INTERNATIONAL CRIMINAL POLICE ORGANISATION STRATEGIES AND THE NATIONAL EFFORT IN THE FIGHT AGAINST CYBERCRIME IN NIGERIA

DR. AUDU MOMOH AMINU
PROF. YAHAYA ABDULLAHI ADADU
PROF. MUHAMMED BELLO BABAN'UMMA
ASSOCIATE PROF. LUKA RUTH CALEB
DR. MICHAEL MASHAL JEMLAK
DEPARTMENT OF POLITICAL SCIENCE, FACULTY OF SOCIAL SCIENCES, NASARAWA STATE UNIVERSITY, KEFFI. NASARAWA STATE, NIGERIA.
Corresponding Email: audu.aminu5@gmail.com

KEYWORDS
Interpol, Cybercrime, Strategies, National Effort, Space Transition

ABSTRACT
Cybercrime has remained a serious challenge in Nigeria. Various efforts of government to fight the menace have failed to yield the desired result. Most academic writings in Nigeria place much emphasis on the causes and effects of cybercrime, while very little has been done on the Strategies to combat it. On this note, this study examines Interpol Strategies and the national efforts in the fight against Cybercrime in Nigeria. The study is mixed in nature which deals with review of previous literatures and documents. Questionnaires were administered on three hundred and seventy-five (375) respondents drawn from the International criminal Police Organisation (ICPO-Interpol) National Central Bureau (NCB) Abuja, Nigeria Police Force (NPF), Economic and Financial Crime Commission (EFCC) and the Department of State Services (DSS). Interview was conducted on fifteen (15) selected Participants. The study adopted the Space transition theory propounded by Jaishankar (2008) on the assumption that identity flexibility, dissociative anonymity and poor deterrence in Cyberspace motivate Cybercrime. The study found that some of the Interpol Strategies have positive complement on the national efforts in the fight against cybercrime in Nigeria. It therefore recommends increased investment on training and capacity building of Law enforcement agencies and Cyber security stakeholders in Nigeria as well as synergy and increased utilization of Interpol platforms/tools for winning the war against Cybercrime in Nigeria.

1.1 Introduction

The global advancement in Information Communication Technology (ICT) has brought significant relief to human activities due to the ease of interaction, exchange of products and services it presents. As good as the benefit seems, it has transformed the hitherto conventional crime landscape to a more coordinated and more sophisticated. The pattern of crime has now graduated from the purely conventional and physical to a more coordinated and virtual type where criminals may not necessarily know themselves nor meet in physical space but cooperate to carry out criminal activities through the cyberspace. Jaishanker (2008) examines the Space transition as an explanation about the nature of the behavior of persons who bring out their conforming and non-conforming behavior from physical space to cyberspace and vice versa. These indiscriminate migrations simplify activities of cybercriminals, which has attracted significant loss in terms of money, time, trust and reputation. According to Morgan & Calif (2020) the global loss to Cybercrime amounts to 3 Trillion US Dollars in 2015, 6 trillion US Dollars in 2021 and is projected to rise to 10.5 trillion US Dollars in 2025. Nigeria lost ₦127Billion annually to cyber attacks (Awhefeada & Bernice, 2021). This is in addition to the indiscriminate disruption of services, unwarranted hardship and panic, loss of trust, respect and reputations in events of cyber attacks. The outbreak of covid-19 pandemic helps to further accelerate the frequencies of cyber attacks and increase the vulnerabilities of internet users in Nigeria. A report by Kaspersky Protection Technologies indicates that over 9,000 people in Nigeria suffered malware attacks launched by cybercriminals in 2019 alone (Umeh, 2020). Between 2011 and 2020, fifteen billion records have been exposed or breached through the activities of Cybercriminals as opposed to 103 million records in the previous decade (Neethu, 2020). That is over 1400% increase in record exposure or breaches within a decade which is extremely high.

Interpol has been identified as a leading global organization that is charged with the prevention and fight against cybercrime across the globe. Akimbayo (2001), Timothy & Afia (2013), Neethu (2020) all attested to the great potentials of the Interpol in tackling trans-border crimes. In spite of the outstanding credentials presented for the Interpol, the fight against cybercrime in Nigeria remains a mirage as cases of Cybercrime continues to rise. Whereas the national law enforcement agencies and government fighting the menace seems to have been overwhelmed. Perpetrators of this crime seem to have found a safe haven and are taking advantage of the anonymity and boundless borders of the cyberspace and poor awareness of potential victims to perpetrate their nefarious activities.

Akuta, Ong'oa & Jones (2011) ranked Nigeria among the top-ten countries of high prevalence of cybercrime in the world and first in Sub-Sahara Africa ahead of Cameroon, Ghana and South Africa. Frank & Odunayo (2013) made an overview of the menace of Cybercrime in what they described as the Evolution of 'the new type of war' which they referred as the internet Cybercrime and predicted a destruction of greater magnitude than the first and second world war, if serious measures are not taken to nip it in the bud. In Nigeria there was a revolution in the telecom industry in the early 2000 without commensurate cyber security measures which has exposed internet users to unintended consequences. The implication of this development has been well articulated by Osho & Onoja (2015) when he argued that Conventional crimes can easier be curbed through physical measures involving detection, investigation, apprehension and prosecution, adopting traditional methods requiring the use of physical techniques. However, when these crimes become digitalized, severe complications arise, making the solutions cumbersome or in some cases, infeasible to find. Digitalization of crimes have presented law enforcement agencies with mutations in conventional crime, resulting from the technicalities involved, advancements in crime commission methods, increased anonymity, reduced possibility of successful criminal profiling amongst others. Hence, traditional methods of solving crimes have become unhelpful with the computerization of these crimes (Osho & Onoja, 2015). While cybercriminals exploit borderless playing fields in the digital world, law enforcement structures are limited to their national borders.

Interpol as an international body came into being in 1923 to facilitate police cooperation against emerging threats of transnational criminal activities. Its mandate includes providing investigative support, expertise and training to law enforcement operatives globally,

while focusing on three major areas of transnational crime: terrorism, cybercrime, and other organized crime (Buzan & Hansen, 2009). Interpol's mandate actually covers nearly all kinds of crime which include: crimes against humanity, child pornography, drug trafficking and production, political corruption, copyright infringement, and white-collar crime. It also facilitates cooperation among national law enforcement agencies via its Criminal databases and i247 communication network. For the purpose of this study Interpol mandate shall be limited to the fight against Cybercrime.

1.2 Statement of the Problem

The major challenge facing the international community in this era of globalization has been how to curb the menace of cybercrime. Some of the advancement recorded in information communication technology in the 21st century has almost erased the usual barriers placed by distance and time. People over the world are now more closely linked than ever. This has led to increase interaction among people which has equally attracted some negative implications. Cybercrime is one of the negative implications presented by this global ease of interactions. Criminal individuals, groups and organizations are taking advantage of the borderless Cyberspace to perpetrate their nefarious activities

According to Awhefeada & Bernice (2021) Nigeria state lost NGN127 billion to cyber attacks annually. This is in addition to disruption of services, lost of trust, reputation and respect among others in event of cyber attacks. While cybercriminals exploit the borderless cyberspace in the digital world and transit from one space to another with ease, law enforcement structures are been limited to their national borders base on legal and territorial barriers. Perpetrators of Cybercrime seem to have found a safe haven and are taking advantage of the anonymity and boundless borders of the cyberspace and poor awareness of potential victims to perpetrate their nefarious activities. Chioma Et'al. (2017), Adesina (2017), Olayemi (2018), Abiodun & Obioro (2020), Viko (2021) have all alluded to the increasing cases of cybercrime in Nigeria which has become worrisome. Most of the scholarly efforts have succeeded in identifying the causes and effects of cybercrime, whereas very little has been made to examine the strategies adopted or to be adopted in the fight against cybercrime in Nigeria. Whereas, the benefits of Interpol's wide membership, extraterritorial cooperation, jurisdiction and strategies may not have been felt as Cybercrime continues on the rise, hence the need to examine Interpol strategies vis-a-vis the national efforts in the fight against Cybercrime in Nigeria, with the aim of finding their points of convergence or otherwise, toward a more effective fight against Cybercrime in Nigeria.

1.3 Research Questions

i. What are the strategies adopted by Interpol in the fight against Cybercrime in Nigeria?

ii. How has the Strategies adopted by Interpol Complements the National efforts in the fight against Cybercrime in Nigeria?

1.4 Objectives of the Study

i. To ascertain the strategies adopted by Interpol in the fight against Cybercrime in Nigeria.

ii. To examine how the Strategies adopted by Interpol Complements the National efforts in the fight against Cybercrime in Nigeria.

1.5 Conceptual Clarification

1.5.1 International Criminal Police Organization (ICPO-Interpol)

The International Criminal Police Organization (ICPO-INTERPOL); more commonly known as INTERPOL, is an international organization that facilitates worldwide police cooperation and crime control. Founded in Vienna, Austria in 1923, it's Headquarters is located at Lyon, France with seven (7) regional Bureaus globally and a National Central Bureau in all 195 member states, making it the world largest police organization (Aminu, 2024a). Interpol's mandate actually covers nearly all kinds of crime which include: crimes against humanity, child pornography, drug trafficking and production, political corruption, copyright infringement, and Cybercrime. The agency also facilitates cooperation among national law enforcement agencies via criminal databases and communications networks. Contrary to

popular belief, Interpol is not a law enforcement agency. Moreover, Interpol runs an annual budget ranging around €113 million (US$131 million), most of which is realized from annual contributions by police forces in the existing 195 member states worldwide. It is also governed by a General Assembly that is composed of all member countries, which elects the Executive Committee and the President. However, Interpol vies to remain politically neutral in as its charter regulates it from carrying out any interventions or activities of a political, military, religious, or racial nature or involving itself in disputes over such matters (Interpol, 2023).

Interpol is not immune from some of the challenges facing law enforcement agencies across the globe. It has however remained the biggest umbrella that covers the police and other law enforcement agencies, ever in the history of mankind and it has assisted to promote the requisite technical innovations and cooperation amongst police and law enforcement agencies in the fight against trans-border crime, especially Cybercrime.

1.5.2 Cybercrime

One of the major challenges in the study of cybercrime is the absence of a perfect single definition, even among the law enforcement agencies charged with tackling it (Adesina, 2017). The complex nature of the term Cybercrime has made it very difficult to give it a precise definition. It is often complicated in getting a unique and consistent definition of Cybercrime. This is because of the diverse perspectives and orientation of the authors, which has resulted in multiplicity of terms and vocabularies such as computer crime, computer-related crime, digital crime, information technology crime, internet crime and virtual crime. The term cybercrime referred to crimes over networks, especially the internet but the term has increasingly become a general term or replacement for computer crime. Kamal, Chowdhury, Haque, Chowdhury and Islam (2017) articulated that Crimes which are committed in the cyber world are so complex in nature and its coverage is very wide and massive.

Cybercrime is a split word which can be better understood by understanding the split meaning of cyber and crime. Ordinarily, a crime remains an unlawful act that is punishable by a state or existing authority. Cybercrime are Crimes committed using the computer as either a tool or a targeted victim. It encompasses all illegal activities perpetrated by one or more people referred to as scammers, hackers, internet fraudsters, cyber citizens or 419ners, using the internet through the medium of networked computers, telephones and other information and communications technology (ICT) equipments (Halder & Jaishankar, 2019).

The rising cases of Cybercrime in Nigeria have been attributed to different factors. Christopher, (2014) gave an insight on most likely causes of cybercrime by arguing that cybercrime is more associated with young people in Nigeria who constitute a larger percentage of people seen perpetrating the act of internet fraud and cyber pornography etc. He identified Unemployment, Urbanization, Weak Implementation of Cyber Crime Laws and Ill-equipped law enforcement agencies, Quest for quick wealth and Negative role models as some of the causes of cybercrime in Nigeria.

In a bid to further understand cybercrime as different from other crime. McAfee Inc., (2014) gave an insight on some of the distinguishing features that defines cybercrime, which includes;

i. Digital technology: Cybercrimes inevitably involve some form of digital technology, ranging from a Smartphone or a desktop computer to encrypted data or secure networks.

ii. Borderless and global: Cybercrimes are not limited by any borders; they are transnational. An attacker may target an unknowing victim next-door, or in another continent.

iii. Lack of physical evidence: Unlike traditional crimes, cybercrimes do not involve the usual crime scene. The crime may even go undetected for a significant period.

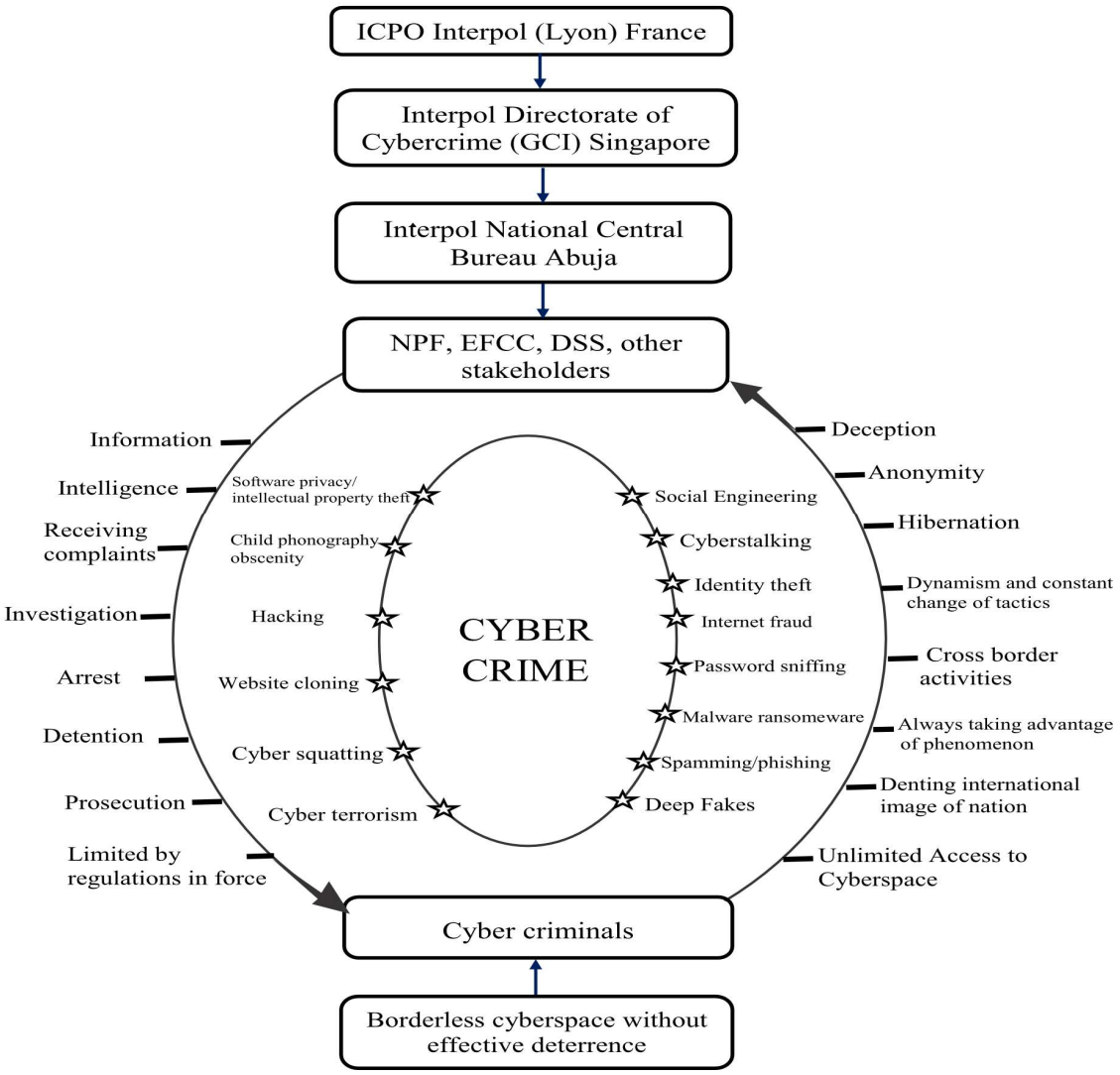
iv. Lesser effort and time: In general, cybercrimes can be committed at greater ease and at a faster pace than traditional crime, making it further challenging to curb its rise.

v. Vast negative impact: A one-time cybercrime can result in severe long-term damage to an extension section of the society, or even entire countries.

Therefore, based on the sophisticated nature of cybercrime, how easy and fast it could be committed, the difficulty in getting evidence and the negative consequences it attracts there is need to take urgent possible steps to checking the rising trend in Nigeria.

Fig1:1 Nigeria Cybercrime Circle

Fig.1;1: Cybercrime Cycle



Source: Author's Compilation July, 2023

From the details in fig. 1.1 above, it becomes clearer that the Nigeria cyberspace is characterized by different kinds of cybercrime which includes Hacking, website cloning, cyber stalking, identity theft, internet fraud among others; Nigeria Cyberspace is a borderless terrain that's lacks effective deterrence thereby giving chances for cybercrimes to grow. Cybercriminals has unlimited access to the cyberspace, they engage in cross border activities, always taking advantage of natural phenomenon such as covid-19 pandemic. Whereas its headquarters is in France, Interpol has a special Directorate of Cybercrime otherwise known as the global complex for Innovation located in Singapore, which maintains close contact with all Interpol National Central Bureau including NCB Abuja, which in turn relates with other law enforcement agencies like the Nigeria Police Force (NPF)

Economic and Financial Crimes Commission (EFCC) The Department of State services (DSS) and other cyber security stakeholders in Nigeria for the purpose of the fight against Cybercrime. However, law enforcement agencies in Nigeria are making efforts through information and intelligence sharing, complaints received and arrests among others to deal with the menace, but with efforts limited by law and other factors, contrary to the unlimited access that cybercriminals enjoy.

1.5.3 Interpol Strategies and National efforts against Cybercrime in Nigeria

Cybercriminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of crimes that know no borders, either physical or virtual. These activities cause serious harm and pose very real threats to victims worldwide. In the past, cybercrime was committed mainly by individuals or small groups. Today, Interpol is seeing highly complex cybercriminal networks bringing together individuals from across the globe in real time to commit crimes on an unprecedented scale. The strategies adopted by the Interpol in dealing with the menace of cybercrime are not different from those used to fight other trans-border crimes.

Interpol, (2022) in its document titled 'Organized and emerging crime strategy' outlines plan to support its 195 member countries in tackling serious transnational crime in line with Interpol strategic framework to support member countries in reducing the impact of serious organized and emerging crime, thereby protecting societies and vulnerable communities for a safer world. The objectives are as follows; to reduce the impact of serious organized and emerging crime through enhanced law enforcement information exchange; To enrich actionable intelligence products by crosschecking information and analyzing data sets on serious organized and emerging threats; To support countries investigations and develop their abilities to prevent and respond to serious organized and emerging crime through operational support and capacity building; To optimize Interpol support to the global law enforcement community to tackle transnational, serious, organized and emerging crime through forging and fostering synergies, sharing resources and knowledge and strengthening partnership.

The above objectives combine to serve as benchmark for Interpol Strategies in dealing with Cybercrime which are; Training and Capacity Building, Intelligence Sharing, Joint Operations, Technology and Infrastructural Support and Use of Interpol Platforms/tools. These strategies were interrogated in line with the national efforts against cybercrime in Nigeria which shows some positive points of impact in the areas of Intelligence Sharing, Cyber Security Awareness/Education, Political Neutrality, Synergy and Utilization of Interpol Platforms/tools as well as funding for LEA

FGN (2021) in its document titled Nigeria National Cyber Security Policy and Strategy argued that National Cyber Security Strategy (NCSS) is the nation's readiness strategy to provide cohesive measures and strategic actions towards assuring security and protection of the country's presence in cyberspace, safeguarding critical information infrastructure, building and nurturing trusted cyber-community. It established that Nigeria has a robust national cyber security policy from where the national cyber security strategies were drawn. It identified Nigeria Cybercrime Working Group (NCWG) and the Computer Emergency Response Team (CERT) domiciled in the office of the National Security Adviser (NSA) as the major arms of the office in terms of coordination, operations and leadership in the fight against cybercrime in Nigeria.

Whether the office of the NSA have been able to provide the needed leadership to the security intelligence and law enforcement agencies in Nigeria remains a matter of debate. However, available data indicates serious inter-agency rivalry and clashes amongst the security, intelligence and law enforcement agencies in Nigeria. That is to say a lot still need to be done on Nigeria security management, bearing in mind the current threats of Cybercrime in Nigeria.

1.5.3 Summary of Literature Gap

Akimbayo (2001), Timothy & Afia (2013), Neethu (2020) were all united on the potentials of the Interpol in tackling trans-border crimes. In spite of the outstanding credentials presented for the Interpol in the fight against cybercrime in Nigeria, cases of Cybercrime continue to rise. Chioma E'tal. (2017), Adesina (2017), Olayemi (2018), Abiodun & Obioro (2020), Viko (2021) have all specifically averred to the increasing cases of cybercrime in Nigeria which has become worrisome. Most of the scholarly efforts have

succeeded in identifying the causes and effects of cybercrime, whereas very little has been done to examine strategies such as the Interpol strategies and the National effort in the fight against Cybercrime in Nigeria with a view to sharpen it for optimum results, which forms the thrust of this study.

1.6 Theoretical framework - Space Transition Theory

In an attempt to highlight the dichotomy between physical and cybercrime Yar, (2005) earlier argued that a gulf separates the virtual and the terrestrial types of crime. In a chapter publication titled 'Crimes of the Internet', Jaishankar, (2008) develops the "Space Transition Theory" as an explanation about the nature of the behavior of persons who bring about their conforming and non-conforming behavior in the physical space and cyberspace. Space transition involves the movement of persons from one space to another (e.g., from physical space to cyberspace and vice versa). Space transition theory argues that, people behave differently when they move from one space to another. The Space Transition theory is hinged on seven major assumptions amongst which are;

i. Persons, with repressed criminal behavior (in physical space) have a propensity to commit crime in cyberspace, which they would not otherwise commit in physical space due to their status and position.

ii. Identity Flexibility, dissociative anonymity and the lack of deterrence factors in cyberspace provides the offenders with the choice to commit cybercrime, etc.

The 'physical space' constitutes a 'moral community' governed by the regulated conduct of people by formal and informal mechanisms. This, in itself, serves to check the bogus manifestation of a deviant or criminal act. However, a repressed youth within the physical space may elect to migrate to the 'virtual space' for uninhibited and unregulated conduct or behavior, which allows dissociative anonymity. The space transition theory provides a better explanation of criminal behavior in the cyberspace and it's relevant to this study because it explains better the simplicity of the internet space and the challenges of anonymity and poor deterrence in the cyberspace which offered the offenders the choice of commit crime. It therefore suffices that space transition related strategies will be effective in the fight against cybercrime in Nigeria.

1.7 Research Methodology

This study adopted a descriptive research design, which involves Data collection, presentation and analysis on the topic, Interpol Strategies and the National efforts in the fight against Cybercrime in Nigeria. It relies on existing literatures and documents. Questionnaires were administered and In-depth Interviews were conducted to gather insights from officials of the Interpol NCB Abuja, personnel of the Cybercrime units of the Nigeria Police Force (NPF), Economic and financial crime commission (EFCC) and the Department of State Services (DSS) and other relevant Stakeholders. The choice of the selected law enforcement agencies is informed by their records of cybercrime investigation and prosecution in Nigeria. The study population is 15280 been the summation of number of personnel attached to their cybercrime units. Sample size of 400 was ascertained through the use of Krejcie and Morgan (1970) Sample size table.

Out of four hundred (400) questionnaires distributed, only three hundred and seventy-five (375) copies representing 93.5% were returned whereas 25 representing 6.5% were not returned.

Table: 1.1 Study Populations and Sample of Interpol NCB Abuja and Selected Law Enforcement Agencies in Nigeria.

Interpol NCB Abuja and selected Law enforcement Agencies in Nigeria.	Population of Personnel Attached to Cybercrime Department/Units	Sample of Personnel attached to Cybercrime Department/Units	Percentage of Population and Sample size
Interpol NCB Abuja	1601	39	10.47%
NPF	8498	209	55.61%
EFCC	3196	78	20.91%
DSS	1985	49	12.99%
Grand Total	15280	375	99.98 ≈ 100%

Source: Field Survey July, 2023

In addition to administration of questionnaires, this study equally adopted interview as tool. Though the participating organisation for the interview session is similar to that of questionnaire, it however expounded to capture other relevant segments of the research such as the office of the National Security Adviser (ONSA), because of its roles as the National Coordinating body of cybercrime and cyber security in Nigeria, as well as Suspects and Victims of Cybercrime. Purposive sampling techniques were used to select fifteen (15) interviewee's bases on their expertise and experience on the subject under investigation. The study employs descriptive statistics and Triangulation as method of data presentation and analysis.

1.8 Data Presentation and Analysis

Table: 1.2 Respondents views on the Strategies adopted by Interpol in the fight against Cybercrime in Nigeria?

The following are the major Strategies adopted by Interpol in the fight against Cybercrime in Nigeria.	SA Freq. (%)	A Freq. (%)	UD Freq. (%)	D Freq. (%)	SD Freq. (%)	Total ∑Freq (%)
Training and Capacity Building	189 (50.4%)	107 (28.5%)	14 (3.7%)	61 (16.3%)	4 (1.1%)	375 (100%)

Intelligence Sharing	288	65	6	4	12	375
	(78.8%)	(17.3%)	(1.6%)	(1.1%)	(3.2%)	(100%)
Joint Operations	312	42	4	11	6	375
	(83.2%)	(11.2%)	(1.1%)	(2.9%)	(1.6%)	(100%)
Technology and Infrastructural Support	317	31	19	7	1	375
	(84.5%)	(8.3%)	(5.1%)	(1.9%)	(0.3%)	(100%)
Use of Interpol Platforms/tools.	212	81	54	21	7	375
	(56.5%)	(21.6%)	(14.4%)	(5.6%)	(1.9%)	(100%)

Source: Field Survey July, 2023

From table 1.2 above, it could be deduced that intelligence sharing is one of the most significant strategies of Interpol in the fight against cybercrime in Nigeria as overwhelming majority of the 353 representing 96.1% of the respondents agreed while 16 representing 4.3% of the respondents disagree. Meanwhile 6 representing 1.6% of the respondents were Undecided. Joint Operation is considered another strong Strategy of the Interpol in its fight against cybercrime in Nigeria as 354 (94.4%) of the respondents Agreed while 17 representing 4.5% of the respondents Disagreed. However, 4 respondents representing 1.1% were Undecided. Another favourable strategy adopted by Interpol in the fight against cybercrime in Nigeria is Technology and Infrastructural Support on which 348 respondents representing 92.8% agreed while only 8 representing 2.2% of the respondents disagreed. However, 19 of the respondents representing 5.1% were Undecided.

Training and Capacity Building is the next most significant strategy adopted by the Interpol In the fight against cybercrime as 296 respondents representing 78.9% either agreed, while 65 representing 17.4% of the respondents disagreed. Meanwhile 14 representing 3.7% of the respondents were undecided. However, Use of Interpol Platforms and tools like i24/7, Notices, activities of the Bureau of Deportation and Extradition received the least, 293 respondents representing 78.1% either agreed, while 28 respondents representing 7.5% disagreed. However, 54 respondents representing 14.4% were undecided.

The implication of the above findings is that intelligence sharing, joint operation and Technology and Infrastructural Support are the most remarkable strategy adopted by the Interpol in the fight against cybercrime in Nigeria. This is corroborated by IP3 who asserted that;

> *The Nigerian Police Force usually exchanges confidential details and information regarding cybercrime with relevant international agencies such as Interpol, FBI. (IP3 July, 2023)*

IP2 noted that;

> *Interpol has been engaging in a lot of sensitization and public awareness such as short messages, videos, digital animation etc to educate members of the public and potential victims of cybercrime on preventive measures (IP2 July, 2023)*

It can be gleaned from the submissions of the respondents that Interpol is adopting different strategies to tackle cybercrime. Specifically, the strategies being used by the Interpol includes intelligence sharing, joint operations, public enlightenment about the antics of cyber

fraudsters, prosecuting cybercrime suspects, conducting surveillance in parts of Nigeria that are notorious for the activities of cybercriminals, using tracking and intercepting devices, and collaborating with relevant international law enforcement agencies in Nigeria.

This is in agreement with the view of IP5

> *On a serious note, Cybercrime is an international crime that cuts across borders and the Interpol over the years has been assisting the Police in terms of intelligence sharing, Crime awareness, Modus operandi and joint operations and the results has been very impressive. (IP5 July, 2023)*

Other Participants asserted;

> *Through actionable intelligence and swift response of the Interpol in collaboration with relevant or competent authorities, several Cybercriminals syndicate has been busted, investigated and perpetrators brought to face the wrath of the law. (IP8 July, 2023)*

> *Through intelligence shared from Interpol Platforms some of these money and assets traced to cybercriminals are usually seized and returned back to the victims or deposited with the Central Bank of Nigeria before victims are traced (IP7 July, 2023).*

The implication of the above assertions is that Interpol has done more in the fight against Cybercrime in Nigeria through, intelligence sharing, joint operations and Technology and Infrastructural Supports.

Table: 1.3 Respondents views on the ways Interpol Strategies has complements national efforts in the fight against Cybercrime in Nigeria.

The following are the ways Interpol Strategies has Complement National efforts in the fight against Cybercrime in Nigeria.	**SA** **Freq. (%)**	**A** **Freq. (%)**	**UD** **Freq. (%)**	**D** **Freq. (%)**	**SD** **Freq. (%)**	**Total** **∑Freq** (%)
Intelligence Sharing	336 (89.6%)	21 (5.6%)	10 (2.6%)	7 (1.9%)	1 (0.3%)	375 (100%)
Awareness/Education on Cyber Security	307 (81.8%)	43 (11.5%)	13 (3.5%)	9 (2.4%)	3 (0.8%)	375 (100%)
Political Neutrality	308 (82.1%)	30 (8.0%)	16 (4.3%)	17 (4.5%)	4 (1.1%)	375 (100%)
Synergy and Utilization of Interpol Platforms/tools	194 (51.7%)	110 (29.3%)	9 (2.4%)	61 (16.3%)	1 (0.3%)	375 (100%)

Funding for LEA	247 (65.9%)	67 (17.9%)	43 (11.5%)	8 (2.1%)	10 (2.6%)	375 (100%)

Source: Field Survey July, 2023

From table 1.3 above, Intelligence sharing has been identified as the most effective area Interpol strategies has complements national efforts in the fight against Cybercrime in Nigeria as overwhelming number of respondents, 357 representing 95.2% agreed while only 8 representing 2.2% of the respondents disagreed, meanwhile 10 of the respondents representing 2.6% were undecided. Cyber Security Awareness/Education is another important area Interpol has complemented the national efforts in fight against Cybercrime in Nigeria as significant number of respondents 350 representing 93.3% agreed while twelve (12) of the respondents representing 3.2% disagree, whereas Thirteen (13) representing 3.5% of the respondents were undecided. 338 respondents representing 90.1% agreed on Political Neutrality, while 21 representing 5.6% of the total respondents disagreed, whereas 16 representing 4.3% were undecided. Funding for Law Enforcement Agencies is another area the Interpol has complements national efforts in the fight against Cybercrime in Nigeria. 314 respondents which constitute 83.8% agreed while 18 representing 4.7% of the respondents disagreed meanwhile 43 representing 11.5% were undecided. Synergy and Utilization of Interpol Platforms and tools is another area Interpol complements national efforts in the fight against cybercrime in Nigeria that has receives least entry, as only 304 respondents representing 81% agreed while 62 representing 16.6% of the respondents disagreed with this assertion, meanwhile 9 representing 2.4% of the respondents were undecided.

The implication of the above is that while Interpol has complemented the national efforts in Fighting Cybercrime in Nigeria in the area of Intelligence Sharing, Cyber Security Awareness/Education and Political Neutrality which has received significant endorsement of 95.2%, 93.3% and 90.1% respectively. Meanwhile, Funding of LEA, Synergy and use of Interpol Platforms/tools remains behind with just 83% and 81%.

A key Participant had mentioned this:

> *Cyber threat actors continue to cause a lot of damage in Nigeria and outside; I believe a lot need to be done by Nigeria law enforcement agencies and stakeholders to fight the scourge of cybercrime in Nigeria through effective synergy of stakeholders and international collaboration a lot can be achieved. (IP9 July, 2023)*

Another participant asserted:

> *The fight against Cybercrime in Nigeria cannot be fully achieved without extending the Interpol i24/7 tools to other relevant law enforcement agencies, such as the Nigeria Customs Service (NCS), Independent Corrupt practices and other related offences commission (ICPC) National Agency for the Prohibition of Traffic in Persons (NAPTIP), Nigeria Correctional Services (NCS) same way it was extended to the Navy, EFCC, NDLEA and Immigration Service. Interpol is currently working on the MOU with these agencies for the extension of tools and services to their door steps (IP1 July, 2023)*

It can be understood from the above submissions of the two respondents that synergy among relevant law enforcement agencies in Nigeria as well as extension of the Interpol tools and services to other law enforcement agencies in Nigeria are very key in winning the war against cybercrime in Nigeria. This is in agreement with the position of Al-Raisi (2023) who argued that at the center of tackling Africa's Crime threats is the need for greater information sharing, the lifeblood of international police cooperation. He argued further that Africa member countries use of Interpol Databases has traditionally lagged behind that of other world regions. It is important to acknowledge that Interpol strategies has complement national efforts through the Nigeria Police Force National Cybercrime Center NPF-NCCC, as noted by IP6 follows;

Yes, through credible intelligence and training offered by Interpol there was a major breakthrough which led to the arrest of PPE supply scammers in Nigeria at the heat of covid-19 Pandemic. Secondly through Interpol the center recently trained 15 certified ethical hackers and 15 forensic analysts. I know a lot more of this training is needed but it will certainly complement the national efforts in the fight against cybercrime in Nigeria. (IP6 July, 2023)

The major indications of the findings above is that Intelligence Sharing, Cyber Security Awareness/Education as well as political neutrality are the most remarkable areas the Interpol has complement national efforts in the fight against cybercrime in Nigeria.

1.9 Summary of Findings

Findings on the strategies adopted by Interpol in the fight against cybercrime in Nigeria reveals that, Intelligence sharing, joint Operations, Technology and Infrastructural Support, recorded the highest positive entry of 96.1%, 94.4% and 92.8% respectively, while Training and Capacity Building, Use of Interpol Platforms and tools recorded the least positive entry of 78.9% and 78.1% each.

On how Interpol Strategies Complements National efforts in the fight against cybercrime in Nigeria, Intelligence Sharing, Cyber Security Awareness/Education and Political Neutrality recorded the highest positive entry of 95.2%, 93.3% 90.1% respectively, while Synergy and Utilization of the Interpol platforms/tools, Funding of Law enforcement agencies recorded the least positive entry of 83.8% and 81.0% each.

1.10 Conclusion

The study established that;

i. Intelligence sharing, joint operations, Technology and Infrastructural Supports constitute the most significant strategies adopted by Interpol in the fight against Cybercrime in Nigeria.

ii. Intelligence Sharing, Increase Cyber Security Awareness/Education and Political Neutrality are the major areas the Interpol Strategies complements the National efforts in the fight against Cybercrime in Nigeria.

1.11 Recommendation

To better complement the national effort in the Fight against Cybercrime in Nigeria, this study recommends the following;

i. Interpol through its National Central Bureau Abuja should increase focus and investment on training and capacity building of Law enforcement agencies and Cyber security stakeholders in Nigeria to enable it deal more effectively with the rising cases of Cybercrime. This could be achieved through increased funding and strategic budgeting in favour of training and capacity building of Law enforcement agencies and Cyber security stakeholders in Nigeria.

ii. That all law enforcement agencies and stakeholders involved in the fight against Cybercrime in Nigeria should strengthen synergy in order to maximize the Cyber security opportunities, platforms/tools offered by the Interpol for a more effective fight against Cybercrime in Nigeria. This could be achieved through inter-agency training of recruits and existing personnel of law enforcement agencies in Nigeria where they can be exposed to the rudiments of synergy and the fight against Cybercrime in Nigeria.

References

Abiodun, F. & Abioro, D. (2020). Roles and challenges of international criminal police organization (Interpol) in investigation of crimes and maintenance of global security. *Research Journal of Management and Social Sciences,* 10(3), 7-26.

Adesina, O. S. (2017). Cybercrime and poverty in Nigeria. *Canadian Social Science Journal*, 13(4), 19-29

Akimbayo, O. O. (2001). The place of Interpol in the control of transnational organised crime. A course essay as requirement for the award of cadet ASP rank, *Academic board of Police staff College, Jos-Nigeria*. 2001

Akuta, E. A, Ong'oa I. M & Jones C. R (2011). Combating cybercrime in sub-sahara Africa: A discourse on law, policy and practice. *Journal of peace, Gender and Development Studies* Vol. 1(4), 129-137. http://www.interesjournals.org/JPGDS

Al-Raisi, A. N. cited in Aminu, M. A. (2024). International criminal police organisation and the challenges in the fight against Cybercrime in Nigeria. *Kashere Journal of Politics and International relations* Vol. 2(1), 48-56.

Awhefeada, V. & Bernice, O (2020). Appraising the Laws Governing the Control of Cybercrime in Nigeria. *Journal of Law and Criminal Justice 8 (1) 30-49*

Buzan, B.& Hansen, L. (2009). The Evolution of International Security Studies. *Cambridge University Press.*

Chioma, C. Samuel, U. Daniel, M. & Macarthy, O. (2017). Proliferation of cyber insecurity in Nigeria: A root cause analysis

Ebenezer, A. E. (2015) Mitigation of cybercrime in Nigeria through adoption of national strategies on cybercrime security skill and manpower development. *Inte rcontinental journal of education, science and technology* 3(1) 65-79

Federal Government of Nigeria (2015) Cybercrime Prohibition and Prevention act. *Retrieved from http://cert.gov.ng /images/uploads/cybercrime_act_2015.p df*

Federal Government of Nigeria (2021) Nigeria National Cyber Security Policy and Strategy. *from http://cert.gov.ng / Nigeria National Cyber Security Policy and Strategy _2021.pdf*

Frank I. & Odunayo E, (2013) Approach to Cyber Security Issues In Nigeria: Challenges and Solution. (IJCRSEE) *International Journal of Cognitive Research in Science, engineering and Education Vol. 1 No. 1 2013*. www.ijcree.com

Halder, D. & Jaishankar, K. (2019). Cyber socializing and victimization of women. Temida: *The Journal of victimisation, human rights and gender,* 12 (3), 5-26.

Interpol (2022) Cybercrime: Categorization of the new type of crime. Retrieved from www.interpol.inc 24/5/2023

Interpol, (2023) Constitution of the International Criminal Police Organization, ICPO-Interpol I/CONS/GA/1956.

Jaishankar, K. (2008). Space Transition Theory of cybercrimes. In Schmallager, F., &Pittaro, M. (Eds.), Crimes of the Internet. *(pp.283-301) Upper Saddle River, NJ: Prentice Hall. © 2007 International Journal of Cyber Criminology.*

Krejcie, R. V., & Morgan, D.V. (1970). *Determining the sample size for research activities*. Educational and Psychological Measurements, 3 (2), 607-610

McAfee Inc. (2014) Net Losses: Estimating the Global cost of Cybercrime. *Retrieved from htts://www.mcafee.com/ca/resources/re ports/rp-economics-impact- cybercrime2.pdf*

Morgan S. & Calif S. (2020) Special Report: Cyber Warfare in the C-suite. Cybercrime Facts and Statistics. *Published by Cyber*

security Venture and Intrusion Jan. 2021 Ed. pp.1-5

Neethu N., (2020). Role of International Orgainsation in Prevention of cybercrime: An Analysis Nalsar *University of law Hyderadad. MSTL33-20*

Okonji E. (2022) Cyber Security Expert Predicts Increase in Cyber Attacks in 2022 https://www.thisdaylive.com/index.php/2022/01/06/cyber-security-expert predicts-increase-in-cyber-attacks-in-2022/ retrieved Thursday, 23rd June 2022.

Olayemi, J. (2018). Combating the Menance of Cybercrime. *International Journal o*

f Computer Science and Mobile Computing, 3(6), 980-991.

Osho O. & Onoja A. D. (2015) National Cyber-security Policy and Strategy of Nigeria: a

Qualitative Analysis. *International Journal of Cyber-criminology (IJCC)*

Timothy, A.O. & Afia E.S. (2013) International Police (Interpol) and Crime Control in the

West African Sub-Region. *American Journal of Social Issues and Humanities. AJSIH*/ISSN:2276-6928

Tsado, Raufu, Ben-Edet & Krakrafaa-Bestman (2023) Combatting the threat of Cybercrime in Nigeria: Examining Current laws and policies. *Journal of applied theoretical and social science JATSS,* 2023; 5(4) 413-33

Umeh J. (2020) Cybersecurity: 9000 Nigerians attacked by Malware in 2019 vanguard.Retrievedfrom *https://vanguard.com/2020/02/cyber-security-9000- nigeriansattacked-by-malware-in-2019/*

Viko I.J. (2021) Analysis of the legal and institutional Framework for fighting cybercrime in Nigeria. *International journal of comparative law and legal philosophy (IJOCLLEP)* 3 (2)

Yar, M. (2005). The Novelty of Cybercrime: An Assessment In Light Of Routine Activity Theory. *European Journal of Criminology* 2(4), 407-27.