Mykolo Romerio universitetas

ISSN 1822-8038 (online)
INTELEKTINĖ EKONOMIKA
INTELLECTUAL ECONOMICS
2024, No. 18(2), p. 261–283

THE IMPACT OF CYBER SECURITY MANAGEMENT ON THE DIGITAL ECONOMY: MULTIPLE CASE STUDY ANALYSIS

Asta Valackiene
Faculty of Public Governance and Business,
Mykolas Romeris University, Vilnius, Lithuania
avala@mruni.eu
https://orcid.org/0000-0002-0079-9508

Rasheed Olalekan Odejayi
Faculty of Public Governance and Business
Mykolas Romeris University, Vilnius, Lithuania
rasheedolalekan48@yahoo.com

DOI: 10.13165/IE-24-18-2-02

Abstract

Purpose: The paper has empirically investigated the security impact of cyber security management on the digital economy across sub-Saharan African countries using Nigeria and Cameroon as a case study. To achieve these goals, 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; 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.

Methodology: This study adopted a descriptive design. The research is constructed using a mixed research strategy (quantitative and qualitative methods; primary and secondary data collection and analysis) to highlight the main findings (three hypothesized research questions are tested about respondents' views using content analysis of semi-structured interviews and triangulation of the results) and draw a valid and reliable conclusion.

Findings: The analysis revealed three main findings: it highlighted the key link between understanding the digital economy and cyber security management to provide the

main framework; it examined the nature of cyber security protocols and laws in combating cybercrimes in the digital economy; and it evaluated the roles of economic stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cybercrimes.

Originality: This study's results, findings, and discussions/recommendations will have future positive consequences in the fight against cyber insecurity in the private and public global digital space.

Keywords: cyber security management, information security, cyber security protocols, digital economy, resilience

JEL classification: D23, D81, M21, A13, K22, K24

1. Introduction

In recent years, innovation has been highly promoted and integrated into the structure of many societies because of its capacity to generate dual value both for customers and organizations; it can also bring broader benefits to society by providing previously unavailable or highly improved products and processes. It can be stated that innovation is one of the major drivers of intensive economic growth and determinants of the economy's performance. At the same time, we face the security of transmitted data and cybersecurity challenges, and consumerization has brought security into focus in cyberspace.

In today's digital economy, more than 60 percent of total commercial transactions are done online, and this has left cyberspace highly vulnerable, hence requiring a high quality of security for transparent and best transactions. To mitigate this global menace posed by cyber criminals, security spending has significantly increased as security has shifted from a non-functional requirement to an everyday business and governance requirement. Hence, it is important to implement an adequate cyber security management policy, which would encourage innovation activities and lead to economic growth, as it can also promote the restructuring processes inside the economy, thus making it more dynamic and adaptive to global economic tendencies. Security impact on the digital economy is viewed as a social license for businesses 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 of. Consequently, cybersecurity ensures that your organization's data is safe from attacks from both internal and external bad actors. It can encompass various technologies, processes, structures, and practices that protect networks, computers, programs, and data from unauthorized access or damage.

Statement of the problem and the level of its examination. Endeavor to analyze this social phenomenon (cyber risk, cyber insurance, cyberspace, cyber liability insurance) has been gaining substantial attention among researchers (Branley-Bell et al. l, 2012; van Bavel et

al., 2019; Singer et al., 2014; Low. 2017; Florin, 2022; Maluleke,2023). Moreover, cybercrime has been analyzed as an activity that uses systems, computer networks in general, and the Internet to perpetuate criminals prohibited by law (Ekoa et al., 2018). However, with a new decade beginning, the continent of Africa, which was regarded as "backward," has been able to leap into the world of ICT. This leap has not come without a heavy price. Many sub-Saharan African countries' international reputations have been affected by the continuous rise of cybercrime. The rapid diffusion rate of cybercrime in Africa has been a call for concern (Kshetri, 2019; Akuta et al., 2011; Report of International Finance Corporation, 2018). By the way, 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). Since technical measures alone cannot prevent crime, law enforcement agencies must be allowed to investigate and prosecute cybercrime effectively. The fight against cybercrimes needs a comprehensive and safer approach and new applied research on cybersecurity management, seeking to highlight the impact of security on the digital economy in African countries. This transformation highlights the urgent need to ensure cyber security parameters and standards meet this community's demands and future needs, including financial inclusion (Report of International Finance Corporation, 2018). However, the absence of these standards is pervasive in Africa. 90% of African businesses operate without the necessary cyber security protocols (Rights group launches tool to stem cybercrime in Africa, 2021). Threat actors can exploit increasing vulnerabilities without these protocols as they invent new cyber-attack vectors. This leads to significant financial loss. For example, in 2016, cybercrime cost the Kenyan economy about 36 million USD, the South African economy 573 million USD, and the Nigerian economy 500 million USD (Cybercrime in Africa: Facts and figures, 2016). In the past year, the COVID-19 pandemic has accelerated the cyber-crime ecosystem with a persisting digital divide and increasing cyber security vulnerabilities across the region. Similarly to other regions, the African region experienced attacks against critical infrastructure and frontline services during the pandemic. This was most prominently seen 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 (Life Healthcare Group takes its systems offline after a cyber attack, 2020).

Looking at the situation, we say that little has been done to prevent cybercrime in the African region, including management efficiency and investigation, to identify the effect of cyber security management on the digital economy across sub-Saharan African countries. This study argues that the growing rate of digital transformation within the African region is facilitating the emergence of new attack vectors and opportunities for cybercriminals. In recognition of the magnitude of the problem caused by cyber threats in Africa, Against the backdrop, this study seeks to investigate how cyberspace 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 cybercriminals.

Emphasizing the importance of cyber security management and preventing cybercrime in the digital economy in African countries, the *research problem* was identified, and *the general research question was constructed (GRQ)*: *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?* This scientific approach leads to a conceptual, theoretical argumentation and empirical findings that security management is the ability to plan, respond, recover, and adapt to the situation of the digital economy. For this reason, an empirical study (applying a Qualitative strategy) is presented to validate a conceptual framework explaining how to examine the security impact of cybersecurity management on the digital economy across sub-Saharan African countries.

This paper makes *several contributions*. *First,* it provides empirical evidence that acknowledges the dimensional structure of cyber security management and preventing cybercrime in the digital economy. *Second*, it explores the associations between cybersecurity management and digital economy-forward stages. *Third*, the testing/verifying of the above-outlined hypotheses explains the interaction of cyber security management and its impact on the digital economy in Sub-Saharan African countries. The findings contribute to the extension of knowledge about the practical structure of cybersecurity management and allow us to explore how the dimensions of this social phenomenon are associated with each other in the digital economy area.

The paper is structured as follows: 1 Introduction; Section 2 examines the conceptual framework, introduces theoretical approaches to cybersecurity phenomena, followed by the hypotheses of this study; Section 3 introduces the methodology of this study and research design; Section 4 discusses the results of empirical research, concludes the paper; Section 5 - the empirical findings are discussed comparing with the results of other researchers and gives suggestions for further studies.

2. Theoretical background: justification of the framework and hypotheses

2.1. The concept of digital economy

The concept of *digital economy* should be discussed, considering the phenomenon's scale and social changes. United Nations Report (2019) emphasizes that the dynamic development and growth in using ICTs, including digital technologies, is a driver of change in shaping modern economies. 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. Analysing the notion of digital economy through the different conceptual frameworks proposed in the literature makes it possible to identify some fundamental concepts. Many new terms have been coined for this new economy, such as "knowledge-based economy," "borderless economy," "weightless economy," "networked economy," "digital economy,"

"information-based economy," and "the networked economy" to name a few phenomena (Sharma et al., 2004). Some researchers support the idea that the digital economy is about converging communications, computing, and information. Don Tapscott (1995) was one of the first to describe the digital economy. He listed 12 features distinguishing the digital economy from the industrial economy. Williams (2021) discussed the meaning of the digital economy, focusing on three-scope methodologies to comprehend the digitalized economy. Some definitions, especially the first ones, emphasize using Internet Protocol (IP) –)-enabled communications and networks in the digital economy (Brynjolfsson, Kahin, 2002).

Johansson, Karlsson, and Stough (2006) highlight the role of rapid development, adaptation, and use of ICT innovations in transforming the economy and all sectors towards the digital economy. Due to this evolutionary process, society has access to new products, production processes, and services. As Mulligan (2017) stated, the US leader in the digital economy amassed USD 5.9 trillion through the digital economy, which equates to 33% of its Gross Domestic Product (GDP). Digital investments have a growth multiplier effect on national GDP, increasing the national economic output. In the US, this digital investment is expected to translate into an additional 2.1% of GDP in 2020, equivalent to USD 421 billion. Nations are in the infancy of the Fourth Industrial Revolution, transitioning to a new era where the digital, biological, and physical worlds merge (Al-Khouri, 2012). Other studies (Weill et al., 2013; Knickrehm et al., 2016; Baller et al., 2016) support the idea that the digital economy sometimes falls in the face of disruption and can trigger different digital disruptions. In this digital revolution, opportunities and growth rest on a conducive regulatory and business environment, ICT readiness on emerging technologies, and usage of ICT in societal-wide adoption and leverage (Knickrehm et al., 2016). Murthy et al., 2021, discussed the digital economy from a global perspective, highlighting evidence of a digital divide, as the global digital economy is dominated by developed economies, especially in e-commerce, while developing countries face serious challenges.

However, digital intervention is unavoidable for a nation to thrive and prosper in this century. To reinforce such attitudes and approaches, the World Economic Forum regularly publishes the Network Readiness Index (NRI) to assess and quantify countries' readiness to capture and benefit from emerging technologies in the digital economy.

2.2. The concept of cyber-crimes

Many definitions have evolved to describe cybercrimes. Grabosky (2001), using a metaphor, describes cybercrime as a case of 'old wine in new bottles.' Douglas and Loader (2000) define cybercrime as 'computer-mediated activities which are either illegal or considered illicit by certain parties and 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 Lynn (2010) calls intellectual espionage "the most significant cyber threat faced by the United States." 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. However, assessing its scope is challenging since many companies are reluctant to disclose an attack. Actual numbers are hard to come by.

Also, a report by the U.K. government (Report by information intelligence experts, 2011) estimates that U.K. businesses lost over £16 billion, 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 cybercrimes, 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 disclose espionage details 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; global losses from cybercrime now total over $1 trillion, a more than 50 percent increase from 2018; Two-thirds of surveyed companies reported some cyber incident in 2019 (The report by McAfee Corp, 2020). This would put cybercrime on course to be close to 2 percent of the global economy, more significant than the pharmaceutical industry. A familiar 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 (Friedman, 2011). At the same time, another suggests $37 billion (Javelin et al.: Identity Fraud Survey Report, 2011). These two estimates indicate a fraud rate of 0.25 percent or 1.1 percent of the $3.34 trillion credit card transactions in 2009. Even these numbers are misleading, given how inefficient many cyber schemes are.

We point out that crime also has a limited impact, with incidence contained mainly in value sectors. Cyber crooks attack banks, bank-like services, and identity platforms because "that is 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 (Anser et al., 2020).

Accordingly, we are guided by the notion that crime, as a matter of public interest, poses a dual 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 government attention but not a huge priority. As fraud grows, though, it might approach a tipping point. If attacks on a particular digital platform or application grow too large, components of the information infrastructure could be abandoned (Friedman, 2011). The "World Cyber-crime Index" (2024, April) shows which countries are most at risk from cybercriminals. Researchers (Bruce et al., 2024) identified five major categories

of cybercrime: Technical products/services (e.g., malware coding, botnet access, access to compromised systems, and tool production.; Attacks and extortion (e.g. denial-of-service attacks, ransomware); Data/identity theft (e.g., hacking, phishing, account compromises, credit card comprises); Scams (e.g. advance fee fraud, business email compromise, online auction fraud); Cashing out/money laundering (e.g., credit card fraud, money mules, illicit virtual currency platforms).

2.2.1. Intensives in cyber-crime

On the other hand, analyzing the notion of *incentives in cybercrime* through the different conceptual frameworks proposed in the management literature makes it possible to identify some fundamental concepts and *crime practices*. In one recent case, as Reddy & Reddy (2014) have noted, the United States Secret Service apprehended an individual possessing over 300,000 credit card accounts, which have been linked to some $36 million in fraud. However, the best estimates in the criminal filing claim that the defendant personally received over $100,000 from his credit card fraud scheme. Estimates vary on the value of credit card information on the black market. However, the low end is almost always less than one dollar for a usable credit card number and expiration date, while the upper estimates seldom exceed a few tens of dollars. The low returns for those who steal credit card information are due to the large number of stolen accounts flooding the market, leading to lower prices. This demands 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. Law enforcement is unlikely to deter all crimes in this area completely. The international and fluid nature of many online crimes makes it difficult to engage in enforcement models specifically designed to deter crime, such as those described by Kleiman and Kilmer (2009).

2.2.2. An online scam

As far as the African continent is concerned, the number of different types of cyber-crime is increasing. *An online scam* is a fraudulent scheme 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. The Federal Bureau of Investigation, USA (2016) has noted that an online scam is an attempt by an individual or group to trick individuals into providing personal or financial information for illegal purposes. The FBI noted that online scams are becoming more sophisticated and complex to detect and that people should be careful when giving out personal information or sending money online. According to a report by

Kaspersky Global Cybersecurity Company (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.

2.2.3. Digital extortion

Following Zetter (2019), *digital extortion* 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. The ransom is typically demanded in a digital currency, such as Bitcoin, to make it more difficult for authorities to trace the transaction. Digital extortion often involves using technology to access someone's computer or other digital devices and can be carried out remotely from anywhere in the world. It is a growing threat that has serious consequences for individuals and organizations.

2.2.4. Ransomware

Another type of cybercrime - *ransomware*- is malware that encrypts a victim's data and demands a ransom payment in exchange for the decryption key. Liptak (2017) noted that this type of cyber-attack has increased in recent years, with victims ranging from individual users to large businesses and government agencies. A ransomware attack known as "WannaCry" infected many computers in different countries. 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, businesses, 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 (Palo et al., 2021).

2.2.5. Business email compromise

Business email compromise (BEC) is a new form of cybercrime. The FBI defines business email compromise as a sophisticated email scam that targets businesses working with foreign partners who regularly perform wire transfer payments (Trend Micro & INTERPOL, Cybercrime in West Africa, 2017).

The COVID-19 pandemic and the war in Ukraine have shown that cyber-security attacks occur in almost every country. Record-breaking temperatures, fires, storms, and floods also alarm planetary systems increasingly out of whack. According to a report published by the UNDP (United et al. on Human Security, 2022), digital technologies are increasingly central in people's lives as consumers, citizens, workers, entrepreneurs, and even in their relationships.

As we can see, there is much discussion in various sources on this area, but there is no

conceptual justification that the digital economy and cybercrime are in close interaction. Qualitative empirical studies in different countries are significantly lacking. For this reason, we argue that there is a need to further elucidate the governance of cyber security based on qualitative empirical research data and reflections to prevent cyber-crime in the digital economy in African countries in order to leverage experience, learn from mistakes, and empower them to strengthen and break away from the current criminological situation.

2.3. Conceptualization of research framework

Seeking to *conceptualize our research framework*, this social phenomenon was anchored on the theory of Planned Behaviour (TPB), Protection Motivation Theory (PMT), and Alagappa's theory on the national security of developing countries. These theories were chosen because of their permeability, comprehensiveness, and broader horizon in embracing all the elements and variables discussed in the study, such as cyber security, cybercrimes, national security, digital economy, policy responses, and collective security in general.

According to Lebek et al. (2014) and Nasir et al. (2018), three main theoretical models are often applied in this field: Planned Behavior Theory (TPB), Protection Motivation Theory (PMT), and General Deterrence Theory (GDT). The Technology Acceptance Model (TAM) can also be applied, but certainly not as often as mentioned above. Nasir et al. (2018) described it as the most dominant theory with the most significant primary constructs in predicting and explaining employees' ISP compliance behavior. For example, a widely quoted study by Ifinedo (2012) shows that including PMT structures in the TPB model can increase research results and demonstrate model verification.

For this reason, cyber security assessment in the digital economy field should be based on integrating these approaches. To support this thesis, *three fundamental hypotheses* are formulated *(H; H2; H3)*. It can be stated that the following research questions have been validated in the course of this empirical research:

H1. What are the past and current trends of cybercrimes perpetrated in the digital economy of the selected sub-Saharan African countries?

H2. What are 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?

H3. What are the roles of economy stakeholders in the repositioning and enforcing cyber security protocols to effectively combat cybercrimes in the digital economy of the selected sub-Saharan African countries?

In the following section, the research methodology and design are outlined.

3. Methodology: Materials and Methods

3.1. Research design and methods development

A descriptive research design was adopted for this study. This design is suitable because it uses primary data sources as key and first-hand evidence. This research design method allows the researcher to maintain a cordial interaction with the focus group in the identified study population. The research is constructed on *a mixed research strategy (quantitative and qualitative methods; primary and secondary data collection and analysis*). Hence, this study will be centered on sub-Saharan African countries, using Nigeria and Cameroon as case studies. As Bryman (2006) explained, the mixed strategy method in the context of triangulation is a traditional view where quantitative and qualitative researchers are combined to triangulate findings to be mutually corroborated. The other primary sources (strategies and policy documents) have been analyzed: the Nigerian and Cameroonian government's cyber security policy documents and reports from relevant agencies, while those secondary sources consisting of secondary statistical data, journals, and internet sources relevant to the topic at hand were also analyzed.

3.2. Measurement instrument

The primary research involves interviews and analysis of the opinions provided by the primary respondents. The research instrument for this research will be the interview method: a semi-structured interview guide/questionnaire will be employed as a research tool. The research will ask specific questions to each group and 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. The quantitative research strategy will use previous literature, digital resources, and a closed questionnaire (survey). Following the ethical standards, the researcher would anonymize the names of the participants; informants are not personally identified but instead codified as (*I*) informants. The interview was conducted in June 2022 and lasted from half to one hour. After analyzing the collected data, the informants were asked to review the findings and to provide their comments.

3.3. Data collection and sample characteristics

The study will use diverse sources, including categories within the study, the Nigerian and Cameroonian government's cyber security policy documents, and reports from relevant agencies. The population of this study comprises 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. A total number of sixty participants (N=60) were selected to be sorted into four categories: Category A (sixteen military or paramilitary security personnel will be selected from different agencies directly dealing with security issues (N=16), B (twenty senior officials will be chosen from institutes and agencies handling security issues in Nigeria and Cameroon (N=20), C (a group of academics scholars, consisting of twelve professors chosen from three universities, based on the proximity to the target audience (N=12), and D (twelve members of private institutions that deal with cyber activities will be selected randomly and interviewed (N=12) through non-probability sampling type, the purposive sampling technique. This technique is suitable because it affords the target audience an equal chance 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 the 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.

Criteria for informants' selection. There are *three criteria* used in identifying informants to be interviewed in this study: *the first* is the identification of stakeholders who are closely linked and related to the subject matter of cyber security, cybercrimes, digital economy, and national security. The chosen sources were interviewed under the condition of anonymity and confidentiality. *The second* was based on the ease of access and high-quality data on the subject studied for some government ministries and agencies. *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), the minimum number of interviewees for a qualitative research project should be either four or five, and the maximum should not be more than sixty, depending on the availability of the resources and informants with quality information.

4. Data analysis and results

For this research, 60 informants were selected, and copies of the semi-structured interview questionnaire were provided. *Reliability of the interview questionnaire*: Only 54 copies of the semi-structured interview questionnaire were wholly and correctly 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 presenting and distributing respondents' demographic characteristics, which shows the relationship among others: respondents' gender, cadre, position, and experience, as indicated in the research instrument.

Also, the second category of the analysis presents and analyzes the respondents' views on the subject matter (the security impact of cyber security management on the digital economy across sub-Saharan African countries, using Nigeria and Cameroon as

a case study) about the hypothesized research questions as responded and collated in the semi-structured interview questionnaire.

Finally, the analysis discusses its findings about 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. Table 1 presents the demographic and social characteristics of the respondents.

Table 1. Distribution of respondents' demographic characteristics.

Variable	Demographic characteristics	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	

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 (Nigeria and Cameroon). Here, the hypothesized research questions are tested with respondents' views portrayed in the semi-structured interview checklist.

Theoretical hypotheses were examined by testing hypothesized research questions: Hypothesized Research Question One: H1 What is the past and current trend of cybercrimes perpetrated in the digital economy of Nigeria and Cameroon? In a bid to provide an answer to the hypothesized research question stated above, the researcher assessed 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. The main results are presented in Figure 1.

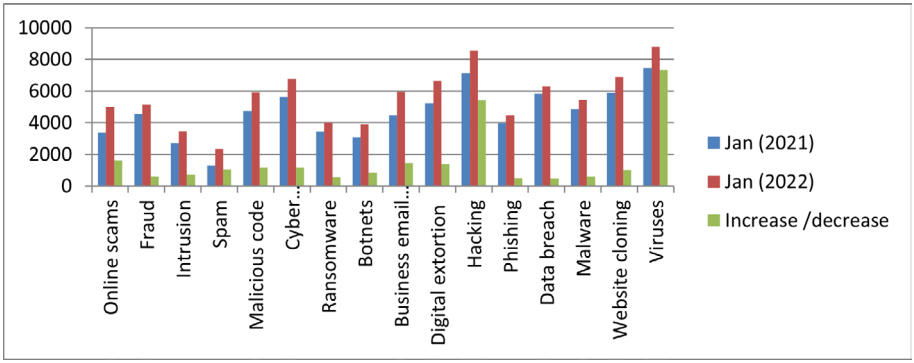

Figure 1. Past and current trends of cybercrime perpetrated in the digital economy of the selected sub-Saharan African countries.

From the graphical presentation in Figure 1, it was evident that the majority of the sampled respondents purported the series of cybercrimes perpetrated in their digital economy of the selected sub-Sahara African countries 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 the graphical illustration, the crimes relating to those viruses and hacking as of 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). These further showed an absurd increase in the trend of viruses and cyber-vices being hacked.

Hypothesized Research Question Two: H2 What are the nature and types of cyber security protocols and already established laws in combating cybercrimes in the digital economy of Nigeria and Cameroun? In a bid to provide an answer to the hypothesized research question stated above, the researcher conducted an assessment of 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 concerning your country what is your assessment on cyber security protocols and already established laws in combating cybercrimes in the digital economy of your country…" as indicated in Section B (Numbers 1-16) of the semi-structured interview questionnaire. The main results are presented in Table 2.

Table 2. Analysis of 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.

Statements	Responses	Remarks
The situation of cybercrime and attacks <...>."	Worst and decaying	Very true
Nature, types, and trend of cybercrimes <...>."	Viruses and hacking	Very true
Major perpetrators and victims of the cybercrimes	Youths and unemployed	Very true
The primary motive behind cybercrimes <...>."	Poverty and idleness	Very true
Presence of CSPs managing cyber activities <...>"	Present and established	Very true
Mention CSPs already established and in <...>"	EFCC, ICPC, Police, CCB etc.	Very true
CSPs have legal backing to checkmate <...>"	Legal backing to prosecute	Very true
Position of laws of CSPs on cyber offenders in <...>"	Right to arrest/prosecute	Very true
Established laws that serve as deterrents <...>"	Provision of Criminal Acts	Very true
CSPs engage tracking devices to checkmate users <...>"	Do engage tracking devices	Very true
CSPs perform periodic drills to ensure that <...>"	Perform periodic drills	Very true
CSPs grant preferential access to particular users to <...>"	Depends on purpose/ usage	Very true
CSPs restrict application access to users operating <...>"	Depends on the users	Very true
The percentage of users who secure their devices <...>"	60-86 percent	Very true
CSPs keep users informed on threats and best <...>."	Massive awareness	Very true
CSPs enable usage of external devices based on <...>"	Depends on purpose/ usage	Very true

Hypothesized Research Question Three: H3. What are the roles of economy stakeholders in repositioning and enforcing cybersecurity protocols to effectively combat cybercrimes in the digital economy of Nigeria and Cameroun? Furthermore, in a bid to provide an answer to the hypothesized research question stated above, the researcher also conducted an assessment of 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 cybercrimes 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. The main results are presented in Table 3.

Table 3. Analysis of the perceived roles of economy stakeholders in the repositioning and enforcing cyber security protocols in effectively combating cybercrimes in the digital economy of the selected sub-Saharan African countries.

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

4.1. Triangulation findings of the semi-structured experts interview Content Analysis

In this study, the Interviews aimed to triangulate the empirical data: the researcher gathered Qualitative data from field professionals and used it as supporting data for Quantitative data. This data helped explain quantitative data in detail and elaborate on the results.

The main requirements for the Interviews were: 1. To ensure the research question is straightforward. 2. The line of questioning was prepared unbiasedly and clearly. 3. Interviewees had clear information prior to the interview about the research conducted and the purpose of the interviews. 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 et al., 2002). Content Analysis for the semi-structured interview questionnaire was applied. The authors emphasized that the three main dimensions of the interview focused on the relationship between science, business, and society to reinforce the implementation of the responsible cybersecurity area in ecosystems. To get the information under discussion: the security impact of cybersecurity management on the digital economy across sub-Saharan African

countries and outcomes.

Interview transcripts were analyzed to quantify patterns and trends, coded, and summarized to interpret Qualitative data and draw a conclusion.

In this case, direct quotations were used to support analysis and present the gathered information to the reader as it is. Following ethical standards, the researcher anonymized the names of the participants; they were not personally identified but codified as (I) informants. The coding method was based on the research questions. Table 4 presents the primary information of the findings.

Table 4. 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 sub-Saharan African countries	(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 loss of goodwill and national resources;
	(b) Assessment of most common perpetrated cyber-attacks in the countries under survey	6	'<...>viruses and hacking;
		3	'<...> digital extortion and cyber harassment;
	(c) Factors behind the perpetration of cybercrimes and the age bracket of its perpetrators in the countries under survey	8	'<...>the high state of unemployment, poverty, and get-rich-quick syndrome, and its 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 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 the 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 offense;
		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;

III. The roles of economic stakeholders in repositioning and enforcing cyber security protocols to combat cybercrimes effectively in the digital economies of sub-Saharan African countries.	(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 classified information and applications among specific and general cyber users	6	'<...> Well, it all depends on the nature and purpose of the classified applicant or user;
		5	'<...> preference should be accorded to 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 the 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;

5. Discussion and Conclusion

The findings reveal that most respondents attested that viruses and hacking were the most common cybercrimes in the digital economies of these countries (Nigeria and Cameroon), with a significant increase in the trend of these crimes.

Based on the outcome of the test of *the first research question*: "on the past and current trend of cybercrimes perpetrated in the digital economy," findings revealed that the majority of the informants attested that among the commonly perpetrated cybercrimes in the digital economy (Nigeria and Cameroon) 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 sub-Sahara African countries. The outcome was in line with the empirical views of Aghatise (2006), who also submitted that the arrival of the internet in Nigeria has enabled criminals and their activities to increase the number of their unsuspecting victims, which invariably makes it difficult to track them down.

Based on the outcome of the test of *the second research question*: "on the nature and types of cyber security protocols and already established laws in combating cybercrimes in the digital economy," findings revealed that the majority of the informants described the situation of cybercrime and attacks as very worst which has brought about societal and economic decadence in Nigeria and Cameroon. Also, the majority acclaimed the most commonly perpetrated cybercrimes as viruses and hacking, pointing to an alarming rise in cyber-attacks in Nigeria and Cameroon. Informants affirmed that youths and the unemployed are major perpetrators of cybercrimes; poverty, idleness, and get-rich-quick syndrome are the motives behind why youths and those who fall within the unemployed bracket engage in cybercrimes in Nigeria and Cameroon. The majority affirmed that cyber security protocols (CSPs) monitor and check all illicit cyber activities in the selected sub-Saharan African countries. Findings showed that the majority admitted that CSPs in the selected sub-Saharan African countries embark on massive awareness in keeping users informed on threats and best practices to safeguard and protect their cyber assets (vital data and information). Furthermore, the majority submitted that CSPs often discourage the usage of external devices by corporate or personal users, except the purpose is defined before usage can be granted.

Based on the outcome of the tested *the third research question*: "on the roles of economy stakeholders in the repositioning and enforcement of cyber security protocols in effectively combating cybercrimes in the digital economy," findings revealed that the majority of the informants described (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. Majority of informants (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; (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; (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; (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; (92.6%) believes that users (corporate and individuals) turn to external managed security service providers for a relatively broad spectrum of needs, ranging from tactical device monitoring to more strategic areas where they may lack the institutional knowledge, while the remaining; (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. Lastly, the majority (74.1%) do not believe that only very few users would use third parties for governance, risk, and compliance management support.

The findings reveal that most informants attested that the most common cybercrimes in the digital economy of these countries were viruses and hacking, with a significant increase in the trend of these crimes. The study also found that youths and the unemployed are major perpetrators of cybercrimes, motivated by poverty and idleness, among other factors. The study found that cyber security protocols are in place to monitor and check illicit cyber activities, and the law backs them. The study also found that these protocols engage in periodic drills and awareness programs to keep users informed and secure. Additionally, the study found that access to classified applications is restricted, and users' devices are often secured with passwords. The study confirms that cybercrime is flourishing in Nigeria and affecting its national security, and Nigeria should adopt measures to strengthen its cyber security.

The rise in these crimes is attributed to the arrival of the internet, which has enabled criminals to increase the number of their unsuspecting victims. The existing cyber security protocols (CSPs) in the two countries (have the full backing and authorization of the law to prosecute cyber criminals, but the situation of cybercrime is still very concerning and is leading to societal and economic decadence. There is a need for practical and logical solutions to tackle the threat of cybercrime and for a vast population of users to outsource and manage their IT and security infrastructure through service partners. The article concludes by highlighting the need for stakeholders to have high trust and confidence in digital technology and for policymakers to have a sound knowledge of cybersecurity management.

Admittedly, the study carried out in this paper has some limitations, including generalizing the conclusions obtained here to the entire population; it should be discussed in the broadest context. The research results showed that the authors should conduct a longitudinal study to get a broader picture of the lessons learned by the countries. The authors also intend to expand the research geography to include EU countries in future research projects.

References

1. Aghatise, J. (2006). Cybercrime definition: Report of the HND project entitled "Level of awareness of Internet intermediary liability *Auchi Polytechnic*. Retrieved from www.researchgate.net/publication/265350281_Cybercrime_definition.
2. Akuta, E. A., Monari, I., & Renne, C. (2011). Combating cybercrimes in Sub-Sahara Africa: A discourse on law, policy, and practice. Journal of Peace, Gender and Development Studies, 1(4), 129–137.
3. Al-Khouri, A. M. (2012). Emerging markets and the digital economy. International Journal of Innovation in the Digital Economy, 3(2), 57–69. https://doi.org/10.4018/jide.2012040105
4. Anser, M. K., Yousaf, Z., Nassani, A., Alotaibi, S., Kabbani, A., & Zaman, K. (2020). Dynamic linkages between poverty, inequality, crime, and social expenditures in a panel of 16 countries: Two-step GMM estimates. Economic Structures, 9(43), 1–25. https://doi.org/10.1186/s40008-020-00220-6
5. Baller, S., Dutta, S., & Lanvin, B. (2016). The global information technology report: Innovation in the digital economy. World Economic Forum.
6. Branley-Bell, D., Gómez, Y., Coventry, L., Vila, J., & Briggs, P. (2021). Developing and validating a behavioral model of cyber insurance adoption. Sustainability, 13(17), 1–16. https://doi.org/10.3390/su13179528
7. Bryman, A. (2006). Integrating quantitative and qualitative research: How is it done? Qualitative Research, 6(1), 97–113. https://doi.org/10.1177/1468794106058877
8. Brynjolfsson, E., & Kahin, B. (Eds.) (2002). Understanding the digital economy: Data, tools, and research. Cambridge, MA: Massachusetts Institute of Technology Press.
9. Bruce M, Lusthaus J, Kashyap R, Phair N, Varese F (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. PLoS ONE 19(4): e0297312. https://doi.org/10.1371/journal.pone.0297312.
10. Campbell, J. (2019, July 25). Last month, over half a billion Africans accessed the internet. Council on Foreign Relations. Retrieved from https://www.cfr.org/blog/last-month-over-halfbillion-Africans-accessed-internet
11. Cybercrime in Africa: Facts and figures. (2016, July). Retrieved from https://www.scidev.net/sub-saharan-Africa/features/cybercrime-Africa-facts-figures/
12. Detica & Office of Cyber Security & Information Assurance. (2011). The estimated cost of cybercrime. Office of Cyber Security & Information Assurance. Retrieved from http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime.
13. Douglas, T., & Loader, B. (2000). Cybercrime: Law enforcement, security, and surveillance in the information age. Journal of Social Policy, 30(1), 149–188. https://doi.org/10.4324/9780203354643
14. Ekoa, R., & Mungwe, M. (2018). A review of cybercrime in Sub-Saharan Africa: A study of Cameroon and Nigeria. International Journal of Scientific & Engineering Research, 9(5), 211–228.
15. Florin, M. V. (2022). Risk governance and 'responsible research and innovation' can be mutually supportive. Journal of Risk Research, 25(8), 976–990. https://doi.org/10.1080/13669877.2019.1646311

16. Friedman, A. (2011). Economic and policy frameworks for cybersecurity risks. Center for Technology Innovation at Brookings, pp. 1–24.
17. Grabosky, P. N. (2001). Cybercrime and the law. *Thomson Legal & Regulatory Ltd, 10*(2). https://doi.org/10.1177/a017405
18. Ifinedo, P. (2012). Understanding information systems security policy compliance: Integrating the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007
19. Javelin Strategy & Research. (2021). Identity Fraud Survey Report: "Friendly fraud" and consumer costs are rising; non-credit card and new account fraud have also increased. Retrieved from https://javelinstrategy.com
20. Johansson, B., Karlsson, C., & Stough, R. (Eds.) (2006). *The emerging digital economy: Entrepreneurship, clusters, and policy* (pp. 1–19). Berlin: Springer.
21. Kaspersky Global Cybersecurity Company. (2020). The year of social distancing or social engineering? Phishing goes targeted and diversifies during COVID-19 outbreak. Retrieved from [https://www.kaspersky.com](https://www.kaspersky.com/about/press releases/2020_the-year-of-social-distancing-orsocial-engineering)
22. Kleiman, M., & Kilmer, B. (2009). The dynamics of deterrence. *Proceedings of the National Academy of Sciences of the United States of America, 106*(34), 14230–14235. https://doi.org/10.1073/pnas.090551310
23. Knickrehm, M., Berthon, B., & Daugherty, P. (2016). Digital disruption: The growth multiplier. *Accenture Strategy.* Retrieved from https://www.accenture.com
24. Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management, 22*(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527
25. Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review, 37*(12), 1049–1092.
26. Life Healthcare Group. (2020). Life Healthcare Group takes its systems offline after cyberattack. Retrieved from https://www.thesouthafrican.com
27. Liptak, A. (2017, May 14). The WannaCry ransomware attack has spread to 150 countries. *The Verge.* Retrieved from https://www.theverge.com
28. Low, P. (2017). Insuring against cyber-attacks. *Computer Fraud and Security, 17*(4), 18–20. https://doi.org/10.1016/S1361-3723(17)30034-9
29. Lynn, W. (2010). Defending a new domain: The Pentagon's cyber strategy. *Foreign Affairs.* Retrieved from https://www.foreignaffairs.com
30. Maluleke, W. (2023). Exploring cybercrime: An emerging phenomenon and associated challenges in Africa. *International Journal of Social Science Research and Review, 6*(6), 223–243. https://doi.org/10.47814/ijssrr.v6i6.1360
31. Mathers, N., Fox, N., & Hunn, A. (2002). *Trent Focus for Research and Development in Primary Health Care: Using interviews in a research project.* Produced by Trent Focus Group, London.
32. Mulligan, C. (2017). Cybersecurity: Cornerstone of the digital economy. *Imperial College Business School, London.*
33. Murthy, K. V. B., Kalsie, A., & Shankar, R. (2021). Digital economy in a global perspective:

is there a digital divide? *Transnational Corporations Review,* 13(1), 1–15. https://doi.org/10.1080/19186444.2020.1871257
34. Nasir, A., Ruzaini, A. A., & Ab Hamid, M. R. (2018). The significance of primary constructs of the theory of planned behavior in recent information security policy compliance behavior studies: A comparison among top three behavioral theories. *International Journal of Engineering & Technology, 7*(2), 737–741.
35. Palo Alto Networks. (2021). Extortion payments hit new records as ransomware crisis intensifies. Retrieved from https://www.paloaltonetworks.com
36. Reddy, G. N., & Reddy, G. J. U. (2014). Study of cybersecurity challenges and its emerging trends on latest technologies. *International Journal of Engineering and Technology - UK, 4*(1). https://doi.org/10.48550/arXiv.1402.1842
37. Report of International Finance Corporation. (2018). Digital access: The future of financial inclusion in Africa. Retrieved from https://www.ifc.org
38. Rights group. (2021, May 14). Rights group launches tool to stem cybercrime in Africa. *Phys.org.* Retrieved from https://phys.org
39. Sharan, M. P. (2009). *Qualitative research method.* San Francisco: John Wiley & Sons.
40. 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.), *Hershey, PA: Idea Group Publishing.* https://doi.org/10.4018/978-1-59140-146-9.ch017
41. Hershey, PA: Idea Group Publishing. DOI: https://doi.org/10.4018/978-1-59140-146-9.ch017
42. Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar. Network Security, 4, 4–10. https://doi.org/10.1016/s1353-4858(14)70039-x
43. United Nations Development Programme (UNDP). (2022). Special report on human security: Human development reports. Retrieved from https://www.undp.org
44. Tapscott, D. (1995). The digital economy: Promise and peril in the age of networked intelligence. New York: McGraw-Hill.
45. Trend Micro & INTERPOL. (2017). Cybercrime in West Africa: Poised for an underground market. Retrieved from https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-Africa.pdf
46. United Nations. (2019). Digital economy report: Value creation and capture – Implications for developing countries. Geneva: United Nations Publications.
47. van Bavel, R., Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. International Journal of Human-Computer Studies, 123, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003
48. Weill, P., & Woerner, S. L. (2013). The future of the CIO in a digital economy. MIS Quarterly Executive, 12(2), Article 3. Retrieved from https://aisel.aisnet.org/misqe/vol12/iss2/3
49. Williams, L. D. (2021). Concepts of digital economy and Industry 4.0 in intelligent and information systems. International Journal of Intelligent Networks, 2, 122–129.
50. Zetter, R. (2019). Protection in crisis: Forced migration and protection in a global era. Migration Policy Institute.