Crimes Commission (EFCC) and also the Independent Corrupt Practices Commission (ICPC).

Researcher:

Do cyber security protocols in your country have direct control and authorized backing to checkmate, prosecute and punish cyber offenders?

Interviewee:

Yes, they both have the full backing and support of the Nigeria legal system as enshrined within the jurisdiction of the Nigerian Criminal Acts as amended.

Researcher:

What is the position of the established laws of cyber security protocols on cyber offenders in your country?

Interviewee:

The cyber security protocols are solely charged with the responsibility of detecting, arresting and arraign of cyber offenders for persecution before an accredited court of law in Nigeria.

Researcher:

Are the established laws strong enough to serve as deterrents to combat cybercrimes in your country?

Interviewee:

Well, I will admit yes to a reasonable extent but I believe more efforts and measures should still be enacted in the laws guiding against any form of cyber criminality and such as it will totally become impossible for anyone to perpetrate cybercrime in the country.

Researcher:

Do cyber security protocols in your country engage tracking devices to checkmate and monitor users operating corporate owned and self-managed devices?

Interviewee:

Well, based on my profession, I have been opportune to seen a couple of tracking devices and software's engaged by the cyber security agencies in monitoring users operating corporate owned and self-managed devices in the country.

Researcher:

Do cyber security protocols in your country perform security drills on a periodic basis to make sure that users are prepared to mitigate the impact of cyber attacks?

Interviewee:

Yes, they do. I have witnessed a couple of security drills on a periodic basis solely engaged to educate and prepare population of users in reducing and combating cybercrimes in the country.

Researcher:

Do cyber security protocols in your country grant preferential and unfettered access to certain users to classified applications while others only have access to general-issued devices?

Interviewee:

Well, to my best of knowledge, I would say yes; because not all application should be made accessible regardless of the personality involved due to the nature of data sensitivity. However, I believe access to such classified applications should only be accessed on preferential basis by users with permit lenience.

Researcher:

Do cyber security protocols in your country restrict application access to users operating corporate owned and self-managed devices?

Interviewee:

Well, just as explained earlier, I am still of the opinion that restriction of access to certain application by users operating either corporate owned and self-managed devices should be based on preference with permit lenience. This will help the cyber security protocols to monitor and have an adequate stream of data base of persons accessing the so called 'classified data".

Researcher:

In your personal opinion, what's the percentage of users' who secure their cyber devices with a password?

Interviewee:

Well, I will admit a ratio of 75 to 85percent; because people these days are very conversant and are much aware of the state of cybercrimes in the country.

Researcher:

Do cyber security protocols in your country engage and keep users informed on communicating information both about potential threats and about best practices with which to protect their assets?

Interviewee:

Yes, they do, even of periodic basis; and this have helped in sensitizing an average Nigerian perceptive on the position of cyber threats and how it can be curtailed and/or combated.

Researcher:

Do cyber security protocols in your country enable external devices based on the role of the user?

Interviewee:

Well, I am not so clear on that, I might not be able to proffer answer in that light.

Researcher:

What are your responses to the following sub questions to the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes as in the case of trust in this evolving complex digitalized economy as both corporate and individual users hands-off/outsource their cyber assurance in terms of monitoring, managing and safeguarding highly sensitive information internally to cyber security protocols regarded as "third party" in your country?

Interviewee:

Roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes

Questions	Yes	No	Not sure
Do you think as a matter of urgency a vast population of users (corporate and individuals) outsource and manage their IT and security infrastructure through service partners?	√		
Do you think a vast percentage of users (corporate and individuals) security needs are well protected and managed effectively by existing service partners?	√		
Do you think more than forty-five percent users (corporate and individuals) outsource less than 20 percent of their security functions to a third party?	√		
Do you think not less than twenty five percent users (corporate and individuals) handle the bulk of their IT security internally but do enlist the help of consultants for support?	√		
Do you think users (corporate and individuals) seek outside help to fill in resource and knowledge gaps in their security resources and meet critical compliance and security demands?	√		

Do you think users (corporate and individuals) turn to external managed security service providers for a fairly broad spectrum of needs, ranging from tactical device monitoring to more strategic areas where they may lack the institutional knowledge?	√		
Do you think due to the fast evolving digital economy and mitigate any damage following cyber attacks most users (corporate and individuals) would prefer to manage their compliance needs in-house?	√		
Do you think only very few users would use third parties for governance, risk and compliance management support?	√		

SUMMARY

This research work has empirically investigated the security impact of cyber security management on digital economy across sub-Saharan African countries using Nigeria and Cameroon as a case study. To achieve these main objectives, the study considered three specific objectives such as examining the past and current trend of cyber crimes perpetrated in the digital economy of the selected sub-Saharan African countries; examining the nature and types of cyber security protocols and already established laws in combating cyber crimes in the digital economy of the selected sub-Saharan African countries; and also evaluating the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes in the digital economy of the selected sub-Saharan African countries.

To further enhance a better analysis, the study was restricted to two selected sub-Saharan African countries using Nigeria and Cameroon as a case study. The research design adopted for this study was descriptive research design. In that it enabled the use of primary sources of data as it key and first hand evidence. The researcher made use of both the qualitative and quantitative method of research in order to be able to draw a valid and reliable conclusion.

The population of this study comprised of a host of respondents such as military and paramilitary security personnel in Nigeria and Cameroon; *researchers* of research institutes and *agencies handling security issues* in Nigeria and Cameroon; *academicians* (professors) of recognized universities in Nigeria and Cameroon; and as well as *personnel(s) in private setups such as banks*, telecommunication industries etc, in Nigeria and Cameroon.

For the purpose of this study a total of 60 sample size was selected from the study population and were administered copies of the semi-structured interview questionnaire. However, only 54 copies of the semi-structured interview questionnaire were correctly and completely responded to by the sampled respondents and were returned and collated by the researcher for data analysis. All the participants were selected and interviewed directly online through the use of semi-structured interview questionnaire. The semi-structured interview checklist was developed and generalized upon two fundamental constructs with the motive to identify the nature and types of cyber security protocols and already established laws in combating cyber crimes in the digital economy of the selected sub-Saharan African countries; and the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cyber crimes in the digital economy of the selected sub-Saharan African countries.

Finally, data obtained in the course of the study were grouped into themes and analyzed using content analysis in which the previously existing literatures were analyzed in relation to the findings of this work and the application of the theoretical framework for conclusion and findings.

Rasheed Odejayi (2022), *Cyber security management: security impact on digital economy across sub- saharanafrica countries.* (Master Thesis). Vilnius: Mykolas Romeris University

ANNOTATION

This Master's Thesis has thoroughly considered security impact of cyber security management on digital economy across sub-Saharan African countries using Nigeria and Cameroon as a case study. The first chapter critically reviewed the concept of digital economy within the context of cybercrime and security management. It considered the different types of cybercrimes of perpetrated and the problems associated with it. Also, the chapter considered the motives initiating such attacks e.g., incentives. In addition, the chapter also emphasized on the uncertain times, unsettled lives on how it shapes cyber ethics for the future in a transforming world we live in a world of worry as it gives credence to digital technologies and threats to human security. In the second chapter, the substantiation of the research methodology is performed, which was used in the research part. In the third part, empirical data generated by the researcher were analysis and discussed using both qualitative and quantitative methods with the using of content analysis. The obtained indicators revealed a high prevalence of cyber perpetration and attacks on the digital economies of Nigeria and Cameroon. It is therefore of most importance to bare to heart that this phenomenon "cyber insecurity" is not a new concept in everyday living and social exchanges but everyone in the Internet of Things (*IoTs*) must adequate and constructive cyber measures across sub-Saharan African countries in the corporate fight against all forms of cyber insecurity. Also, it is most paramount to note that the concept cyber insecurity is a most fight for all whether advanced, developing or less developed countries in any part of the globe. It can also be likened to technological epidemic (outbreak) that most be eradicated otherwise it may see the end of many digital economies across the globe. Results, findings and discussions generated by this study has future consequences in the fight against cyber insecurity both in the private and public global digital space and it makes provision on corporate insight in tackling it menace thereof.

K**ey words:** Cyber Insecurity, Cyber Management, sub-Saharan African Countries, Digital Economy, Internet of Things.