Information Systems and Cyber Security for Sustainable Development in Nigeria

Oluwatoyin Taiwo BANJO
oluwatoyinbanjo@gmail.com;+2348066838211
Department of Mass Communication and Media Technology
Lead City University, Ibadan, Oyo State, Nigeria.

Abstract

This study examines Information Systems and Cyber Security for Sustainable Development in Nigeria. Increased internet penetration has brought with it challenges such as cyber security and digital privacy issues. Addressing these issues in a way that protects the tremendous economic and social values that information technology presents, without stifling innovation, requires a fresh look at the enhanced sustainable development goals of the United Nations. The study made use of a survey research design in which 105 respondents who were IT professionals and cyber security experts were administered questionnaires.Data analysis was done using SPSS version 25.0. The findings showed that cyber-security, data regulation and sustainability are the key to the digital transformation processes in the coming years. Also, further findings revealed that the development of environmental technologies along with their cyber-security is one of the aims of the realization of sustainable production and domestic security concepts. The study recommends the need for improved cyber-security strategies, policies, and programs.

Keywords Cyber-attack, Cyber security, Sustainable Development, E-commerce, Online Transactions

Introduction

Communication is very essential in day-to-day activities. Over the years the pattern of communication has evolved. The advent of Information and communication technologies have brought dramatic changes in the way people communicate with others, the way they work, as well as the way organizations do business. The ability to digitize information and to exchange them with anyone around the world via electronic devices now enables humans to connect globally. Such technologies allow people to share information immediately and expansively as 21st century organizations are now more interconnected through file sharing, blogs, and social networking sites, to name a few[1].

The rise of technology and online communication has not only produced a dramatic increase in the incidence of cyber insecurity and digital privacy issues, but has also resulted in the emergence of what appears to be a new variety of threat to the attainment of sustainable development of information and communication technology in Nigeria. Both the increase in the incidence of cyber insecurity and digital privacy invasion and the possible threat to the role

of information technology and to the attainment of sustainable development poses challenges for the larger internet users, as well as for law enforcement agents[2].

Impressive leverages of information and communication technologies (ICT) allow efficient exchanges of data, streamlining of operations, virtualization of numerous products and services, and the adoption of diverse electronic payment methods. These, in turn, create conditions for the emergence of new trade approaches, models, functionalities, and, potentially, new sales channels and markets.

The 2030 Agenda for Sustainable Development highlights the importance of information and communication technologies (ICT) and global interconnectedness as powerful enablers of growth, to accelerate human progress, to bridge the digital divide and to develop knowledge societies[3]. Sustainable development leads to fulfillment of societal ideals considered relevant to the needs and aspirations of the society. Factors, which influence such developments, are based on human ability to explore, invent, and utilize.
Reference to information and communication technology can be found explicitly as a target under SDG goal 9 which states that "Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation"

Statement of the Problem

Privacy and security of data will always be top security measures that any organization takes care of. The present world is a world where all the information is maintained in a digital or a cyber form. Cybercriminals continue to target social media sites to steal personal data. Not only for social networking but also during bank transactions required security measures must be taken. Over the past twenty years, immoral cyberspace users have continued to use the internet to commit crimes; this has evoked mixed feelings of admiration and fear in the general populace along with a growing unease about the state of cyber and personal security. This phenomenon has seen sophisticated and extraordinary increase recently and has called for quick response in providing laws that would protect the cyber space and its users.

However, one of the goals of Sustainable development is to build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation. The goal of the SDG is to ensure that there is cyber peace and this makes cyber security to be very essential in our daily living. Also, to protect cyber space from cyber criminals and prevent unauthorized access to government, organizational and personal information. Therefore, this study examines Information Systems and Cyber Security for Sustainable Development in Nigeria.

Aim and Objectives of the Study

The Primary aim of this study is to examine Information Systems and Cyber Security for Sustainable Development in Nigeria. The secondary objectives are to:

i. examine the relevance of information systems and cyber security for sustainable development in Nigeria.
ii. access the communication challenges of cyber security

Research Question

i. To what extent is information systems and cyber security relevant to sustainable development in Nigeria?
ii. What are the communication challenges of cyber security?

Hypothesis

H_0**:** There is no significant impact ofinformation systems and cyber security on sustainable development

Literature Review

Cyber Security

Cyber security refers to a set of techniques used to protect the integrity of networks, progra ms, and data from attack, damage, or unauthorized access. Cyber security is the protection of computer systems and networks from attack by malicious actors that may result in unauthori zed information disclosure, theft of, or damage to hardware, software, or data, as well as fro m the disruption or misdirection of the services they provide[4]. It is the protection of Internet connected systems, including hardware, software, and data from cyberattacks. It is made up of two words one is cyber and the other is security. Cybersecurity is a process that's designe d to protect networks and devices from external threats. Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productiv ity, and enhance customer confidence in products and services. Cyber Security involves prot ecting key information and devices from cyber threats. It is a critical part of companies that collect and maintain huge databases of customer information, social platforms where person al information is submitted, and government organizations where secret, political, and defens e information are involved. It describes how personal and key government data is protected

against vulnerable attacks that possess threats to important information, may it be on the cloud, or across various applications, networks, and devices.

Information System

Information System are integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products. An information system (IS) is an interconnected set of components used to collect, store, process and transmit data a nd digitalinformation[5]. At its core, it is a collection of hardware, software, data, people and p rocesses that work together to transform raw data into useful information. Business firms an d other organizations relyon information systems to carry out and manage their operations, i nteract with their customers and suppliers, and compete in the marketplace. Information syst ems are used to run inter-organizational supply chains and electronic markets[6]. For instance, corporations use information systems to process financial accounts, t o manage their human resources, and to reach their potential customers with online promotio ns. Many major companies are built entirely around information systems.

Sustainable Development

Sustainable development is means to balance the needs of the present and future generations without compromise. The concept of sustainability means a capacity to maintain some entit y, outcome or process over time. The concept of sustainability connotes improving and susta ining a healthy economic, ecological and social system for human development[3]. Sustainability is a dynamic equilibrium in the process of interaction between t he population and the carrying capacity of its environment such that the population develops to express its full potential without producing irreversible adverse effects on the carrying capacity of the environment upon which itdepends[7]. Sustainable developmen t refers to the development agenda that can be initiated and maintained by either government or nongovernment organisations which aimed at meeting the pressing needs of the present ge neration without having any detrimental effecton the incoming generations. Sustainable deve lopment is the type of development which meets the basic needsofdisadvantaged group in ter ms of provision of employment, food, energy, water, housing, manufactures, power and serv ices. The environment, the society and the economy as three phases to sustainable developm ent and the wellbeing of the people would depend on effective interwoveness of these components[8]. For instance, it is hoped that a healthy and prosperous society is a function of healthy environment to provide necessary resources for it's citizen to survive and excel in all

ramifications. In the light of this, sustainable development is expected to give people in ever y part of the world the support they need to lift themselves out of poverty in all its manifesta tions.

Cyber-security Risks

The security risk presents several components or dimensions, one of the most concerning is t he cybersecurity risk. The high level of interconnectivity, which characterizes modern societ y and theinternational trade, has opened many avenues for cyber attacks, rendering cybersec urity an issue of major concern for all organizations[9]. Even though, in recent years, there we re notable advances in the understanding and mitigation of cyber risks, as empirical data sho ws, the number of incidents augmented and continued to grow in sophistication, becoming m ore thorough and inflicting often majorlosses[10]. Through advanced tools, tactics and procedu res (TTP), such as SQL injection; malware infection; advertisement click fraud; business em ail compromise (BEC); and exploitation of zeroday vulnerabilities, used in watering hole att acks, cyber criminals pose major threats to organizations and citizens. Cyber incidents have t he potential to negatively affect organizations' activity, economic development, and users' p rivacy and other fundamental rights.

Risk Communication

Risk communication is a relatively mature field and has been researched in detail for many y ears, especially within the health and natural disaster domains. Risk communication can be d efined as the interactive process of exchanging information about a risk (its nature, meaning, consequences, likelihood and response options) to individualsso that they can make informe djudgements[11]. This activity can be split into three goals, advancing/changing knowledge an d attitudes, modifying risk relevant behaviour, and facilitating cooperative conflict resolution and decision making . All of these goals require individuals to initially consume risk informa tion or in other words, perceive it. As a result, risk perception forms one of the critical initial stages within risk communication that considers the ways in which a person actually views a risk and the various factors that affect their perspective. Some of the other processes core t o risk communication which are implicit to the goals mentioned above are risk analysis, risk evaluation and risk treatment.

The Communication of Cybersecurity Risks

To reiterate, risk communication in the cybersecurity context considers how best to commun icate security risk information to users of a system in order to facilitate understanding and pr omote informed judgement. In some cybersecurity situations, persuading users to adopt a par ticular course of action may also be the goal. Research in the security communications space is relatively new and at this stage may be broken into work on perception of security risks a nd decision-making regarding these risks—this somewhat mirrors early work in the risk-communications[12].

Communication Challenges of Cyber security

No matter the cause of the cyberattack, having to contact stakeholders (i.e., employees, stock holders, and customers) to tell them your organization has lost their data is not only a difficu lt exercise but also one that holds a potentially significant reputational risk. This reputation r isk is especially true considering how quickly and easily information is shared on social media. When considering cybersecurity, organizations need to keep the communica tions elements in mind before, during, and after a cyberattack.

i. Cybersecurity requires a culture of risk.

Benjamin Franklin is often credited as saying, "By failing to prepare, you are preparing to fa il". Operating in a culture of risk means that the company's default expectation should be th at it is at risk of losing its reputation. Additionally, organizations should conduct a risk asses sment to identify the level of risk, in relation to cyberattacks, that they are willing to tolerate . Not all organizations are the same, so levels of tolerance are different and subsequently so are levels of cybersecurity.

With trust and loyalty of stakeholderson the line, risk assessment and crisis plans need to ad dress stakeholder engagement in the event of a data breach. Additionally, given the frequent changes in technology, crisis plans should be updated regularly. Mock tests or simulations of plans are an excellent way to work toward being prepared. All plans should be fully aligned with IT's operational cybersecurity plan and the business continuity plan. The role of comm unications should be included in all plans so expectations are clear and will not need to be d eveloped or negotiated in the middle of a cyber attack crisis.

ii. Cyber security should not be "owned" by any department.

By having a seat at the executive table, members from IT, legal, production, communication s, compliance, and all other departments can work together to identify possible warning sign als. In isolation a singular odd situation may seem just odd, but when considered with other odd situations the oddity may indicate a reason for concern. As such, frequent cross departm ent meetings with company boards and senior management teams can serve as an excellent e arly warning system. Additionally, having multiple departments and individuals working tog ether can help provide a more consistent application of policies.

iii. The public shares some level of cybersecurity responsibility.

Many security experts believe that the weakest link in cybersecurity is humans. In fact, some data breaches are the result of human error. Aside from the errors made (intentionally or uni ntentionally) in or on behalf of a company, many cyberattacks are the result of individuals m aking a mistake. While it is highly likely that many people understand that there are risks wi th being online, it is possible that many do not know what their role is. Unless someone has personally been impacted or knows someone close that has, for example, had their identity st olen, he or she is unlikely to really understand. As such, cybersafety can be considered a top ic that is subject to education gap. If individuals better understood how their actions in social media and online place them at risk, some of the cyberattacks may be easier to prevent.

Theoretical Review

Technology Acceptance Model

The technology acceptance model (TAM) is an information systems theory that models how users come to accept and use a technology. It was developed by Fred Davis and Richard Bagozzi[13]. The actual system use is the endpoint where people use the technology. Behavior al intention is a factor that leads people to use the technology. The behavioral intention (BI) is influenced by the attitude (A) which is the general impression of the technology. The mod el suggests that when users are presented with a new technology, a number of factors influen ce their decision about how and when they will use it, notably: Perceived usefulness (PU) – This was defined by Fred Davis as "the degree to which a person believes that using a parti cular system would enhance their job performance". It means whether or not someone percei ves that technology to be useful for what they want to do. Perceived ease-of-use (PEOU) –

Davis defined this as "the degree to which a person believes that using a particular system would be free from effort". If the technology is easy to use, then the barriers conquered. If it's not easy to use and the interface is complicated, no one has a positive attitude towards it.

Empirical Reviews

A systematic review on Human-Human Communication in Cyber Threat Situations was carried out in Norway[14]. In cyber threat situations, decisionmaking within organizations and between the affected organization and external entities are highstake situations. This require human communication entailing technical complexity, time pressure, interdisciplinary, and often insufficient information basis. The aims of this study are to (1) outline how human human communication performance in cybersecurity settings have been studied; (2) to uncover areas where there is potential for developing common standards for information exchange in collaborative settings, and; (3) to provide guidance for future research efforts. The review was carried out according to the PRISMA guidelines and articles were searched for on Google Scholar, ScienceDirect, Taylor & Francis, and IEEE. Primary research articles and reviews focusing on human human communication in cyber threat situations published in peer reviewed journals or as conference papers were included. A total of 17 studies were included in the final review. Most of the studies were correlational and exploratory in nature. Very few studies characterize communication in useful goal-related terms.

A comprehensive study on cyber attacks and cyber security; emerging trends and recent developments was conducted in China[15]. Today's world is highly dependent on electronic technology, and protecting this data from cyber attacks is a challenging issue. The purpose of cyber attacks is to harm companies financially. In some other cases, cyber attacks can have military or political purposes. Some of these damages are: PC viruses, knowledge breaks, data distribution service (DDS) and other assault vectors. The aim of this study is to survey and comprehensively review the standard advances presented in the field of cyber security and to investigate the challenges, weaknesses and strengths of the proposed methods. Different types of new descendant attacks are considered in details. Standard security frameworks are discussed with the history and early generation cyber security methods. In addition, emerging trends and recent developments of cyber security and security threats and challenges are presented. It is expected that the comprehensive review study presented for IT and cyber security researchers will be useful.

A study on Information Security: an effective tool for Sustainable Nigerian National Securit y and Development was conducted in Nigeria[16]. An effective information security strategy w ould be the best measure to adopt to tackle the insecurity challenges faced by Nigeria which as well obstructs its potentials to drive a sustainable national security and development. The study adopted a narrative literature review methodology. The study defines those effective in formation security measures and strategies to be adopted as a tool to attain the desired said i nformation security goal. The study concludes that these measures and strategies will be effe ctive for sustainable Nigerian national security and development. Nevertheless, the study pro vides recommendations that will enhance sustainable Nigerian national development through adopting these information security measures.

Research Methodology

This study made use of a survey research design. This method is best suited for studies that have individual people as the unit of analysis. They can have multiple purposes, and researc hers can conduct it in many ways depending on the methodology chosen and the study's goa l

The population of this study are cyber security experts and IT professionals.
A total number of 105 cyber security experts and IT professionals were selected from this st udy from online communities and social media platforms. The study made use of a purposiv e sampling method.
The research questionnaire was used as the research instrument and data was analyzed using SPSS software version 25.0. The descriptive statistics such as frequencies, percentages for a nalyzing demographic characteristics of respondents while hypothesis was analyzed using M ultiple Regression Analysis.

Data Analysis

Table 1: Socio-Demographic Characteristics of Respondents

Gender of Respondents	Frequency	Percent
Male	58	55.4
Female	47	44.6
Age (Years)		
Less than 25 years	7	6.7
26-35 years	46	43.8

36-45 years	40	38.1
46-55 years	12	11.4
Education		
OND	10	9.5
Professional Certification	34	32.4
BSC/HND	46	43.8
Postgraduate	15	14.3
Job Title		
Cyber security experts	43	40.9
IT Professionals	62	59.1
Total	**105**	**100.0**

Table 1 shows that 58(55.4%) of the respondents are male, 47 (44.6%) are female. Also, 46 (43.8%) of the respondents are within the age category of 26-35 years, 40 (38.1%) are within the age category of 36-45 years, 12(11.4%) are within 46-55 years. Furthermore, 46 (43.8%) of the respondents have First degree educational qualification (BSC/HND), 34 (32.4%) have Professional certificate, 15 (14.3%) have Postgraduate degree while 10 (9.5%) have OND certificate. Also, 43 (40.9%) of the respondents are Cyber security experts while 62 (59.1%) are IT professionals.

Research Question One: To what extent can information systems and cyber security be utilized for sustainable development in Nigeria?

Table 2: The extent at which information systems and cyber security are relevant to sustainable development in Nigeria

Statement	SA	A	D	SD	Mean	Stand Dev
Cyber-security, data regulation and sustainability are the key to the digital transformation processes in the coming years	43 (40.9%)	58 (55.2%)	4 (3.9%)	-	3.46	2.17

The development of environmental technologies along with their cyber-security is one of the aims of the realization of sustainable production and domestic security concepts	48 (45.7%)	56 (53.4%)	1 (0.9%)	-	2.69	1.81
Information system is the acclaimed engine room of modern day global development and sustainable growth	39 (37.1%)	61 (58.1%)	3 (2.9%)	2 (1.9%)	3.07	2.43
Cyber security ensures the protection of cyber space, data and information for sustainable growth and development	51 (48.6%)	53 (50.5%)	1 (0.9%)	-	3.73	2.64

Source: Field work, 2023

Table 2 shows that 43 (40.9%) of the respondents strongly agree, 58 (55.2%) agree while 4 (3.9%) disagree that Cyber-security, data regulation and sustainability are the key to the digital transformation processes in the coming years, 48 (45.7%) of the respondents strongly agree, 56 (53.4%) agree while 1 (0.9%) disagree that the development of environmental technologies along with their cyber-security is one of the aims of the realization of sustainable production and domestic security concepts, 39 (37.1%) of the respondents strongly agree, 61 (58.1%) agree, 3 (2.9%) disagree while 2 (1.9%) strongly disagree that Information system is the acclaimed engine room of modern day global development and sustainable growth. Also, 51 (48.6%) of the respondents strongly agree, 53 (50.5%) agree while 1 (0.9%) disagree that Cyber security ensures the protection of cyber space, data and information for sustainable growth and development.

Research Question Two: What are the communication challenges of cyber security?

Table 3: The communication challenges of cyber security

Statement	SA	A	D	SD	Mean	Stand Dev
Problem of communicating cyber attack risk directly to organizations	55 (52.4%)	47 (44.8%)	2 (1.9%)	1(0.9%)	3.23	2.20
Poor internal communication channels can enhance cyber attack	43 (40.9%)	59 (56.2%)	3 (2.9%)	-	2.79	1.63
Ineffective communication plan on updates and upgrades of cyber security facilities can enhance cyber attack	41 (39.1%)	56 (53.3%)	5 (4.8%)	3 (2.9%)	3.07	2.43
Inadequate knowledge and awareness on cyber security can enhance cyber attack	44 (41.9%)	60 (57.1%)	1 (0.9%)	-	3.89	2.09

Source: Field work, 2023

Table 3 shows that 55 (52.4%) of the respondents strongly agree, 47 (44.8%) agree, 2 (1.9%) disagree while 1(0.9%) strongly disagree that Problem of communicating cyber attack risk directly to organizations, 43 (40.9%) of the respondents strongly agree, 59 (56.2%) agree while 3 (2.9%) disagree that Poor internal communication channels can enhance cyber attack, 41 (39.1%) of the respondents strongly agree, 56 (53.3%) agree, 5 (4.8%) disgaree while 3 (2.9%) strongly disagree that ineffective communication plan on updates and upgrades of cyber security facilities can enhance cyber attack. Furthermore, 44 (41.9%) of the respondents strongly agree, 60 (57.1%) agree while 1 (0.9%) disagree that inadequate knowledge and awareness on cyber security can enhance cyber attack are some of the communication challenges of cyber security.

Hypothesis

H_0**:** There is no significant impact ofinformation systems and cyber security on sustainable development

The hypothesis was tested using Multiple Regression Analysis

Table 4: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.802[a]	.643	.641	1.182

a. Predictors: (Constant), Information Systems, Cyber security

Table 4: ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	303.151	2	151.576	91.864	.000[b]
	Residual	168.349	102	1.650		
	Total	471.500	104			

a. Dependent Variable: Sustainable development

b. Predictors: (Constant), Information Systems, Cyber security

Table 5: Coefficients

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	2.140	.438		5.004	.000
Information Systems	.069	.073	2.149	15.348	.000
Cyber security	.873	.092	1.697	10.938	.000

Dependent Variable: Sustainable development

The result from table hypothesis shows that Information Systems and Cyber security jointly significantly influence Sustainable development [(R^2 = .643; F (2,104) = 91.864; $p < .05$)].

This infers that Information Systems and Cyber security jointly accounted for about 64.3% of the variance observable in Sustainable development.

In addition, the result of the coefficients of multiple determination for the model shows that the independent contribution of Information Systems and Cyber security were positively significant ($\beta = 2.149$; $t = 15.348$; $p < .000$) and ($\beta = 1.697$; $t = 10.938$; $p < .000$). Also, in terms of magnitude, Information Systems had the highest magnitude with ($\beta = 2.149$).

Conclusion

The study used a survey research design with the aid of questionnaire that was administered to respondents. The population of this study are 105 respondents who were IT professionals and cyber security experts selected from online communities and social media platforms. The study concludes that Information Systems and Cyber security significantly influence Sustainable development. The finding of this study showed that Cyber-security, data regulation and sustainability are the key to the digital transformation processes in the coming years ($X = 3.46$, $SD = 2.17$), the development of environmental technologies along with their cyber-security is one of the aims of the realization of sustainable production and domestic security concepts ($X = 2.61$, $SD = 1.81$) and Problem of communicating cyber attack risk directly to organizations ($X = 3.23$, $SD = 2.20$). The result of the hypothesis revealed that Information Systems and Cyber security significantly influence Sustainable development with Information Systems having the highest magnitude with ($\beta = 2.149$). This finding supports a study which reported that cyber security measures and strategies will be effective for sustainable Nigerian national security and development[16].

Recommendations

i. This study recommends that government and related authorities should invest more on cyber security and information systems.
ii. The study also recommends that government should put in place programs that would train more professionals on cyber security.
iii. This study also recommends the need for improved cyber-security strategies, policies, and programs.

Endnotes

1. S. Widup, m. Spitler, D. Hylender& G. Bassett. *2018 Verizon Data Breach Investigations Report (2018).* Retrieved from http://www.verizonenterprise. com/ de/ DBIR/ on September 12, 2019.

2. A. Latham & P. Watkins. *China's New Data Security Law: What to Know, 2021.* Retrieved from LW website: https://www.lw.com/thoughtLeadership/china-new-data-security-law-what-to- know

3. J. Mensah& S.R. Casadevall. *Sustainable Development: Meaning, History, Principles and Implications For Human Action: Literature Review*. Cogent Social Sciences, 2019, 5(1), 1653531..
4. Schmälzle R, Renner B, & Schupp H.T.(2017). *Health Risk Perception and Risk Communication.*Policy Insights from the Behavioral and Brain Sciences. 2017;4:163–9.
5. J.A., Williams, H.G., Torres & T. Carte. *A Review of Information System Strategy Literature: Current Trends and Future Opportunities*. Forthcoming in Journal of Computer Information Systems, 2020, 60.10.1080/08874417.2019.1681327
6. Vial, G. *Understanding Digital Transformation: A Review and a Research Agenda*. The Journal of Strategic Information Systems 2019, 28 (2), 118–144. 10.1016/j.jsis.2019.01.003.
7. M. Ben-Eli. *Sustainability: Definition and Five Core Principles, A Systems Perspective*. Sustainability Science, 2018, 13. 10.1007/s11625-018-0564-3. (2018).
8. S.I. Akpama, C.D. *Bessong& N.O. Bessong. Attainment of the Sustainable Development Goals (SDGs): The Relevance of Adult Basic Education*. Journal of Faculty of Education, University of Calabar, Calabar – Nigeria, 13(1): 2017, 13-20
9. World Economic Forum. *The Global Risks Report 2018*. Retrieved from http://www3.weforum.org/docs/WEF_GRR18_Report.pdf
10. IDG. *2017 U.S. State of Cybercrime. In Re Equifax, Inc., Customer Data Security Breach Litigation*, MDL No. 2800 (Judicial Panel Mar. 20,2018).
11. Calman, K. "*The Language of Risk: A Question of Trust*," Transfusion, vol. 41, no. 11, 2001, 1326–1328, 2001.
12. D. Schatz, R. Bashroush& J. Wall. "*Towards a More Representative Definition of Cyber Security"*. Journal of Digital Forensics, Security and Law. 2017, 12 (2). ISSN 1558-7215.
13. F. D. Davis. "*Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology*", MIS Quarterly, 1989, 13 (3): 319–340, doi:10.2307/249008, JSTOR 249008, S2CID 12476939
14. T. Ask, R.G.Lugo, B.J. Knox & S. Sütterlin . *Human-Human Communication in Cyber Threat Situations: A Systematic Review*, 2021, Research Gate Publications. https://www.researchgate.net/publication/352321352

15. Y. Li & Q. Liu. *A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments*. Energy Reports 7 (2021) 8176–8186
16. A. A. Ahmed. (2022). *Information Security: An Effective Tool for Sustainable Nigerian National Security and Development*. Paper presented at Annual International Conference on Peace Building: The Role of Faith-Based Organizations Directorate of Peace and Conflict Resolution, Fityanul Islam of Nigeria, Abuja, Nigeria 19th-20th March, 2022