Intelligence, Financial Crimes Commission and War against Cybercrime among Youths in the Federal Capital Territory in Nigeria

Muyiwa B. AFOLABI PhD & Ikiyouleimo Goodluck DOGI

[1]Department of Intelligence and Security Studies, College of Social & Management Sciences, Afe Babalola University. Ado-Ekiti, Ekiti State, Nigeria.
[2]Department of Intelligence and Security Studies, Open and Distance Learning Center, Afe Babalola University. Ado-Ekiti, Ekiti State, Nigeria.
Email: afobam1840@gmail.com, afolabimb@abuad.edu.ng & dogigoodluck@odl.abuad.edu.ng

Abstract

Without any tittle of doubt, the proliferation of digital technologies has brought about unprecedented opportunities for connectivity and innovation, but it has also given rise to a surge in cybercrime, particularly among the youth population, despite the efforts of the Economic and Financial Crimes Commission (EFCC) to combat this menace in Nigeria. This study assesses the impact of EFCC intelligence operations on cybercrime in the Federal Capital Territory (FCT) of Abuja, Nigeria. The study derives its data from primary and secondary sources. One hundred and fifty (150) questionnaires were administered and were returned valid for the analysis. The collected data were analyzed through statistical methods. A major finding in this study revealed a significant concern among the public regarding the potential consequences of cybercrime on Nigeria's national security. And also, findings of the study reveals that well-executed intelligence operations enhance the efficiency of cybercrime investigations, aiding in the identification and apprehension of cybercriminals. Efforts have been made to curb the menace, but they seem unproductive when compared to the degree of the menace. To this effect, this study recommends, among others, that there is a need for the government, in liaison with the EFCC, to develop strategies to reduce or possibly curb cybercrime in order to be proactive and reactive. There is a need for more analytical, technical, or technological capabilities in order to curb cybercrime and be able to detect and analyze cyberattacks. It is important for the nation to rebrand its image; there should be vigorous inter-agency synergy, cooperation, coordination, and collaboration among law enforcement agencies instead of competition in order to ensure national security.

Keywords: Cybercrime, intelligence, youth & financial crimes commission

Introduction

In recent times, the issue of cybercrime has become deeply ingrained in the lifestyle of today's youth, despite ongoing efforts by authorities such as the Economic and Financial Crimes Commission (EFCC) to curb this menace. Intelligence operation is the process by which governments, military groups, businesses, and other organizations systematically collect and evaluate information for the purpose of discovering the capabilities and intentions of their rivals. With such information, or intelligence, an organization can both protect itself from its adversaries and exploit its adversaries' weaknesses. The successful conduct of intelligence operations requires a successful synchronization of intelligence, surveillance, and reconnaissance (Richard, 2017).

Depending on the type of organization involved, intelligence operations can result in many different types of information. Information regarding foreign nations, gathered by governmental intelligence agencies, constitutes strategic or national intelligence. Strategic intelligence commonly encompasses national security, political, economic, and social trends in the target nation. Specially trained military or civilian analysts generate military intelligence, encompassing details such as the strengths, weapons technology, and estimated military capabilities of actual or potential adversaries. On the other hand, industrial intelligence refers to information collected by a business firm regarding its competitors in the marketplace. Political intelligence, as practiced in the United States, is usually concerned with ascertaining the campaign strategy of a political opponent. Political intelligence can also apply to the efforts of a ruler to uncover conspiracies. Counterintelligence embraces the wide variety of activities undertaken to forestall an adversary's intelligence efforts. This is accomplished by physically protecting one's own sensitive information and by penetrating and disrupting hostile intelligence organizations (Berkowitz, 2016). Intelligence operations are wide-ranging activities conducted by intelligence staffs and organizations to provide commanders and national-level decision makers with timely, relevant, accurate, predictive, and tailored intelligence. For the purpose of this study, intelligence operation is the process by which the EFCC and other related organizations systematically collect and evaluate information for the purpose of discovering the capabilities and intentions of cybercriminals. The six steps of an intelligence process are planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback.

In Africa, cybercrimes have been indigenously named. For instance, in Nigeria, it is called ‘Yahoo Yahoo’ while the perpetrators are called ‘Yahoo boys’. In Ghana, it is called ‘Sakawa’ or ‘yahoo yahoo’ (Coonsom 2017) and ‘Faymani’ in Cameroon (Oumarou 2016). In Nigeria, the majority of cybercriminals are young people and are found in universities. Yahoo boys are youths involved in cybercrimes using e-mails. This social tag originated via the mode employed by Yahoo boys in defrauding, which involves sending sinister and deceptive e-mails using Hotmail, Gmail, Yahoo Mail, and the like. Alubo (2015), Informs us that the web has created a platform for fraudsters to engage in advance-free fraud via the sending of spam e-mails. This act, Alubo notes, is called 419, and perpetrators are called Yahoo boys. They usually make use of free e-mail accounts (e.g., Yahoo, Gmail, Hotmail, etc.) to communicate with their targets.

Some individuals in Nigeria have embraced cybercrime as a way of life. Many have become rich, while others have been caught by the law (Tade & Aliyu 2016). Thus, new crime is denting and drilling holes in the economy of the nation. For example, a recent report by the internet crime complaint center, which is a partnership between the FBI and America's National White Collar Crime Center, revealed that Nigeria now ranks third among the top ten sources of cybercrime in the world (Abdulhamid *et al., 2*015). Also, the Central Bank of Nigeria (CBN), in its banking sector supervision report, revealed that the Nigerian banking sector lost N7.2 billion to internet fraud (Ajewole, 2015). Losing N7.2 billion in a developing economy such as ours is not something to be proud of.

Studies have been conducted on the emergence of the yahoo boy’s subculture within the social organization of internet fraud in Nigeria (Tade & Aliyu 2016), ICT and perpetration of cybercrime, and the cost and attractiveness of cybercrime (Kshetri 2016). In a somewhat similar study conducted in Ghana, Warner (2016), reports the use of a klepto-theological paradigm created to abet the perpetration of internet crime. He calls this Sakawa. According to Warner, Sakawa serves two main functions: it protects cybercriminals and ensures their financial success. Melvin and Ayotunde (2015) treat cybercrime as a unit and analyze it as such from purely philosophical and psychological perspectives. However, this attack by humans through machines (Jaishankar 2015) has now incorporated spiritual elements in Nigeria.

Demonstrating the gravity of the problem of cybercrime in the country recently, a young Nigerian musician, Naira Marley, and a couple of other musicians released a hit song called "Am I a Yahoo Boy?" There is even what is called "night browsing," where, for a fee, they stay on the internet all through the night to carry out their businesses. The boys often team up to practice their businesses in order to get ideas from each other (Melvin & Ayotunde, 2015).

To this end, the more desperate among them have had to resort to spiritual means to enhance their businesses. This is referred to as "Yahoo Plus". Yahoo Plus is an advanced form of Yahoo, whereby the "yahoo boys" employ traditional spiritual means like voodoo or juju to hypnotize their victims into doing their bidding and parting with whatever amount of money they request (Ayotunde, 2016). The Yahoo boys indulge in occultic ritual practices to enhance their potential to defraud people. It involves employing traditional spiritual means like voodoo or juju to ensure that the cybercriminal hypnotizes his victims and thereby brightens the swindler's chances. Once this is successfully done, the victim is guaranteed to keep remitting money from wherever he or she is in the world. There are various strategies deployed to achieve this feat. The yahoo boy approaches a spiritualist or diviner who consults the "oracle" or the "gods". He is then given diverse options for rituals to perform. These include sleeping in a coffin for certain numbers of days, sleeping in the cemetery, and bringing human body parts. In other words, he kidnaps a victim, kills him or her, and extracts the body parts needed. Some are even told to sleep with virgins as part of the rituals. Most often, young girls are kidnapped, raped, and sometimes killed by these ambitious young people. Other forms of rituals performed include sleeping with pregnant women or mad women, and sometimes the yahoo boy may be told not to take his bath for days or months as doing so may have terrible repercussions (Aliyu, 2015).

The situation is such that international financial institutions now view paper-based Nigerian financial instruments with skepticism. Nigerian bank drafts and checks are not viable international financial instruments anymore. Nigerian Internet Service Providers (ISPs) and email providers are already being blacklisted in e-mail blocking blacklist systems across the Internet. Also, some companies are blocking entire Internet network segments and traffic that originates from Nigeria. Newer and more sophisticated technologies are emerging that will make it easier to discriminate against and isolate Nigerian e-mail traffic. To this extent, various agencies, such as the Economic and Financial Crimes Commission (EFCC), have taken vast measures through intelligence processes in order to be proactive and reactive in dealing with the menace of cybercrime in the country.

Security and intelligence agencies in Nigeria have implemented various measures to combat the menace of cybercrime. Several security and intelligence operations in liaison with foreign agencies have been successful, while others have proven stagnant. Intelligence operations in this sense refers to the process by which governments, military groups, businesses, and other organizations systematically collect and evaluate information for the purpose of discovering the capabilities and intentions of their rivals (Richard, 2017). Intelligence operations consist of a large number of tasks, phases, subphases, and individual activities, all of which contribute to the complex structure of the intelligence project. Big intelligence ventures with several operations, run by extent and structure, have a very large number of stages and activities, and usually last long (ed. Rodney, 2016). The connections between phases and activities that make up the operation are numerous and come from the complex structure of the operation and of the use of the resources (George, 2014). A large number of individual stages of intelligence activities, but also a number of connections and relations between them and between them and the environment or security milieu in which they are carried out, contribute to the complexity of the process of the realization of an intelligence operation (Manojlović, 2018).

The Economic and Financial Crime Commission (EFCC) was established in 2003 and has made giant strides to rid Nigeria of the popular advance fee fraud and cybercrime, otherwise known as 419 or the Nigerian Scam. It is a major tool for fighting official corruption in Nigeria and money laundering. EFCC partners with several agencies like the FBI, metropolitan police, German police, Canadian police, United States Agency for International Development (USAID), Department for International Development (DFID), the World Bank, the United Nations Office on Drugs and Crime (UNODC), and the Commonwealth Secretariat, etc.

In the past, the Economic and Financial Crimes Commission has conducted intelligence operations in collaboration with agencies within and outside the nation, such as the Federal Bureau of Intelligence, in order to curb the menace of cybercrime and bring the perpetrators to book. According to FBI legal attaché Ahmadi Uche, a sweep operation was conducted from May through September of 2019 with the EFCC, focused on dismantling the most significant cybercriminal enterprises. The EFCC said a “sizeable number” of 77 Nigerian suspects had been detained since August 2022 for alleged computer-related crimes or fraud under “Operation Rewired”, in coordination with the FBI. The efforts in coordinating the EFCC/FBI joint intelligence operations in Nigeria recorded tremendous success against the infamous Yahoo boys. According to the EFCC’s Director of Information, Mohammad Abba, the EFCC recovered from the arrested fraudsters the sum of $169,850 as well as the sum of N92m. Despite these efforts by the EFFC to combat the menace of cybercrime, it is evident that the rate of this menace has relatively increased in comparison to previous years. The world is becoming more globalized, and this has made it easier for these criminals to successfully exploit their victims.

Statement of the Problem

Cybercrime constitutes a major threat to Nigeria. As it stands, cybercrime affects the economy of Nigeria in various sectors. The lack of confidence in the banking sector as a result of the impact of cybercrime is damming the economy. The impact of cybercrimes on the Nigerian economy is becoming compelling and manifests to many as computer literacy increases, adding that organizations seem to pay less attention to security in contrast to the more technology that these scammers adopt. In Nigeria, organizations are busy adopting information technologies without commensurate investment in information security. This is a predisposition to cybercrime because Nigerian society is technologically investing its way into cyber insecurity.

The growing rate of this crime has the capability of wiping out our developmental gains, retarding growth fortunes by many decades, and most importantly, affecting the national security of the nation at large. The inability of the Economic and Financial Crimes Commission, through its intelligence operations, to make sure the cybercrime rate is reduced, the safety of lives, property, and organizations is assured, and the alarming prevailing continuous cybercrime issues in the country are all sources of concern. The sources of cybercrime issues in the country are too numerous to mention and cannot be blamed on one arm of the system. Therefore, dealing with cybercrime constitutes a great problem for the Nigerian government and its established agencies.

Objectives of the Study

The aim of this study is to assess the impact of the EFCC intelligence operations on Cybercrime in Nigeria, this was achieved through the specific objective are to;

i. Assess the impact of cybercrime on Nigeria's national security

ii. Evaluate the impacts of intelligence operations by the EFCC on curbing cybercrime and;

iii. Identify the challenges faced by the EFCC in combating cybercrime

Overview of Cybercrime in Nigeria

Recently, a report indicated that cybercrime has been an eluding factor in cyberspace transactions in Nigeria, where cybercrimes and computer-related crimes are endemic. The integration of computer technology as a global issue is accessible through the use of information, communication, and technology and is at stake (Dillon *et al*, 2016). With the opportunity opened to the general public in use for viable objectives, certain high-level crimes are committed, and some of the perpetrators of these crimes are referred to as 'Yahoo boys' syndrome. They took advantage of cyberspace transactions available on the internet to defraud the unsuspected victims, who are mostly foreign transactions in thousands and millions of dollars. Fraudulently, they represent themselves as having particular goods to sell or that they are involved in shipping or in a loan scheme. Most of the perpetrators - criminals or Yahoo boys - take advantage of some people looking for spouses through the internet. These criminally minded individuals will have a discussion with the victims through the internet, and they will pretend to be interested and loving. Before the victim realized it, the criminals would have succeeded in luring them to send dollars to facilitate travel documents (Ehimen & Bola, 2017).

Cybercriminals, falsify documents and tell all sorts of lies to get money or that they are beneficiaries of a thousand dollars in a trust account, but they need a little money to secure the services of a counselor to claim the trust fund. Cybercrime in Nigeria is difficult to prove and thus requires the knowledge of experts in computer technology and internet protocols. In Nigeria's battle against cybercrimes, efforts have been put in place by directing the sources and channels through which cybercrimes are perpetrated, which are generally targeted at individuals and not directly at computer systems; hence, they require less technical expertise on the part of the criminals (Ehimen & Bola, 2017).

Nigeria is losing about 80 million dollars a year to software piracy. The report was the result of a study conducted by the Institute of Digital Communication; a market research firm based in South Africa. Also, the American National Fraud Information Center reported Nigerian money offers as the fastest online scam, up to 90% in 2015. The Center also ranked Nigeria's cybercrime impact per capita as exceptionally high. Email scams and spam are the most repulsive phenomena among cybercrime; these are ways used to present false financial investment (This Day, 2015). Nigeria's image is in question and has been tarnished as a result of her citizens' involvement in cybercrime. The criminals send an email stating that the victim is the named beneficiary of a will of an estranged relative and stands to benefit the estate or the trust fund. Sometimes they used online charity; the criminals sent emails to the victims soliciting funds and assistance from charitable organizations that did not exist (Akano, 2016). This discussion is not meant to portray Nigeria as the only country that engages in these types of crimes. Although electronic scams or spam emails are generally believed to be linked to Nigeria, the scam is now prevalent in many other African countries, and the targets are usually innocent individuals who could be anywhere in the world. The shift in the act has now extended to text messages. With the increased use of cell phones, text messages are sent to mobile users to lure the victim into captivity. In the mist of their act, a mobile user will receive a text message congratulating the user for winning a certain amount of money in a promo by directing the user to call a particular number to claim the prizes or a package sent from the US to be delivered, but someone has to pay doorstep delivery or clearing agent fees. The criminals have developed different strategies aimed at luring their victims (Akano, 2016).

In an attempt to fight the menace of cybercrime, the EFCC suggested that for Nigeria to fight the prevalent challenges of a growing menace of cybercrimes and cyberterrorism, there is a need for cyber security experts—nothing less than one million—in the next two years. And analysts of crime further stressed that Nigeria has to prepare for cyber warfare to protect its economy in the 21st century and that in 2015, an estimated $1 trillion was lost to cyber-related frauds globally, 'although only $390 billion was reported for obvious reasons (The Economic Times, 2015). Although the Nigerian government is silent on the awards of contracts as to the true picture of 'internet surveillance for the purpose of gathering intelligence and national security'(hanging sentence In a country of capacity development like India, it is targeting five million cyber security experts from now to the next three years. Currently, North Korea has already sponsored 15, 000 cyber security experts well trained to defend the cyberspace of their country, while China has over 25 million cyber commandos. Recently, the Nigerian government awarded a contract to Elbit Systems, an Israeli firm worth $ 40 million, a cyber-intelligence expert, for the purpose of spying on and monitoring phone conversations, texting, and reading private email messages (The Economic Times, 2015). Although the Nigerian government is silent on the awards of contracts as to the true picture of 'internet surveillance for the purpose of gathering intelligence and national security'. The opinion of the Nigerian citizens across was not the nature of the contract that worried neither the citizens nor the company profile, but the company is reputed as being 'a world leader in the fields of intelligence analysis and cyber defense, with proven solutions highly suitable for countries armies and critical infrastructure sites' (The Economic Times, 2015).

Naturally, the contract should not have been a source of worry to any right-thinking individual since its purpose is to "track down terrorist activities online." The worry comes from the fact that history is replete with governments of different countries abuse of such enormous power that gives them legitimate access to their citizens' private lives. So even though it was rumored that the federal government awarded the contract for the purpose of tracking and fighting the online activities of the Boko Haram members, Nigerians in general were quick to be critical, and maybe to justify their fear, the federal government has been silent on the matter.

The general manager of Elbit, Yehuda Vered, announced that 'Elbit Systems will supply its Wise Intelligence Technology (WiS) system to an unnamed country in Africa under a new $40 million contract. For intelligence analysis and cyber defense'. A cyber intelligence expert and ethical hacker view that 'this project will be more offensive than ordinary intelligence gathering or record-keeping systems, classifying it as a 'Black Operation Programme'. And further opined that monitoring systems with or without the Elbit Systems contract, the facts finding of experts that our online and offline extension activities are already being monitored. 'The internet as a whole has no privacy; the biggest technology being used in the world today is the biggest spy project ever created in the world (Akano, 2015).

Another cyber security expert said that 'this is one of the most far-reaching policies ever designed in Nigeria's history to invade the privacy of citizens by secretly awarding Elbit Systems a spy contract on Nigerian citizens. As usual, the justification is that only by having access to our confidential communication can the enforcement agencies and security services keep us safe from criminals and terrorists. He further stressed that maintaining privacy on the internet is nearly impossible; if you forget to enable your protection, click on the wrong link, or type the wrong thing, by implication, you permanently attach your name to a possible anonymous service you are using. If the director of the Central Intelligence Agency (CIA) cannot monitor his privacy on the internet, then we don't have hope' (Yinka, 2015).

The rapid use and communication of cyberspace activities today and the medium of tracking citizens are enormous. For example, Google tracks us both on its pages and other pages it has access to, as well as on its range of Android devices. Same with Facebook, while others use social media. For example, Facebook correlates your online behavior, and even your cell phone has location data. This is a clear case of all-around surveillance. We are all being monitored and watched at all times, and that data has been stored forever. These available data can be utilized and analyzed effectively in tracking cyberspace criminals' activities (Groene & Todd, 2016). Cybercrime is a global practice today, particularly in Nigeria, where it has become a predominant practice whereby the regulations for these crimes are newly established for the purpose of tackling cybercrime threats. In full compliance with the implementation and enforcement of the Cybercrimes Act 2013, the government shall, in conjunction with other stakeholders such as the EFCC, create a unit of cyber security experts (Yinka, 2015). The formalization of the countries' legal instruments and the implications arising from the ICTs are essential in fighting this menace. The criminals take advantage of innocent citizens, ICT Corporation, and the infrastructure of the government in carrying out their acts, and that is why there is a need for the provision of software trackers by internet service provider ISPs to monitor cybercrimes and make use of patrol units so as to strategize the trace and track of the criminals and ensure that awareness among the general public on cyber security information has been ensured (Akano, 2015).

Before now, the country had become a domicile for economic and financial crime perpetrators. Corruption, lack of accountability, economic mismanagement, and fraudulent activities have been the irritations of the economy. The establishment of the EFCC Act was therefore a major departure from the past, enabling laws for fighting economic and financial crimes. In terms of power, functions, and duties, the commission has high-level support from the presidency, the legislature, and other key securities and law enforcement agencies in Nigeria.

According to EFCC Handbook Information 1, the commission has the power to cause an investigation to be conducted as to whether anybody has committed an offense under the Act. It can also investigate whether anyone is in the process of committing offenses under the Act. Investigate the properties of any person if it appears to the commission that the person's lifestyle and extent of the properties are not justified by his source of income. The commission is also charged with the responsibility of enforcing the following laws:

i. The Advance fee fraud and other related offences Acts 1995 as amended.
ii. The failed banks (Recovery of Debts) and financial malpractices in Banks Act 1994 as amended.
iii. Miscellaneous offences Act (cap. 401: LFN).
iv. Any other law or regulations relating to economic and financial crimes including the criminal code and penal code.

Methodology

In this study, the survey design was used for gathering and collecting data to answer the research questions. Data were derived from primary sources with the use of a structured and multiple-choice questionnaire, while secondary sources covered textbooks, articles from various newspapers written by experts, journals, magazines, and the internet. According to the National Bureau of Statistics of Nigeria, the last population census of Nigeria in 2006 provided the population of FCT Abuja to be 776, 298; According to the most recent publication concerning the employees of the EFCC, it is said to be made up of 2,173 individuals, with about 700 of its branches located in the FCT. Therefore, the population for this study includes staff within the commission, including administrative and ICT staff, for effective coverage of the research inquiry. As well as the entireA population of the FCT. This procedure was taken because the issue of cybercrime has a great effect on the general public.

The sample size for this study is 150. A simple random technique is adopted for this study in order to make it possible for all people within the scope of the study to have equal chances of being selected for the study. A simple random technique is also used to obtain a sample size of 150 from the total population of about 776,998. The administrative and ICT staff as well as individuals who reside in the FCT were selected for this study, of which 50 questionnaires were distributed randomly to the administrative and ICT staff of the commission and 100 to the residents of the FCT. The data collected for the purpose of this study is presented and analyzed using simple statistical methods, frequency distribution tables, graphs, and bar charts.

Result of the Findings

Table 1: Socio-demographic Characteristics of Respondents

Gender	**Frequency**	**Percentage**
Male	122	81.4
Female	28	18.6
Others	0	0
TOTAL	**150**	100.0
Age	**Frequency**	**Percentage**
15 – 25	22	14.6
26 – 35	98	65.4
36 – 45	17	11.4
46 – above	13	8.6
TOTAL	**150**	**100**
Religious Affiliation	**Frequency**	**Percentage**
Christianity	85	56.6
Islam	45	30.0
Traditional Religion	15	10.0
Others	5	3.4
TOTAL	**150**	**100**

Field survey, 2023

The findings of the study in Table 1 reveals that 81.4% of the respondents are male, while 18.6% are female. The gender distribution suggests potential gender-specific differences on the impact of the EFCC intelligence operations on cybercrime in the Federal capital territory Abuja. This provided a possibility to examine the impact

The largest group of respondents, 98%, falls within the 26 – 35 age category. This age group represents the prime working-age population, indicating that they may have a higher likelihood of being involved in or affected by the impact of the EFCC intelligence operations on cybercrime in the Federal capital territory Abuja. 56.6% of respondents identified themselves as Christians, 30.0% as Muslims, and 10.0% adhere to Traditional Religion and 5% affirmed as others.

SECTION B: Public Perception of the Impact of Cybercrime on Nigeria's National security

Table 2: Public perception of the Impact of cybercrime on Nigeria's National security

	ITEM		**Response**					
S/N			**SA**	**A**	**DNK**	**D**	**SD**	**Total**
A	Cybercrime poses a serious threat to Nigeria's national security	F	64	63	0	17	6	150
		%	42.6	42.0	0.0	11.3	4.0	100.0
B	Adequate measures are in place to prevent cyber\attacks that could compromise national security	F	24	60	0	77	19	150
		%	16.0	40.0	0.0	51.3	12.6	100.0
c	Cybercrime can contribute to political and social instability by spreading misinformation, manipulating public opinion, and undermining trust in government institutions	F	66	67	0	22	25	150
		%	44.0	44.6	0.0	14.6	16.6	100.0
d	Public awareness campaigns on cybersecurity are effective in educating the population about the risks to national security.	F	50	69	0	35	26	150
		%	33.3	46.0	0.0	23.3	17.3	100.0
e	The public is well-informed about the potential national security risks associated with cybercrime	F	59	64	0	37	30	150
		%	39.3	42.6	0.0	24.6	20.0	100.0
f	The public is well-informed about the potential national security risks associated with cybercrime	F	50	64	0	40	26	150
		%	33.3	42.6	0.0	26.6	17.3	100.0

Table 2 shows the average summary on the respondents' responses regard public perception of the Impact of cybercrime on Nigeria's National security. In Table 2 (a) shows that (70.6%) of the respondents supported the statement that cybercrime poses a serious threat to Nigeria's national security while (29.4%) did not support it. Further confirming the finding, table 2 (b) shows that (30.0%) of the respondents affirmed the statement that adequate measures are in place to prevent cyber\attacks that could compromise national security, while 70.0% said otherwise. Indicating some other impacts, table 2 (c) shows that 72.9% of the respondents confirmed the statement that cybercrime can contribute to political and social instability by spreading misinformation, manipulating public opinion, and undermining trust in government institutions, while (26.1%) did not. Table 2 (d) shows that (66.1%) of the respondents affirmed the statement that public awareness campaigns on cybersecurity are effective in educating the population about the risks to national security, while just 33.9% did not. (e) shows that majority of the respondents 68.4% of the respondents affirmed the statement that the public is well-informed about the potential national security risks associated with cybercrime, while 31.6% of the respondents felt contrary. Lastly, table 2 (f) shows that 63.4% of the respondents supported the statement that the public is well-informed about the potential national security risks associated with cybercrime, while 36.6% did not see it that way.

Table 3: Impacts of Intelligence Operations by the EFCC on curbing Cyber Crime

Does the EFCC's intelligence operations effectively identify potential cyber threats?	Frequency	Percentage
Yes	95	63.3
No	55	36.7
TOTAL	150	100.00
Does intelligence produced by the EFCC contributes significantly to preventing cybercrime?	Frequency	Percentage
Yes	107	71.3
No	43	28.7
TOTAL	150	100.00
Does the information collected through intelligence operations is timely and actionable?	Frequency	Percentage
Yes	77	51.3
No	73	48.7
TOTAL	150	100.00
Has EFCC's intelligence operations improved the efficiency of cybercrime investigations?	Frequency	Percentage
Yes	91	60.6
No	59	39.4
TOTAL	150	100.00
The information obtained through intelligence helps in identifying and apprehending cybercriminals?	Frequency	Percentage
Yes	87	58.0
No	63	42.0
TOTAL	150	100.00
Does the EFCC effectively collaborates with other law enforcement agencies in addressing cybercrime?	Frequency	Percentage
Yes	117	78.0
No	33	22.0
TOTAL	150	100.00

Table 3 shows responses as regards impacts of intelligence operations by the EFCC in curbing cyber-crime. Majority (63.3%) affirmed that EFCC's intelligence operations effectively identify potential cyber threats while the rest stated otherwise. 71.3% of the responded agreed that intelligence produced by the EFCC contributes significantly to preventing cybercrime while the rest stated otherwise. 51.3% of the respondents agreed that information collected through intelligence operations is timely and actionable while 49.7% of them was of the contrary. majority (60.6%) affirmed that EFCC's intelligence operations improves the efficiency of cybercrime investigations while others stated contrary. 58% agreed that the information obtained through intelligence helps in identifying and apprehending cybercriminals, while 42% stated otherwise. Lastly, majority (78%) supported that the EFCC effectively collaborates with other law enforcement agencies in addressing cybercrime, while the rest responded on the contrary.

Table 4: Challenges faced by the EFCC in Combating Cybercrime

There are gaps in the legal and regulatory framework that hinder the EFCC's effectiveness in combating cybercrime	Frequency	Percentage
Yes	95	63.4
No	55	36.6
TOTAL	150	100.00
The legal framework needs updating to keep pace with evolving cyber threats?	Frequency	Percentage
Yes	107	71.3
No	43	28.7
TOTAL	150	100.00
Insufficient technological resources hinder the agency's ability to respond to complex cyber threats?	Frequency	Percentage
Yes	61	40.7
No	89	59.3
TOTAL	150	100.00
Recruitment challenges and staff shortages affect the agency's capacity to combat cybercrime?	Frequency	Percentage
Yes	63	42.0
No	87	58.0
TOTAL	150	100.00
Coordination challenges with other agencies impact the overall effectiveness in combating cyber threats?	Frequency	Percentage
Yes	87	58.0
No	63	42.0
TOTAL	150	100.00
Budgetary constraints limit the agency's ability to invest in necessary cybersecurity resources?	Frequency	Percentage
Yes	47	31.3
No	103	68.7
TOTAL	150	100.00

Table 4 shows challenges faced by the EFCC in combating cybercrime. Majority 63.4 % of the respondents agreed that there are gaps in the legal and regulatory framework that hinder the EFCC's effectiveness in combating cybercrime, while the rest 36.6% disagreed. 71% agreed that legal framework needs updating to keep pace with evolving cyber threats while others did not support it. Majority 59.3% disagreed that insufficient technological resources hinder the agency's ability to respond to complex cyber threat while 40.7% agreed. 58% disagreed that recruitment challenges and staff shortages affect the agency's capacity to combat cybercrime while 42% affirmed it. Majority (58%) agreed that coordination challenges with other agencies impact the overall effectiveness in combating cyber threats while 42% stated otherwise. Lastly, majority (68.7%) of the respondents disagreed that budgetary constraints limit the agency's ability to invest in necessary cybersecurity resources while 31.3% stated contrary.

Discussion of Findings

Based on findings, the first objective of the study found out that (70.6%) of the respondents supported the statement that cybercrime poses a serious threat to Nigeria's national security, while (29.4%) did not. This indicates a significant concern among the public regarding the potential consequences of cybercrime on the nation's security. The global rise in cyber threats and attacks has been well-documented. Reports from organizations such as the World Economic Forum (WEF) and cybersecurity agencies like INTERPOL emphasize the seriousness of cyber threats to national security (WEF Global Risks Report, INTERPOL Cyber Threat Landscape). 30.0% of respondents affirmed that adequate measures are in place to prevent cyberattacks compromising national security, while (70.0%) disagreed. This suggests a prevailing skepticism among the public regarding the effectiveness of current cybersecurity measures. Studies on the efficacy of cybersecurity measures in various countries highlight challenges in keeping up with evolving cyber threats (Global Cybersecurity Index by the International Telecommunication Union). 72.9% of respondents confirmed that cybercrime can contribute to political and social instability, while (26.1%) did not. This underscores the recognition of cybercrime as a potential destabilizing factor, involving misinformation, public opinion manipulation, and erosion of trust in government institution. Success stories of cybersecurity awareness campaigns, such as those conducted by national cybersecurity agencies and initiatives (e.g. European Cyber Security Month), support the idea that education plays a crucial role in mitigating cyber risks. The majority of respondents (68.4%) believed that the public is well-informed about the potential national security risks associated with cybercrime. However, a significant portion (31.6% in (e) and 36.6% in (f)) held the opposite view. This indicates a nuanced perception within the public regarding the level of awareness about cybersecurity risks. Public perception studies on cybersecurity awareness and knowledge can provide additional insights into the factors influencing public understanding and beliefs (Pew Research Center, cybersecurity awareness surveys).

Secondly, in an attempt to understand the impacts of cybercrime to Nigeria’s National Security, the study found out that the majority of respondents (63.3%) affirming that EFCC's intelligence operations effectively identify potential cyber threats suggests a positive perception of the agency's capabilities in threat detection. The high agreement (71.3%) among respondents that intelligence produced by the EFCC significantly contributes to preventing cybercrime aligns with the recognized role of intelligence in proactive cybersecurity measures (Anderson, 2017; Arquilla & Ronfeldt, 2001). The division of opinion on the timeliness and actionability of intelligence operations (51.3% agreed, 49.7% disagreed) highlights a potential area for improvement. Literature on effective intelligence operations stresses the importance of timely and actionable information for successful cyber threat mitigation (Clapper, 2017; Kahn, 2013). The majority (60.6%) affirming that EFCC's intelligence operations improve the efficiency of cybercrime investigations suggests a positive impact on investigative processes. Research on intelligence-driven investigations supports the idea that well-executed intelligence operations enhance efficiency (Ratcliffe, 2016; National Research Council, 2008). The agreement of 58% regarding the information obtained through intelligence helping in identifying and apprehending cybercriminals underscores the role of intelligence in law enforcement efforts. Literature emphasizes the importance of actionable intelligence for successful cybercriminal identification and apprehension (Arquilla & Ronfeldt, 2001; Goodman & Brenner, 2002). The strong majority (78%) supporting the EFCC's effective collaboration with other law enforcement agencies in addressing cybercrime reflects the importance of coordinated efforts. Existing literature highlights the significance of inter-agency collaboration in combating cyber threats (Council of Europe, 2001; Brenner, 2010). These findings collectively suggest a positive perception of the EFCC's intelligence operations in the context of combating cybercrime.

Thirdly the study tried to examine the Impacts of EFCC Intelligence Operations on the fight against cybercrime. In view of this, the significant agreement (71%) that the legal framework needs updating to keep pace with evolving cyber threats resonates with the dynamic nature of cybercrime, requiring continual adjustments to legal instruments (Nwoye, 2018). The disagreement by the majority (59.3%) that insufficient technological resources hinder the agency's ability contradicts common challenges faced by law enforcement agencies globally. Literature often highlights the resource-intensive nature of cybercrime investigations (Goodwin, 2016). The divided opinion on the impact of recruitment challenges and staff shortages (58% disagreed, 4s2% affirmed) reflects a complex issue. Existing literature acknowledges the shortage of skilled personnel as a common challenge in the cybersecurity landscape (Dunn, 2014). The agreement of the majority (58%) that coordination challenges with other agencies impact effectiveness aligns with research emphasizing the need for coordinated efforts among various stakeholders in combating cyber threats (Goodman & Brenner, 2002; Brenner, 2010). The disagreement by the majority (68.7%) that budgetary constraints limit the agency's ability to invest in necessary cybersecurity resources contradicts a common challenge faced by law enforcement agencies globally. Many studies stress the importance of adequate funding for effective cybersecurity initiatives (Goodwin, 2016). By implication, these findings collectively point to a complex landscape of challenges faced by the EFCC in combating cybercrime, encompassing legal, technological, human resource, coordination, and budgetary aspects.

Conclusion

As the general population becomes increasingly refined in their understanding and use of computers and as the technologies associated with computing become more powerful, there is a strong possibility that cyber-crimes will become more common. Nigeria is rated as one of the countries with the highest levels of e-crime activities. Cyber security must be addressed seriously as it is affecting the image of the country in the outside world. A combination of sound technical measures tailored to the origin of Spam (the sending ends) in conjunction with legal deterrents will be a good start in the war against cyber criminals. Information attacks can be launched by anyone, from anywhere. The attackers can operate without detection for years and can remain hidden from any counter measures". This indeed emphasizes the need for the government security agencies to note that there is need to keep up with technological and security advancements. It will always be a losing battle if security professionals are miles behind the cyber criminals. Fighting cybercrime requires a holistic approach to combat this menace in all ramifications. There is need to create a security-aware culture involving the public, the ISPs, cybercafés, government, security agencies and internet users. Also, in terms of strategy, it is crucial to thoroughly address issues relating to enforcement. Mishandling of enforcement can backfire.

Recommendations

In order to redress the problems associated with Cybercrime in the country; this study recommends possible measures for curbing this menace not only in Abuja, F.C.T but all over the nation as a whole;

i. There is need for the nation in liaison with the Economic and Financial Crimes Commission and other anti-graft agencies to develop strategies to curb cybercrime in order to be proactive and reactive. While cybersecurity strategies provide guidance on cybersecurity matters (which can include cybercrime prevention) and map out activities, objectives, action plans and measures in order to curb cybercrime.

ii. The menace of cybercrime has with no doubt damaged the image of the nation internationally. International perception about Nigeria are no doubt negative. Therefore, it is important for the nation to rebrand its image

iii. There should be a concerted and coordinated approach and streamlined partnership between the EFCC and other agencies of government involved in the fight against corruption to avoid overlap and ensure a result-oriented networking so that it does not work at cross-purposes as is currently the case with other similar agencies such as ICPC, Police, NDLEA and the CCB as alluded to in the findings. Thus, there should be vigorous inter-agency synergy, cooperation, coordination and collaboration instead of competition.

iv. There is need for more analytical and technical or technological capabilities in order to curb cybercrime to be able to detect and analyze cyber-attacks. As cybercrime is an act defined involving electronic operations which includes interception of IP addresses, stepping up of tactical activities on cyberspace has become important.

v. It is also recommended that appropriate legislation be put in place to ensure that special courts should be set up with all the appurtenances of law to ensure that justice is speedily and quickly dispensed, and judgments rendered swiftly, thus removing all unnecessary legal technicalities that prolong unnecessary trial of accused persons in corruption cases.

References

Afolabi, M.B. (2015). “Concept of Security” in Kunle Ajayi (ed) *Reading in Intelligence and Security Studies*. Ado-Ekiti: Intelligence and Security Studies, ABUAD

Afolabi, M.B. & Mba, N.A. (2015). “Introduction to Cybersecurity and Cybercrime. *Unending Frontiers in Intelligence.* Ado-Ekiti: Intelligence and Security Studies, ABUAD

Akano, D. (2015:1). Switzerland to return S380m Abacha loot. Daily Independent, March, Wednesday, 18th 2015

Allen Freidman (2016), What Everyone Needs to Know: Cybersecurity & Cyberwar.

Ayotunde, T. (2016). Spiritually in Cybercrime (yahoo yahoo). *Activities among Youths in South West Nigeria.* Google Books.

Economic and Financial Crimes Commission (EFCC)(2004). Information Handbook 1, Jexcel Commercial and Securities Printers; EFCC, Pp 1-5.

Kshetri, N. (2016). The Simple Economics of Cybercrime. IEE Security and Privacy. Retrieved from www.computer.org/security

Jaishankar, K (2015). The Future of Cyber Criminology: Challenges and Opportunities. *International Journal of Cyber Criminology 4, 26-23*

Melvin, A.O. & Ayotunde, T. (2016). Spiritually in Cybercrime (yahoo yahoo). *Activities among Youths in South West Nigeria.* Google Books

Oumarou, M. (2017). Brainstorming Advanced Free Fraud: 'Faymani'- the Camerounian Experience. In N.Ribadu, I. Lamorde and D. W. Tukura (Eds). *Current Trends in*

Rodney P.C. (ed.)(2016). Encyclopedia of Intelligence and Counterintelligence, 2 volumes, M. E. Sharpe, Armonk, New York

Singer, P. & Friedman, A. (2017). Cyber security and Cyber Warfare: What Everyone Need to Know. London: Oxford University Press

Tade, O. & Aliyu, I. (2015). Social Organization of Cybercrime among University Undergraduates in Nigeria. *International Journal of Cyber Criminology 5,* 860-875.

Warner, J. (2016) Understanding Cybercrime in Ghana: A view from Below. *International Journal of Cyber-Criminology* 5(1), 736-749.