Pakistan Journal of Multidisciplinary Innovation (PJMI)

Volume 3, Number 1, 2024, Pages 29 – 40

Journal Home Page

https://journals.airsd.org/index.php/pjmi

Cybercrime and its Effect on Nation Identity Image: Pragmatic Evidence from Nigeria

Adegoke Dauda Adejumo[1], Kamar Olawale Oyeniyi[2]

[1]*Department of Marketing, Osun State Polytechnic, Iree, Nigeria*
[2]*Department of Business Administration, Osun State Polytechnic, Iree, Nigeria*

ARTICLE INFO

Article History:

Received:	February	21, 2023
Revised:	March	25,2023
Accepted:	April	15,2023
Available Online:	May	30,2023

Keywords:

Cybercrime, National image, Unemployment, National Functional Database, ICCP

ABSTRACT

This study examines the influence of cybercrime on the national image. Specifically, the overall aim is to identify factors influencing cybercrime in Nigeria and to determine the extent to which cybercrime influences national image. The study utilizes a survey design, employing a purposive sampling technique to select 10 lawyers, 10 EFCC officers, 10 ICPC officers, and 10 judges from each of the following cities: Lagos, Abeokuta, Ibadan, Osogbo, Akure, and Ado-Ekiti. This total of 240 participants comprised the study's sample size. A structured questionnaire was used to collect data and data analysis was performed with the aid of mean, chi-square, and path analysis. The results reveal that high unemployment rates, inadequate security on personal devices, broken homes, lack of moral values and parental supervision, a weak judicial system, weak law enforcement, the pursuit of wealth, negative role models and poverty peer groups, and the absence of a functional national database are major factors influencing cybercrime in Nigeria. Evidence also reveals that cybercrime has an inverse influence on the national image of Nigeria. The findings gleaned from this study strongly underscore cybercrime as a grave threat to Nigeria's national image. Therefore, to safeguard the country's reputation, it is imperative that the government and relevant stakeholders take proactive measures to prevent and combat cybercrime.

Corresponding Author's Email: kamola1973@gmail.com

INTRODUCTION

Nigeria is known as the "Giant of Africa," boasting a rapidly growing presence in sectors like manufacturing, finance, services, communications, technology, and entertainment. Its standing on the global economic stage is remarkable, holding the 21st spot for nominal Gross Domestic Product (GDP) and the 20th position for Purchasing Power Parity (PPP). As the largest economy on the African continent, Nigeria's manufacturing sector experienced a

resurgence that catapulted it to the top in 2013, supplying a substantial share of goods and services to the West African subcontinent. With substantial accomplishments in the oil industry, Nigeria ranks sixth among the continent's oil producers. Its oil reserves are estimated at 35 billion barrels (5.6×10^9 m^3), accompanied by vast natural gas reserves exceeding 100 trillion cubic feet (2,800 km^3). Beyond energy, Nigeria's agricultural prowess is equally impressive. It secures the sixth spot globally and leads Africa in producing crops such as cocoa, groundnuts, natural rubber, and palm oil.

Despite the positive indicators of development, the country's global reputation has suffered a notable blemish, which has become synonymous with dishonesty, dishonor, and disrespect. This tarnished image is primarily a result of the prevalence of cybercrime, corruption, and insecurity deeply rooted within the nation. These issues have significantly hindered progress across all sectors and have been the foremost impediment to the country's rapid development (Bamiduro & Aremu, 2012). On the international stage, the country ranks third in terms of global internet crime, trailing only the United States of America and the United Kingdom. Shockingly, approximately 7.5 percent of the world's hackers are attributed to Nigeria. Often perpetrated by the youth, commonly referred to as "Yahoo" boys – precursors to the notorious '419' email scammers – these fraudsters are capitalizing on the surge in online transactions, e-commerce, electronic shopping, and messaging systems to carry out their nefarious activities.

Alarming evidence underscores the extent of this problem. The Central Bank of Nigeria (CBN) has reported that a substantial 70 percent of attempted or successful cases of fraud and forgery within the Nigerian banking system occur through electronic channels. Similarly, Adebayo Shittu, a former Minister of Communications, has affirmed the escalating rate of cyber-related offenses, including fraudulent financial transactions and child kidnapping facilitated through Internet communications. Regrettably, this prevailing situation paints a negative portrayal of Nigeria's image, sending unfavorable signals to the international community. Recognizing this reality, the Nigerian government enacted the Cybercrimes Act in 2015 to combat cyber offenses ranging from ATM card skimming to identity theft. The law stipulates penalties such as a seven-year prison sentence for various offenders, an additional seven years for online crimes causing physical harm, and even life imprisonment for offenses leading to fatalities. However, akin to many laws within the country, enforcement poses a significant challenge. The law enforcement of the legislation has contributed to a surge in cybercrimes such as ATM fraud, piracy, hacking, pornography, and email scams.

Consequently, Nigeria's standing on the global stage and within Africa has diminished, owing to the multitude of image-related predicaments that have beset the nation, rendering it a sort of outcast. Furthermore, the international community has grown skeptical of Nigerian citizens due to a range of unsavory actions by both individuals and government officials, which cast the nation in an unfavorable light. This negativity permeates every aspect of the nation's existence, deterring potential investors and stifling both domestic and foreign investments. Moreover, it corrodes public trust in the financial sector and acts as a deterrent to academic excellence. A nation takes immense pride in its positive image, and its citizens find great comfort in identifying with it (Adejumo, 2016). The emergence of the idea of branding a nation's image on the global stage brings about significant economic and political consequences. A nation that employs effective branding strategies can achieve heightened international acknowledgment, enhance its economic potential, and foster stronger international relations.

The pertinent inquiries that occupy the thoughts of researchers include: What are the factors influencing cybercrime in Nigeria? And to what extent does cybercrime influence national image?

Theory Framework

The foundational framework driving this research study is the cyber sovereignty theory. The rationale for adopting this theory stems from its ability to elucidate the correlation between cybercrime and a nation's reputation (McGuinness, 2019). The genesis of the concept of cyber sovereignty can be traced back to the challenges presented by the borderless nature of the internet and the escalating reliance on digital technologies. As the internet expanded and integrated into modern society's fabric, countries found themselves contending with issues concerning cybercrime, data privacy, national security, and the influence wielded by foreign entities in their internal affairs through online platforms (Smeaton, 2019). This notion gained prominence as nations endeavoured to tackle these challenges while safeguarding their own interests and security. It embodies a response to the tension between the aspiration for an interconnected global internet and the imperative to protect national security and local values. This theory posits that a country's digital infrastructure and its citizens' security against cyber threats, including cybercrime, can impact its national image. According to Yang (2019), cyber sovereignty encompasses the concept of a nation's capacity to govern and exert control over its cyber domain, analogous to its physical territory. It underscores a nation's entitlement to formulate regulations, rules, and policies for the Internet and digital technologies within its geographical boundaries (Gbegi & Adebisi, 2014). This concept has gained prominence as nations grapple with managing their online landscapes while ensuring digital-age national security (Smeaton, 2019). Odia and Isibor (2014) contend that when a nation fails to effectively counter cybercrime or safeguard critical digital systems, it can engender negative perceptions about the country's capabilities and governance. Evidently, McGuinness (2019) illustrates that recurrent cyberattacks and cybercrimes can destabilize a country's economy and impede technological advancement.

Consequently, foreign investors and businesses might exhibit reluctance to operate in a nation perceived as having inadequate cybersecurity measures, fearing potential breaches of data or financial losses (Aminu, Hamzat & Haruna, 2015). In the same vein, Adejumo (2016) observes that if a country's populace and enterprises consistently fall victim to cybercrimes, faith in governmental institutions to provide a secure digital environment can corrode. This erosion of trust may extend to international relations, impacting diplomatic ties and trade connections. Thus, cybercrimes can yield ramifications beyond monetary losses, such as jeopardizing critical infrastructure or pilfering sensitive government data. A nation's incapacity to fend off such assaults might indicate vulnerabilities to potential adversaries, potentially leading to geopolitical repercussions (Smeaton, 2019; Aminu et al, 2015). This implies that a nation grappling with cybercrime may face international pressure to bolster its cybersecurity measures, triggering adjustments in domestic policies and regulations that influence digital liberties and privacy. Therefore, the theory empowers nations to uphold their cultural and societal values in the digital realm. By overseeing online content and activities, countries can curtail the dissemination of content that may be construed as offensive, detrimental, or inconsistent with their cultural norms. In a parallel investigation, Shires (2018) observes that the cyber sovereignty theory aids countries in establishing robust data privacy and protection regulations tailored to their citizens' needs. This can forestall data breaches, unauthorized data sharing, and other privacy infringements. Echoing this sentiment, Jork (2015) affirms that sovereignty in the cyber domain bestows nations with greater control over their digital infrastructure, mitigating vulnerabilities to cyber threats and other dangers.

It empowers countries to implement measures fortifying critical infrastructure and safeguarding sensitive information. This signifies that cyber sovereignty aids countries in regulating e-commerce, digital trade, and online financial transactions within their boundaries. This can ensure that economic endeavors align with domestic regulations and contribute to local economic growth.

Concept of Cybercrime

The term "cybercrime" emerges from the fusion of "crime" and the prefix "cyber," drawn from the term "cybernetic," originating from the Greek word "Kubernan," signifying the act of leading or governing. According to Yan (2006), a universally accepted definition of cybercrime remains elusive, even within those tasked with combating it. For instance, Halder and Jaishankar (2011) delineate cybercrime as offenses perpetrated against individuals or groups with a criminal intent to tarnish the victim's reputation or inflict direct or indirect physical or mental harm on them. This is achieved using contemporary telecommunications networks such as the Internet (including chat rooms, emails, notice boards, and groups) and mobile phones (SMS/MMS).

Casey (2004) characterizes cybercrimes as unlawful actions carried out using ICT innovations or electronic devices. The Internet Crime Complaint Center (ICCC, 2010) defines cybercrime as any illicit act committed through any facet of the internet, encompassing browsing, pinging, chatting, and email. Wall (2001) notes that the definition of cybercrime remains ambiguous in legal practice but is commonly employed in political discourse, criminal justice, public discussions, media discourse, and academia. Oriola (2005) portrays cybercrime as encompassing various actions involving deceptive acquisition via the Internet, wherein individuals are manipulated into revealing their banking details due to false promises of substantial but non-existent wealth, which is subsequently liquidated.

Cybercrime entails the exploitation and manipulation of the internet to deceitfully gain advantages from unsuspecting users. Some examples of these offenses include spoofing/phishing, spamming or escrow services, web jacking, and fraudulent messages. In harmony with the aforementioned cybercrime definition, the Free Dictionary Website by Farlex defines internet crime as "a criminal act in which the perpetrator devises a scheme utilizing one or more internet elements to defraud a person of property or any legal interest, estate, or right through false representations."

Various authors hold differing perspectives, but in essence, cybercrime involves distorting factual information or withholding information, often performed by individuals known as scammers, hackers, fraudsters, or "419ners." These activities occur over the internet using interconnected computers, telephones, and other ICT devices. Consequently, the genesis of cybercrime traces back to the advent of computers, telephones, and other ICT innovations.

In Nigeria, cybercrime has evolved into a significant avenue for embezzlement and corporate espionage. Check Point, a global cybersecurity network provider, reported in 2016 that Nigeria ranked 16th in terms of cyber attack vulnerabilities in Africa (Ewepu, 2016). Nigerians, whether within the country or abroad, have garnered a reputation as prolific cybercriminals. The count of Nigerians apprehended for deceptive operations conducted via broadcasting outlets far exceeds that of citizens from other nations. While the internet's role in Nigeria's progress has yielded favorable outcomes in multiple sectors like banking, e-commerce, and education, it has also provided the backdrop for cybercrime proliferation.

Concept of national Image

The Notion of National Perception, Odia and Isibor (2014) explored the idea of national perception as an intricate process in which individuals gather, arrange, and interpret sensory cues to construct a coherent and meaningful understanding of the world. This process of recognizing, categorizing, and imbuing sensory inputs with meaning is not purely objective; it is also shaped by individuals' prior experiences, cultural background, and learning (Dinnie, 2008). Fan (2010) similarly examined the notion of national perception from a perspective of beliefs. In this context, the authors associated it with non-official religious conceptions that fall outside the realm of established religious doctrines. Beliefs hold a significant connection to attitudes and stereotypes, often being considered a component of attitudes. Nevertheless, most scholars emphasize that an individual's mental image of a country is not solely influenced by cognitive attributes; emotional and behavioral elements also play a crucial role. Consequently, while beliefs contribute to the understanding of the concept of country image, they represent only a portion of the overall conceptual framework. Incorporating viewpoints and insights into the concept of country image allows for a more nuanced comprehension (Barbara, 2012).

Godwin and Iro (2013) also examined the concept of country image through the lens of viewpoints and insights. Insights, as a psychological concept, depict the impact of external stimuli on individuals' senses. Insights facilitate the formation of opinions (about objects, individuals, events, etc.) following the process of perception. Barbara (2012) noted that opinions and insights seem to be the most suitable components for framing the concept of country image. As per Anholt's findings in 2000, the image of a country, similar to a brand image, encompasses the subsequent aspects: (1) the recognition of a country's exported goods, (2) the perception of a country's governmental entities among foreign individuals, (3) the perception of a country's attractiveness for investments and immigration, (4) the representation of the country's cultural legacy, (5) the collective mindset of its populace, and (6) the state of tourism within the country. Consequently, the analysis of a country's image can be structured around these six facets: products, governance, cultural heritage, populace, tourism, and investment in human capital and migration.

Factors influence Cybercrime

Previous studies have attributed many factors to the high level of cybercrime in Nigeria. For instance, Osisanya (2020) identifies a number of key factors such as a high rate of unemployment, the quest for wealth, a lack of strong cybercrime laws, and incompetent security on personal devices have coalesced to make cybercrime a significant problem for the country. In another study, Ogbonnaya (2020) argues that delays in court, lack of rule of law, weak judicial system, and weak law enforcement are the main factors that influence cybercrime in Nigeria. The study of Hassan, Lass, and Makinde (2012) confirms that urbanization and negative role models are the key factors that influence cybercrime. Similarly, another study conducted by Okeshola and Adeta (2013) reveals that defective socialization, peer group influence, weak laws, easy access to the internet, and poverty are the motivating factors of cybercrime. Ibikunle and Eweniyi (2013) findings suggest that corruption, peer groups, and the university environment are the key factors influencing cybercrime. In the same vein, Omodunbi, Diase, Olaniyan, and Esan (2016) confirm that cultural background, broken home, moral values, and parental supervision and upbringing are germane factors influencing cybercrime.

The work of Tade and Aliyu, (2011) reveals that the greed of the victims, lack of standards and national central control, and lack of national functional database are the main

factors influencing cybercrime. Emeruwa (2011) also notes that the porous nature of the internet, get-rich syndrome, and lack of e-policing are key factors encouraging cybercrime in Nigeria. In the same perception, Adepetun, (2018) established that lack of network control, poor security in organizations, lack of security technologies, inadequate HR for system handling, and exploitation of insider knowledge are the key factors contributing to cybercrime in Nigeria.

Empirical Review

The preceding research relevant to this study was examined as follows:

Ghafur et al. (2019) noted that Cybercrime encompasses a range of criminal activities and harmful behaviors that significantly impact a nation's reputation. Castillo and Falzon (2018) conducted another study affirming that cybercrime presents a detrimental signal to both a nation's image and its economic growth. Similarly, Shires (2018) illustrated a direct correlation between cybercrime and national image. Mohurle and Patil (2017) highlighted how cybercrime has emerged as a significant avenue for embezzlement and corporate espionage. Phillips et al. (2022) conducted a study demonstrating a clear link between cybercrime and risk exposure, deviant behaviors, and victimization. Holt and Bossler (2014) further verified that cybercrime serves as a potent predictor of national image and deviant behaviors. Ho and Luong (2022) reiterated that cybercrime exerts influence over national image and societal values. Smeaton (2019) and Aminu et al. (2015) also established that cybercrime significantly affects domestic policies and regulations that shape digital liberties and privacy. According to Kigerl (2016), cybercrime can predict a country's cultural legacy. Mezzour, Carley, and Carley (2014) discovered a direct correlation between cybercrime and high levels of corruption. Similarly, Kumar and Carley (2016) identified higher levels of corruption and extensive internet bandwidth as indicators of cybercrime. Anderson et al. (2019) conducted a study that demonstrated cybercrime's association with online fraud, digital piracy, and cyberbullying.

Materials and Methods

The study utilizes a survey design, employing a purposive sampling technique to select 10 lawyers, 10 EFCC officers, 10 ICPC officers, and 10 judges from each of the following cities: Lagos, Abeokuta, Ibadan, Osogbo, Akure, and Ado-Ekiti. This total of 240 participants comprised the study's sample size. The selection of these cities is based on their roles as the state capitals of the six states in the Southwest region of Nigeria. Structured questionnaires served as the data collection instruments for this study. The administration and retrieval of the research instruments were personally conducted by the researchers, assisted by four research assistants. Exploratory factor analysis (EFA) was employed to assess the suitability and practicality of the measurement instruments, utilizing the maximum likelihood method and Promax rotation.

The communalities for each variable exceed 0.50, and the Kaiser-Meyer-Olkin (KMO) test yields a value of 0.862. Additionally, Bartlett's test for sphericity demonstrates a statistically significant result at a 1% significance level. These indicators collectively affirm the factorability of the study's data (Morin et al., 2020; Edwards, 2021). (Refer to Table 1 for details). Upon collecting the data, a combination of descriptive and inferential statistics was employed to analyze the gathered information.

Table 1: *Exploratory factor analysis for testing validity of the constructs*

Cybercrime questionnaire	1	2
I feel that the government should play a more active role in combating cybercrime.	.823	
I believe that cybercrime is a serious threat to individuals and organizations	.821	
I take cybersecurity precautions such as using strong passwords, two-factor authentication, and keeping my software up to date to protect myself from cyber threats	.810	
I am confident in my ability to protect my personal information and online activities from cyber threats.	.814	
I believe that cybersecurity education and awareness programs are effective in reducing cybercrime.	.799	
National Image questionnaire		
I have a positive perception of my country's national image on the international stage.		.789
I am proud of my country's national image and what it represents to the world		.826
I believe that my country's national image impacts its diplomatic relationships and international influence.		.837
I think that my country's national image is accurately represented in the global media.		.796
My personal experiences align with the positive or negative national image that my country projects.		.815

RESULTS

Socio-demographic characteristics

The background information included gender, age, and education. Gender composition revealed that most of the respondents, 59% were males while female respondents accounted for 41%. With regard to age, it was revealed that only 10% of the respondents were aged below 30 years, those of the age group 31 to 40 were 30% of the respondents. Those aged groups between 41 to 51 and 52 above accounted for 48% and 12% of the respondents respectively. In respect of education, bachelor's and master's degree holders were at 40% and 55% of the respondents respectively, while doctorate degree holders accounted for 5% of the respondents.

Factors Influencing Cybercrime in Nigeria

Table 2: *Mean and Chi-Square results of perceived factors influencing cybercrime in Nigeria*

Statement	Mean	Chi-Square	Remark
High Rate of Unemployment	4.5304	124.993 (P<.05)	Accepted

The Quest for Wealth	4.4696	117.980 (P<.05)	Accepted
Weak Judicial System, And Weak Law Enforcement	4.4730	110.682 (P<.05)	Accepted
Incompetent Security on Personal Devices	4.4966	120.047 (P<.05)	Accepted
Broken Home, Moral Values, And Parental Supervision	4.4998	121.619 (P<.05)	Accepted
Negative Role Models and Poverty Peer Groups	4.4257	I03.973 (P<.05)	Accepted
Lack of a National Functional Database	4.4189	87.676 (P<.05)	Accepted
Grand Mean	**4.4738**		

Table 2 shows that all the factors listed in items 1-7 are perceived to influence cybercrime in Nigeria. The grand mean of 4.4738 and the p-value of 0.000 indicate that there is a high level of agreement that these factors are strong predictors of cybercrime in Nigeria. This implies that the major factors influencing cybercrime in Nigeria are: High rate of unemployment, Incompetent security on personal devices, Broken homes, Lack of moral values and parental supervision, Weak judicial system, Weak law enforcement, The quest for wealth, Negative role models and poverty peer groups and Lack of a national functional database. These findings are consistent with those of previous studies (Osisanya, 2020; Ogbonnaya, 2020; Hassan et al., 2012; Okeshola & Adeta, 2013).

The high rate of unemployment in Nigeria is a major driver of cybercrime. Many young people are unemployed and have few opportunities to earn a living. They may turn to cybercrime as a way to make money. The lack of security on personal devices is another major factor. Many people do not take the necessary steps to secure their devices, making them vulnerable to attack. Broken homes and the lack of moral values and parental supervision can also contribute to cybercrime. Children who grow up in unstable homes or without strong moral guidance may be more likely to engage in criminal activity.

The weak judicial system and weak law enforcement also make it difficult to prosecute cybercrime cases. This impunity can embolden criminals to continue their activities. The quest for wealth is another motivation for cybercrime. Some people are motivated by the lure of easy money to commit cybercrimes. Negative role models and poverty peer groups can also influence people to engage in cybercrime. People who are surrounded by negative influences may be more likely to see cybercrime as a way to get ahead. The lack of a national functional database makes it difficult to track cybercrime cases and identify criminals. This can make it more difficult to prevent and prosecute cybercrime.

Table 3: *Path analysis (Direct Effect)*

Path	β-value	t-value	p-value	[95% Conf. Interval]	
CC→NI	-.7476979	-7.77	0.000	.5591684	.9362275
Constant	.9075367	7.63	0.000	.6745525	1.140521

Note: CC = Cybercrime, NI= National Image

Table 3 illustrates a notable inverse correlation between cybercrime and a nation's image. Specifically, as the incidence of cybercrime escalates, the national image diminishes. The robust beta coefficient of -0.7476 underscores the substantial adverse impact of cybercrime on a country's image. The p-value of 0.000 attests to the statistical significance of this correlation. This study aligns with the research conducted by Ghafur et al. (2019), which underscores that cybercrime encompasses a spectrum of criminal activities and detrimental behaviors that wield substantial influence over a nation's reputation. In a separate investigation, Castillo and Falzon (2018) substantiate the assertion that cybercrime sends adverse signals, adversely impacting both a nation's image and its economic prosperity.

Similarly, Shires (2018) has provided evidence of a direct connection between cybercrime and a nation's image. Mohurle and Patil (2017) shed light on how cybercrime has emerged as a significant conduit for embezzlement and corporate espionage. Furthermore, Phillips et al. (2022) conducted a study elucidating a clear nexus between cybercrime and heightened risk exposure, deviant behaviors, and victimization. Holt and Bossler (2014) offer additional confirmation that cybercrime serves as a robust predictor of both a nation's image and deviant behaviors. In essence, cybercrime has the potential to undermine a nation's image through various channels. It can result in financial setbacks for businesses and individuals, tarnish reputations, erode trust in the government, heighten fear and anxiety among citizens, and foster a negative perception of the country on the global stage.

The findings gleaned from this study strongly underscore cybercrime as a grave threat to Nigeria's national image. To safeguard the country's reputation, it is imperative that the government and relevant stakeholders take proactive measures to prevent and combat cybercrime.

DISCUSSION

The first objective was to determine the major factors influencing cybercrime in Nigeria. The result showcases that high rate of unemployment, incompetent security on personal devices, broken homes, lack of moral values and parental supervision, weak judicial system, weak law enforcement, the quest for wealth, negative role models and poverty peer groups and Lack of a national functional database are major factors influencing cybercrime in Nigeria. These findings align with Osisanya (2020) that the main factor influencing cybercrime in Nigeria are weak judicial system, weak law enforcement, the quest for wealth broken homes, lack of moral values and parental supervision, weak judicial system, weak law enforcement, and the quest for wealth. In another study, Ogbonnaya (2020) attests that weak law enforcement, the quest for wealth, negative role models and poverty peer groups and Lack of a national functional database are major factors influencing cybercrime in Nigeria. In the same vein, Hassan et al. (2012) reaffirm that weak judicial system, weak law enforcement, the quest for wealth broken homes and poverty peer groups and Lack of a national functional database are major factors influencing cybercrime in Nigeria. While the study by Okeshola and Adeta (2013) confirms that the high rate of unemployment in Nigeria is a major driver of cybercrime. The implication of this finding is that hifg rate of unemployemnt, lack of security on personal devices , broken homes and the lack of moral values and parental supervision the weak judicial system and weak law enforcement make the country a lion den for the foreign investors and indigins.

The evidence presented also indicates an inverse relationship between cybercrime and national image in Nigeria. The study concludes that socio-economic and cultural factors play a significant role in fostering cybercrime in the country. Additionally, it emphasizes the severe negative consequences of cybercrime on the nation's image. To enhance Nigeria's

reputation and reduce cybercrime rates, addressing these factors and implementing effective measures are deemed crucial. Moreover, the study aligns with existing research by Ghafur et al. (2019), highlighting the diverse criminal activities within cybercrime and their substantial impact on a nation's reputation. Castillo and Falzon (2018) support the notion that cybercrime sends adverse signals, negatively affecting both a nation's image and its economic prosperity. Shires (2018) provides evidence of a direct link between cybercrime and a nation's image, while Mohurle and Patil (2017) shed light on cybercrime as a significant conduit for embezzlement and corporate espionage. Furthermore, Phillips et al. (2022) establish a clear connection between cybercrime and heightened risk exposure, deviant behaviors, and victimization. Holt and Bossler (2014) confirm that cybercrime serves as a robust predictor of both a nation's image and deviant behaviors. Essentially, cybercrime can undermine a nation's image through various channels, causing financial setbacks, tarnishing reputations, eroding trust in the government, heightening fear and anxiety among citizens, and fostering a negative global perception of the country.

CONCLUSIONS

This study examines the influence of cybercrime on national image. Specifically, to identify factors influencing cybercrime in Nigeria and to determine the extent to which cybercrime influence national image. The study establishes that high unemployment rates, inadequate security on personal devices, broken homes, lack of moral values and parental supervision, a weak judicial system, weak law enforcement, the pursuit of wealth, negative role models and poverty peer groups, and the absence of a functional national database are major factors influencing cybercrime in Nigeria. Evidence also reveals that cybercrime has an inverse influence on national image in Nigeria. The study, therefore, concludes that there is a widespread perception that various socio-economic and cultural factors contribute significantly to cybercrime in Nigeria. Additionally, the study underscores the severe negative consequences of cybercrime on the nation's image. Addressing these factors and effectively tackling cybercrime could be crucial for improving Nigeria's reputation and reducing cybercrime rates in the country.

RECOMMENDATIONS

Based on the findings and conclusion, the following recommendations are made:

Enhance Cybersecurity Measures: Given the significant adverse impact of cybercrime on a nation's image, it is crucial for governments and organizations to bolster their cybersecurity measures. This includes investing in advanced technology, training personnel, and implementing robust cybersecurity policies and protocols to mitigate the risk of cyberattacks.

Public Awareness and Education: To combat cybercrime effectively, there is a need for comprehensive public awareness and education campaigns. Citizens should be educated about the risks associated with cybercrime, how to protect themselves online, and how to report suspicious activities. Increasing awareness can contribute to a more vigilant and cyber-resilient society.

International Collaboration: Cybercrime often transcends national borders, making it essential for countries to collaborate internationally in tackling this threat. Nigeria should engage in partnerships with other nations, law enforcement agencies, and international organizations to share intelligence, expertise, and resources for a coordinated response to cybercrime. This can help in tracking down cybercriminals and bringing them to justice.

These recommendations aim to address the serious threat of cybercrime to Nigeria's national image and reputation by strengthening cybersecurity, raising public awareness, and fostering international cooperation in combating cyber threats.

Practical Implications

The findings of this study have important implications for the prevention and control of cybercrime in Nigeria. The government and other stakeholders need to address the factors that are driving cybercrime, such as unemployment, lack of security, and weak law enforcement. They also need to raise awareness of cybercrime and its consequences. By taking these steps, Nigeria can reduce the incidence of cybercrime and create a safer online environment for its citizens.

Data Availability Statement: The study incorporates the original contributions, and for additional inquiries, please contact the corresponding author.

Acknowledgments: We express our gratitude to TETFUND and the Management of Osun State Polytechnic for their invaluable support, which made this research possible. Special appreciation goes to the respondents who promptly completed the questionnaire, and we also acknowledge the dedication of our research assistants in administering the survey.

Conflicts of Interest: ” The authors declare no conflicts of interest in relation to the content presented in this paper/article..

REFERENCES:

Adejumo, D.A (2016) Exploring Impact of Public Policy in branding a nation’s Image for Nigeria among Nigerians: A case Study of Economic and Financial Crimes Commission, Nigeria. M.sc Dissertation at University of Gloucestershire, United Kingdom.

Adepetun, A. (2018). Nigeria mobile phone penetration hits 84 percent. The Guardian.Retrieved from: www.guardian.ng.

Anholt, S. (2002): Foreword to the Special Issue on Country Branding. *Journal of Brand Management.* 9(5); 229-239.

Bamiduro J. A., & Aremu, M. A. 2012. Assessment of the need for and effectiveness of the re-branding in Nigeria. *International Journal of Management and Administrative Sciences*, 1(4): 11-22.

Barbara, J. (2012). Theoretical and practical issues in measuring country image. PhD Thesis of Corvinus University of Budapest.Casey, E. (2004). *Digital evidence and computer crime*. St. Louis, MO, Elservier Press.

Clinton, H. (2019). Internet Rights & Wrongs: Choices and Challenges in a networked World. The George Washington University, Washington D. C., American Rhetoric. Online Speech Bank.

Dinnie, K. (2008). *Nation branding: Concepts, issues, practice*. Oxford, United Kingdom: Butterworth-Heinemann.

Ewepu, G. (2016). *Nigeria loses N127bn annually to cyber-crime* - NSA available at: http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-annually- cybercrime –nsa

Emeruwa, O.U. (2011). Nigerian entertainment industry and piracy. *The Guardian online*.

Available at http://www.ngrguardiannews.com/editorialopinion/article.

Fan, Y. (2010). Branding the nation: Towards a better understanding. *Place Branding and Public Diplomacy*, 6(2), 97-108.

Godwin, U.O and Iro,,A. (2013). Image Re-branding in a Fragile State: The Case of Nigeria. *The Korean Journal of Policy Studies*, Vol. 28, No. 2 (2013), pp. 81-107.

Halder, D., & Jaishankar, K. (2011): *Cybercrime and the Victimization of Women: Laws, Rights, and Regulation*. Hershey, PA, USA: IGI Global. ISBN 978-1-60960830-9.

Ibikunle F. and Eweniyi O. (2013): Approach to cyber security issues in Nigeria: Challenges and Solutions. International Journal of Cognitive Research in Science Engineering and Education (IJCRSEE), Vol. 1, No. 1.

ICCC (2010). *Internet crimes complaint center reports.* Available online at http://www.ic3.gov/faq/default.aspx . Accessed march 18,2013.

Jork J. C (2015). The Myth of a Borderless Internet. The Atlantic, 03.06.2015. Available at: https://www.theatlantic.com/ technology/archive/2015/06/the-myth-of-a-borderless-internet/394670.

McGuinness D (2019). How a Cyber Attack Transformed Estonia. BBC news, 27.04.2017. Available at: https://www.bbc.co.uk/ news/39655415.

Odia, E. O., & Isibor, F. O. (2014). Strategic Approach to Nation Branding: A Case of the Nigeria Brand. *International Journal of Business and Management*, *9*(3), 204.

Ogbonnaya, M. (2020)**.** Nigeria's financial institutions' vulnerability to cybercrime. Available at https://enactafrica.org/enact-observer/nigerias-financial-institutions-vulnerability-to-cybercrime.

Omodunbi, B. A., Diase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cyber crime in Nigeria: Analysis, detection and prevention. *FUOYE journal of Engineering and Technology, 1*(1), 2579-0617.

Oriola, T. A. (2005). Advance fee fraud on the internet: Nigeria's regulatory responses. *21st Computer Law and Security Report; P. 237.*

Osisanya, S. (2020). National security versus global security. *UN Chronicle*.

Oyetibo T. (2019). Cyber-Security in Nigeria: The Role of CBN and Other Stakeholders. Available at https://tayooyetibolaw.com/cyber-security-in-nigeria-the-role-of-cbn-and-other-stakeholders/

Röhrig W., Smeaton R. (2019). Cyber Security and Cyber Defence in the European Union. Cyber Security Review.

Sembiring, M.J., Fatihudin, D. Mochklas, M., and Holisin, I (2020). Banking Employee Performance During Pandemic Covid-19: Remuneration and Motivation. *Journal of Xi'an University of Architecture & Technology.* 64- 72.

Shires J. (2018) Between Multistakeholderism and Sovereignty: Cyber norms in egypt and the gulf States. Harward Kennedy School. Belfer Center for Science and International Affairs. October 12, 2018. Available at: https://www.belfercenter.org/ publication/between-multistakeholderism-and-sovereignty-cyber-norms-egypt-and-gulf-states.

Tade, O. & Aliyu, I. (2011). Social organization of internet fraud among University Undergraduates in Nigeria. *International Journal of Cybercrime* 6 (3): 420-448.

Wall, D. S. (2001). *Crime and the internet.* London: Routledge publishers.

Yin, R. K. (2006). *Case study research: design and methods. (2nd Edition).* Newburg Park: Sage publishers.

Yang Yi (2019). Full Text of BRICS Leaders Xiamen Declaration. Xinhua news, 04.09.2017. Available at: http://www.xinhuanet. com/english/2017-09/04/c_136583396_2.htm.