International Journal of Social Science and Human Research

ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 08 Issue 09 September 2025

DOI: 10.47191/ijsshr/v8-i9-75, Impact factor- 8.007

Page No: 7328-7338

Combating Transnational Crime in Nigeria: An Examination of the Activities of Interpol in Curbing Cybercrime, 2000 - 2024

Timothy Zakimayu Barje,[1] Hillary Nwabueze Ugwu[2]

[1,2]Department of History & International Studies, Nigeria Police Academy Wudil, Kano Nigeria

ABSTRACT: Cybercriminals in Nigeria are daily becoming bolder and devising ways to swindle unsuspecting victims in other countries across the globe and find a way of avoiding being detected and arrested by both local security forces and international ones. Cybercriminals have given Nigeria a bad reputation in several countries as their activities has left behind throngs of victims with sad tales. The research aims to study the activities of INTERPOL in Nigeria and how device ways to tackle cybercrimes in collaboration with similar security agencies in the country who are also on the tail of cybercriminals. The article uses a plethora of sources that varies from reports and documents from these agencies, oral interviews and published books and articles. The major findings of the research indicate that INTERPOL and has made significant progress in the fight against crime in the country through major breakthroughs in arrests of key cybercriminals and scammers. And also through collaboration with other Nigerian security agencies like the EFCC, NPF-NCC, NITDA etc., their operation has yielded some significant result. However, a lot still needs to be done to bring cybercrime under significant control in Nigeria.

KEYWORDS- INTERPOL, Cybercrime, Cyberattacks, Cybersecurity, Online Scam

INTRODUCTION

The rapid advancement of technology and the increasing reliance on digital platforms have transformed the landscape of crime, giving rise to a new category of offenses known as cybercrimes (David, 2007). These crimes, which include hacking, identity theft, romance scam, online fraud, and cyberbullying, pose significant challenges to law enforcement agencies worldwide. Nigeria, with its burgeoning internet user base and growing digital economy, has become a hotspot for various forms of cybercrime, impacting individuals, businesses, and the overall economy (Ogunleye, 2022).

Since the turn of the millennium, Nigeria has witnessed a surge in cybercriminal activities, often facilitated by the country's unique socio-economic conditions, including high unemployment rates, widespread poverty, and inadequate cybersecurity infrastructure. The implications of these crimes extend beyond national borders, as cybercriminals often operate transnationally, exploiting the global nature of the internet (Chukwuma, 2010). This has necessitated a coordinated international response to combat cybercrime effectively.

The International Criminal Police Organization (INTERPOL), plays a crucial role in facilitating international police cooperation and combating transnational crime, including cybercrime. Established in 1923, INTERPOL has evolved to address the complexities of modern crime, providing member countries with the tools, resources, and frameworks necessary to enhance their law enforcement capabilities (Guinchard, 2008). In the context of Nigeria, INTERPOL's involvement has been pivotal in fostering collaboration among law enforcement agencies, sharing intelligence, and providing training to combat cyber threats.

Nigeria's legal framework for addressing cybercrime has historically been weak, making it difficult to prosecute offenders effectively. Although laws like the Cybercrime (Prohibition, Prevention, etc.) Act of 2015 have been enacted; enforcement remains a challenge. Cybercrime often crosses national borders, complicating jurisdictional matters and making international cooperation essential yet difficult to navigate. Differences in laws and regulations between countries can hinder collaborative efforts to combat cybercrime. Many law enforcement agencies in Nigeria face resource constraints, including insufficient funding, training, and personnel dedicated to cybercrime units. There is a need for ongoing training and capacity building for law enforcement personnel to effectively handle cybercrime investigations and operations.

This research investigates and highlights the activities of INTERPOL as an international institution that is task with cooperating with the national security in ensuring that those who commit crimes that cut across the borders are brought to justice. The study intends to use some specific case studies to show the level of INTERPOL's involvement in the security architecture of the nation as a vital tool of cooperation with the Nigeria Police Force.

STATEMENT OF THE RESEARCH PROBLEM

The rapid advancement of technology and the increasing reliance on digital platforms have generally led to a significant rise in cybercrimes globally, with Nigeria being no exception. As the most populous country in Africa, Nigeria has witnessed a surge in cybercriminal activities, including online fraud, identity theft, hacking, and cyberbullying, which have profound implications for its economy, security, and social fabric. Despite the growing recognition of cybercrime as a critical issue, the effectiveness of international cooperation in combating these crimes remains a subject of scrutiny.

There is growing concerns about the number of users in the country that are involved in criminal activities using the cyberspace especially the internet. The consistent abuse and criminilisation of the network is speedily giving Nigeria a bad reputation as a nation known for its syndicates who use the internet to defraud unsuspecting victims from other countries.

INTERPOL, as a leading international organization dedicated to facilitating police cooperation across borders, plays a pivotal role in addressing transnational crime, including cybercrime. However, the specific impact of INTERPOL's activities in curbing cybercrimes in Nigeria from 2000 to 2024 needs further critical examination. Where a crime transcends the borders of several countries, it requires a similar network of security agencies to be able to apprehend the criminals. Hence cybercrime has become an international activity of crime that needs a careful study, and the activities of those responsible for checking it becomes a matter of constant review and assessment for better restrategising.[5]

The period from 2000 to 2024, could be considered as the time frame for the emergence and growth of cybercrime in Nigeria, which threw the nation into the limelight in with high level of prevalence in the global scene. From national crime that is popularly restricted to advance fee fraud popularly known as '419', the country's status as been blown globally with the emergence of new generation of crime lords that uses the advance fee fraud methods electronically, now known as 'yahoo yahoo' depicting the web connection from the popular search engine of the early years of the millennial.

CONCEPTUAL FRAMEWORK

Understanding cybersecurity and cybercrime can be understood from the organismic foundation of defining and explaining the concept of cyberspace. This is a digital platform or realm in which people, companies, government and machines communicate with each other and carryout transactions. This type of communications requires two common denominator (i) network connectivity and (ii) the exchange of information through remote access, which explains the external components or access. These communications are susceptible to negative external compromise such as robbery, cyberattacks and cyberespionage.

Hence, cybersecurity is that component which is critical in preventing and identifying the vulnerabilities of the network environment, and analyzing the potential threats and assessing the impact and consequences of such vulnerabilities; then providing the appropriate security measures (Zaballos & Herranz, 2013). There are multiple concepts associated with the word cyber. The challenge today is to clearly understand what these concepts represent and therefore manage a common and unified language. There is no doubt that some of the definitions and meaning might overlap and the concept are often misplaced. But within the context of this research, the following conceptual explanations as defined by Zaballos and Herranz, would be adopted:

Cybercrime: Refers to the different forms of crime that involves computers or networks when they are used to attack or are attacked.

Cybersecurity: Encompasses all the necessary elements required to defend and respond to cyber threats in the cyberspace e.g. technology, tools, policies, security measures, safeguards, guidelines, risk management approaches, actions, training, etc.

Cyberthreats: Are potential cyber events that may cause unwanted outcome, resulting in harm to a system or organisation. Threats may originate externally or internally and may originate from individual or organisation.

Cyberattacks: are the use of malicious codes that may affect computers and networks and lead to cybercrime, such as information and identity theft.

Cyber vulnerability: Is susceptibility in the protection of an asset or individual from cyberthreats.

LITERATURE REVIEW

According to Ezekiel et al (2021), cybercrimes in Nigeria could be said to have evolved in the early 2000s.This period witnessed a comprehensive growth and transformation of cybercrime in Nigeria for over two decades. Scholars have effectively contextualized the rise of cybercrime within the broader socio-economic and technological landscape of the country, making it a valuable resource for researchers, policymakers, and law enforcement agencies. The authors traced the history of cybercrime in Nigeria, by examining the historical context paying attention to those who are perceived to be the significant figures in the early stages. They further categorised cybercrime into distinct phases illustrating how the methods and motivation for cybercriminal activities evolved overtime.

However, the authors' focus was mainly on the evolution and strategy used by cybercriminals in defrauding their victims. In spite of the fact that the book has proven to be a useful source for this research, because it provided an in-depth outlook on areas that are even beyond the coverage of this project, it is important to note that the work lacks depths or analyses on ways through which cybercrime could be curtailed in the country. Also, it did not attempt to look at the role of the security agencies in curbing

cybercrime in the country. Wall and Williams (2013), provide insight into the complexities of cybercrime, making it informative for students, researchers, and practitioners alike. The authors explore the intricate and evolving relationship between cybercrime and cybersecurity on a global scale. This work delves into the definitions, types, and motivations behind cybercrime, illustrating challenges it poses to individuals, organizations, and governments worldwide. Although the work provides a thorough analysis of various forms of cybercrime including hacking, identity theft, and online fraud, while discussing the socio-economic factors that contribute to these criminal activities; It has equally emphasized the need for a comprehensive understanding of the digital landscape, highlighting the interconnectedness of different regions and the varying impacts of culture and law enforcement practices around the world.

In addition to outlining the nature of cyber threats, the authors also examine responses to cybercrime, including legal frameworks, policy developments, and preventive measures. It advocates for international collaboration and a proactive approach to cybersecurity, recognizing that effective solutions must address the technical, legal, and socio-political dimensions of the issue. This serves as a foundational text for academics, policymakers, and practitioners, providing both theoretical insights and practical strategies to combat cybercrime effectively in an increasingly digital world. The work is recognized for several strengths that contribute to the discourse on cybercrime and cybersecurity which centre on perspective, interdisciplinary approach, theoretical frameworks, insightful analysis, policy relevance, and current examples, focus on prevention and response, emphasis on victimology, authority and credibility, encouragement of critical thinking among others.

Taylor, and Fritsch (2015), offers a comprehensive overview of key topics in the field, staying current with the rapidly evolving landscape of digital security threats. Some potential gaps or weaknesses in the book include outdated information due to the rapidly evolving nature of technology and cybercrime. The book lacks in-depth coverage of emerging cyber threats, new attack vectors, or recent case studies. There is insufficient emphasis on practical tools or strategies for combating digital crime and terrorism in real-world scenarios. The limitations stem from the need for more frequent updates to keep pace with the fast-changing landscape of digital crimes and threats. The above limitations notwithstanding, the book exploration of the various forms of digital crime and terrorism in the modern era covering topics such as cybercrime, hacking, cyberterrorism, and related legal and ethical issues. It offers insights into the evolving landscape of digital threats and the challenges faced by law enforcement agencies and policymakers in combating these crimes. It serves as a comprehensive resource for students, researchers, and practitioners interested in understanding and addressing digital crime and terrorism. The book has Comprehensive Coverage as it provides a detailed examination of digital crime and digital terrorism, covering a wide range of topics such as cyber-attacks, cybercrime investigations, threat analysis, and digital forensics; Up-to-date information as of the 4th edition published in 2020, the book includes the latest information and trends in the field of digital crime and digital terrorism.

Holt and Adam (2011), provide an in-depth examination of the challenges law enforcement agencies face in addressing cybercrime and cyberterrorism in the modern digital age. Their research covers various topics such as the nature of cybercrimes, the role of law enforcement in combating cyber threats, and the strategies and techniques used by police to investigate and prosecute cyber offenders. It also discusses the importance of international cooperation and information sharing in effectively tackling cyber threats. Overall, the book offers valuable insights into the complexities of policing cybercrime and cyberterrorism, while also highlighting the need for continuous adaptation and innovation in law enforcement practices to keep up with evolving cyber threats.

The strength of the book covers a wide range of topics related to policing cybercrime and cyberterrorism, including the challenges faced by law enforcement agencies, the techniques used to investigate cybercrimes, and the legal and policy issues surrounding cybercrime and cyberterrorism. However, in as much as the book offers valuable insights into the challenges and strategies for addressing cyber threats, it is important to be aware of the potential weaknesses or gaps in the coverage of the topic which include limited coverage of specific cybercrime and cyberterrorism cases as it does not provide in-depth analysis or detailed case studies of significant cybercrime or cyberterrorism incidents, which could limit the reader's understanding of real-world examples and implications (Holt, 2016). The cybersecurity landscape is constantly evolving, with new threats and attack techniques emerging regularly. The book also does not cover the latest trends and developments in cybercrime and cyberterrorism, which makes the information outdated or incomplete.

Brenner (2011), explores the legal implications and challenges of cybercrime in the digital age. He examines various aspects of cybercrime, including hacking, online fraud, and identity theft, and discusses how these crimes are prosecuted and punished under current laws. Brenner also analyses the effectiveness of law enforcement efforts in combating cybercrime and offers insights into how the legal system can better address these evolving threats. Overall, a comprehensive overview of the complex legal issues surrounding cybercrime had been analysed and it offers recommendations for improving responses to this growing problem. The strength of the book lies in the fact that it provides a thorough examination of the legal challenges and issues related to cybercrime, offering a detailed analysis of various types of cybercrimes, their implications, and the outcomes of legal responses.

Brenner also offers insightful commentary on the effectiveness of current laws and law enforcement efforts in addressing cybercrime. The work provides recommendations for improving legal responses to cyber threats. The author is a renowned expert

in cyber law and policy, brings his expertise and real-world experience to the subject, providing readers with a thorough and authoritative understanding of the legal landscape surrounding cybercrime.

Kshetri (2015), explores the various challenges and issues faced by developing countries in the global south in addressing cybercrime and enhancing cybersecurity. It addresses the evolving nature of cyber threats, the impact of globalization on cybercrime, and the strategies and policies that countries in the global south are adopting to combat cyber threats. Kshetri also highlights the importance of international cooperation and capacity-building initiatives in promoting cybersecurity in the global south. Given the increasing prevalence of cybercrime and the growing importance of cybersecurity Kshetri's analysis sheds light on a pressing issue that affects countries around the world. Akujuobi, and Nwanguma (2019), discusses the prevalence of cybercrime and internet fraud in Nigeria, as well as the challenges faced in combating these crimes. The authors highlight the various types of cybercrimes that are common in the country, such as phishing scams, identity theft, and online scams targeting individuals and businesses. The article also discusses the challenges that law enforcement agencies and cybersecurity professionals face in Nigeria when addressing cybercrime, including limited resources, lack of specialized training, and jurisdictional issues. Extensive data or empirical evidence to support claims and recommendations appears to be a daunting challenge for the authors. More quantitative data and case studies could strengthen the arguments presented in the article. The article could have benefit from more specific examples of cybercrimes and internet fraud incidents in Nigeria to help illustrate the challenges faced in the country. Providing real-life examples can make the issues more tangible and relatable to readers but it is limited in this area. Consequently, the solutions proposed in the article is too broad or general, lacking specific strategies or actionable steps for implementing them.

The National Institute of Standards and Technology (NIST) in 2018 provided a voluntary guideline designed to help organizations manage and reduce cybersecurity risks. It provides a structured approach for organizations to enhance their cybersecurity posture while aligning their cybersecurity activities with business objectives. The Strengths of this framework lies in its flexibility. The framework is adaptable for organisations of all sizes and industries, allowing them to tailor the guidelines to their specific needs and resources. It establishes common language and standards, facilitating better communication about cybersecurity risks across diverse sectors. The framework emphasizes a risk-based approach, helping organisations prioritise actions based on their unique risk environment. However, despite the above promising strengths, it is important to note that the report is weakened by its voluntary nature. Since it is not mandatory, some organizations choose not to adopt the framework, which led to inconsistent cybersecurity practices across sectors. Smaller organizations lacked the resources or expertise to effectively implement the framework, resulting in unequal levels of cybersecurity preparedness.

Smith (2018), Master's thesis, evaluates the effectiveness of government agencies in the United States in combating cybercrime. Using a case study approach, the author examines the strategies and efforts of various agencies in preventing and enforcing laws related to cybercrime. The study highlights the strengths and weaknesses of these agencies in addressing the growing threat of cybercrime, providing insights on areas that may need improvement in order to enhance overall effectiveness in combatting cyber threats. EUROPOL's Internet Organised Crime Threat Assessment (IOCTA) is an important annual report that analyses the evolving landscape of cybercrime and its implications for law enforcement agencies across Europe and beyond (Smith). The Strengths of the assessment lies in its comprehensive analysis. The IOCTA provides an in-depth analysis of current threats posed by cybercriminals, highlighting various crime types, methods, and trends. It serves as a crucial and very reliable source of information for law enforcement agencies, allowing for informed decision-making and improved strategies in combating internet crime. The report fosters cooperation among member states, enabling a unified response to cross-border cybercrime. By illustrating emerging threats, the IOCTA raises awareness and promotes necessary training for law enforcement personnel.

The Weaknesses of the assessment lie in the dynamic nature of cybercrime. Cybercriminal methods evolve rapidly, which can make static assessments quickly outdated, potentially affecting the relevance of its findings. There are also information gaps as some cybercrime activities may go unreported, leading to incomplete data which could hinder comprehensive understanding. There are equally resource limitations. The law enforcement agencies may not always have sufficient resources or training to effectively implement the recommendations from the report. Accessibility too is also an issue of great importance: While aimed at law enforcement, some aspects of the IOCTA may not be easily digestible for those without a technical background, limiting its utility. Overall, while the IOCTA is a vital document for understanding and tackling internet organized crime, its effectiveness can be influenced by the rapidly changing cyber environment and resource constraints within law enforcement.

RESEARCH METHODOLOGY

This study will be based on historical and interdisciplinary approaches relying mostly on qualitative data. The study will benefit from both oral testimonies and evidences, written texts of various forms among others. The sources used in this study generally include primary, secondary and tertiary sources. The primary sources used include interview, study of policy documents, study of previous cases and investigations carried out by INTERPOL, review of INTERPOL reports, press releases, and publications related to cybercrime in Nigeria. The purpose is to gather historical data on INTERPOL's initiatives, strategies, and outcomes in combating cybercrime. In the case of interviews participants will comprise key stakeholders including INTERPOL officials,

Nigerian law enforcement agencies, cybersecurity experts, and representatives from NGOs involved in cybercrime prevention were interviewed. The interview format was semi-structured to allow for in-depth exploration of perspectives and experiences.

The secondary sources are published information which are products of other independent researches derived from primary sources or historical events. They provide context, commentary, and analysis, helping us understand the significance of primary data. This are mostly published books, articles from academic journals, newspapers and magazines and other published sources. Online sources and internet data are also widely consulted in this research. Databases and Digital Archives of institutions that provide access to collections of secondary analyses, articles, and reviews have been consulted.

DISCUSSION

Akinyemi (2019), observed that the fight against cybercrime in Nigeria has become increasingly critical as the nation experiences a surge in internet usage and digital transactions. With this growth, various forms of cybercrime such as fraud, identity theft, hacking, and online harassment have proliferated, posing significant threats to individuals, businesses, and the economy. However, the effectiveness of combatting these crimes is hampered by a range of institutional and operational barriers. Understanding these challenges is crucial for developing effective strategies and policies to enhance cybersecurity and improve law enforcement responses.

Types of Cybercriminal Activities Prevalent in Nigeria

The socio-economic factors contributing to the rise of internet fraud in Nigeria has evolved into a significant issue, encompassing a range of illegal activities that exploit technology and the internet for financial gain or malicious intent (Chukwuma, 2021). The types of cyber-criminal activities prevalent in Nigeria are very numerous and complex too. These include Email scams and phishing. In this case, cyber-criminals often engage in email scams, commonly known as advance-fee fraud or '419 scams (CSEAN, 2023). These involve tricking victims into sending money with the promise of receiving a larger sum in return. Scammers typically impersonate wealthy individuals, government officials, or organizations, claiming that they need assistance in transferring large sums of money. Victims are asked to pay fees to help facilitate the transaction, which is, of course, a ruse.

Online identity theft is another type of cybercrime very common in Nigeria today through which cyber criminals steal personal information to impersonate individuals or create fake identities online. This can include hacking into databases or obtaining information from data breaches, phishing attacks, or social engineering. Once they have personal details, criminals can open bank accounts, apply for loans, or engage in other fraudulent activities.

Fraudulent Financial Schemes is of various forms and schemes which include Ponzi and pyramid schemes that are prevalent in Nigeria today. It often utilizes internet platforms for recruitment and investment. Victims are promised high returns on investment with little risk but are often left with significant losses as funds are redirected to pay earlier investors or for the scammers' personal use.

Ransomware attacks is another very common form of cybercrime in which cyber criminals deploy malware that encrypts victims' files or systems, demanding a ransom for decryption. These attacks can target individuals or organizations, including small businesses, schools, and healthcare facilities (CSEAN). Attackers typically demand payment in cryptocurrencies to maintain anonymity. Social Media Scams is another very common cybercrime in Nigeria which has become a significant issue in the Nigeria cyberspace. It is often characterized by various types of illegal activities that exploit technology for financial gain or other malicious purposes (CSEAN).

Regular and emerging threats on the other hand include government infrastructure as a target (GIAAT), malware, another year of ransomware, attacks on financial institutions, attacks on the cloud, menace of insider threats, cryptocurrency-based threats, Ponzi scheme, rug and pull, pump and dump, phishing and social engineering, privacy breach by online money lenders, increased cyber-attacks through networks of higher institutions among others. Small and medium scale enterprises (SMEs) also feel the heat or brunt of cyber threats. This is because SMEs have limited resources to invest in cybersecurity, they are known to have lesser number of IT staff or less expertise in cyber security and also lack the level of security awareness that big organizations have.

In fact, Adebayo (2020), has adduced that cybercrime have become a significant issue in Nigeria, with various activities perpetrated by cyber criminals. These activities can take many forms, including internet fraud (Yahoo Yahoo). This is one of the most notorious forms of cybercrime in Nigeria, where fraudsters, often young men, use the internet to deceive victims, typically foreigners, into sending money. Their tactics include romance scams, business scams, and lottery scams (Yahaya, 2024).

THE RELATIONSHIP BETWEEN INTERPOL AND OTHER STAKEHOLDERS IN THE NIGERIA CYBER SPACE

Ibrahim, in a thesis on the impacts of INTERPOL on law enforcement collaboration in Nigeria, made reference to the relationship between INTERPOL and various actors and stakeholders in Nigeria's cyber space (Ibrahim, 2022). This is multifaceted and involves collaboration, information sharing, and capacity-building initiatives. The key elements of this relationship are in various levels. At the level of government agencies, we have law enforcement collaboration and policy development. At the private

sector level, we have public-private partnerships, awareness and training. At the academic institutions level, we have capacity building, research and development. At the international organizations level, we have global collaboration and information exchange. At the civil society level, we have engagement with NGOs and community outreach while at the regional initiatives level, we have ECOWAS, African Union and joint operations/trainings among others.

Relationship between INTERPOL and EFCC

The Economic and Financial Crimes Commission (EFCC) had been partnering with Interpol in the fight against cybercrime since its inception. As a matter of fact, the EFCC has a dedicated unit that collaborates with Interpol, and share data and intelligence regarding high target criminals and cybercrime gangs operating in the country. The EFCC is Nigeria's primary agency responsible for investigating and prosecuting economic and financial crimes, including fraud, money laundering, and cybercrime. Established in 2003, the EFCC aims to promote transparency and accountability in Nigeria's financial systems. INTERPOL and EFCC collaborate in providing a secure communication platform for member countries, including Nigeria, to share intelligence and information related to criminal activities. The EFCC utilizes this platform to receive alerts and updates on emerging trends in cybercrime and financial fraud. INTERPOL assists the EFCC in operational matters, such as coordinating joint operations and investigations that involve multiple jurisdictions. This is particularly important in cases of cybercrime, where perpetrators often operate across borders. The EFCC has access to INTERPOL's databases, which contain information on wanted persons, stolen property, and other criminal intelligence. This access aids the EFCC in tracking down cybercriminals and financial fraudsters who may be operating internationally. The real examples and instances of cooperation between the two organizations can be seen in the following:

Operation Falcon: In 2019, INTERPOL launched Operation Falcon, a global initiative aimed at combating online fraud and cybercrime. The EFCC participated in this operation, which involved coordinated efforts to dismantle networks involved in online scams, particularly those targeting individuals and businesses. The operation led to several arrests and the seizure of assets linked to cybercriminals. The relationship between INTERPOL and the EFCC is vital for addressing the challenges posed by cybercrime and financial fraud in Nigeria. Through information sharing, capacity building, operational support, and collaborative efforts, both organizations work together to combat transnational crime effectively. The examples of joint operations, training initiatives, and specific case of collaborations illustrate the importance of international cooperation in enhancing law enforcement capabilities and ensuring justice in an increasingly digital world.

Relationship between INTERPOL and NPF-NCCC

The relationship between Interpol and the Nigerian Police Force's National Cybercrime Centre (NPF-NCCC) is a crucial aspect of international and national efforts to combat cybercrime. This collaboration is essential given the increasing prevalence of cybercrime globally, including in Nigeria, which has become a significant hub for various cybercriminal activities. Interpol facilitates international police cooperation and provides a platform for law enforcement agencies from different countries to collaborate on transnational crime issues, including cybercrime. It offers resources, training, and operational support to member countries (Orji, 2025).

NPF-NCCC is the National Cybercrime Centre, established under the Nigerian Police Force, is tasked with combating cybercrime in Nigeria. It focuses on preventing, investigating, and prosecuting cyber-related offenses, as well as raising awareness about cyber threats. The relationship and cooperation between the two organizations can be seen in the several areas. One of the primary ways INTERPOL and NPF-NCCC collaborate is through the sharing of intelligence and information related to cybercrime. INTERPOL provides access to its databases, which include information on known cybercriminals, trends, and techniques used in cybercrime. This information is vital for the NPF-NCCC to understand the landscape of cyber threats in Nigeria. In 2020, INTERPOL launched an operation called "Operation Goldfish," which targeted online fraud and scams. The NPF-NCCC participated in this operation, sharing intelligence on local cybercriminal networks and receiving insights from other countries involved in the operation.

INTERPOL conducts training programs and workshops for law enforcement agencies in member countries, including Nigeria. These programs aim to enhance the skills and knowledge of officers in dealing with cybercrime. In 2019, INTERPOL organized a training workshop in Nigeria focused on cybercrime investigation techniques. Officers from the NPF-NCCC attended this workshop, learning about digital forensics, cyber threat analysis, and the use of technology in investigations. Joint Operations: INTERPOL and NPF-NCCC often collaborate on joint operations to tackle specific cybercrime issues. These operations may involve coordinated actions across multiple countries to dismantle cybercriminal networks.

INTERPOL assists the NPF-NCCC in developing legal frameworks and policies to combat cybercrime effectively. This includes guidance on legislation that aligns with international standards. INTERPOL has provided technical assistance to Nigeria in drafting laws related to cybercrime, helping to ensure that the legal framework is robust enough to prosecute cybercriminals effectively. The relationship between INTERPOL and the NPF-NCCC is vital for addressing the growing threat of cybercrime in Nigeria. Through information sharing, training, joint operations, public awareness campaigns, and legal assistance, both

organizations work together to enhance Nigeria's capacity to combat cybercrime. Continued collaboration and adaptation to emerging threats will be essential for effective cybercrime prevention and response in the future. NPF-NCCC handles cyber related cases reported either through petitions, cybercrime e-reporting portal or through intel received from informants. A total of 465 cases which include NCB Messages and other sources were distributed to each Team.

Computer related frauds seem to dominate followed by cyber bullying while OBT, Credit card frauds, child exploitation and BEC were very minimal. It was gathered that 34 suspects of various cybercrimes were arrested. It is also very important to note that sequel to the stride made by operatives of the center in tracing and bursting cybercrime kingpins in sting operations, several recoveries have been recorded within the year under review thus: ₦51,444,170.78 cash, USD 7,861 and EUR 640 were recovered from suspects and repatriated to the victims. Six Smartphones, three SIM cards registration machines and unspecified number of automobiles and laptop computers were also recovered. The NPF-NCCC also partook in several operations within the year under review and the two major operations were HAECHI-III and operation Dark SIM. While operation HAECHI-III was an international collaboration with the Korea National Police Agency (KNPA), the Nigeria Financial Intelligence Unit (NFIU) and the National Central Bureau (NCB) of INTERPOL in Nigeria. During the operation, personnel of the center were deployed to different states in Nigeria including Lagos as tracking tools at the disposal of the center to locate persons of interest and threat actors in these states.

Operation Dark SIM was an initiative of the center aimed at curbing the menace of illegal SIM registration which proliferate the number of SIM cards which can't be traced to its actual user. These SIM cards are mostly used by criminal elements to perpetrate frauds, kidnapping and other telecommunication facilitated crimes. The operation was a huge success as threat actors within the federal capital territory were tracked, monitored and arrested. These arrested threat actors are currently undergoing prosecution. The NPF-NCCC annual report (2024) reveals that 508 cybercrime cases were reported with sextortion, cyberstalking and computer related fraud as the most prominent.

Table I: General crime statistics from the NPF-NCCC in the year 2024

Sr. No.	*Cybercrimes*	*No. of Cases*
1	Business Email Compromise	4
2	Computer Related Fraud	92
3	Cyberstalking	83
4	Defamation	14
5	Forgery	2
6	Impersonation	13
7	Intelligence Report	9
8	Romance Scam	3
9	Sextortion	4
10	Threat to life	18
11	Unauthorized Access	2

Source: NPF-NCCC 2024 Annual Report

Table II: Number of Cybercrime Cases Reported and the Means it was Reported

Sr. No.	*No. of Cybercrimes Cases Reported*	*Means through which it was reported*
1	104	Petition
2	42	Intel
3	362	NCB

Relationship between INTERPOL and ngCERT

The relationship between INTERPOL and Nigeria Computer Emergency Response Team (ngCERT), is crucial in addressing cybercrime on a global scale. This collaboration is particularly important in countries like Nigeria, where cybercrime

has become a significant issue. The ngCERT is a national initiative aimed at improving the country's cybersecurity posture. It serves as a focal point for cybersecurity incidents, providing support, guidance, and coordination in response to cyber threats and attacks (Director, 2024). INTERPOL provides a framework for member countries to share intelligence related to cyber threats and incidents. ngCERT can leverage this platform to receive timely information about emerging cyber threats, vulnerabilities, and attack vectors that may affect Nigeria. For example, if INTERPOL identifies a new malware strain being used in cyberattacks across multiple countries, it can disseminate this information to ngCERT, which can then alert Nigerian organizations and individuals to take preventive measures.

INTERPOL and ngCERT can collaborate on public awareness campaigns to educate citizens and businesses about cybersecurity risks and best practices. This is essential in a country like Nigeria, where awareness of cyber threats may be limited. An example of this collaboration could be a joint campaign to raise awareness about phishing scams, where both organizations provide resources and information to help individuals recognize and avoid such threats.

Relationship between INTERPOL and NITDA

The relationship between INTERPOL and NITDA (the National Information Technology Development Agency) in Nigeria is primarily focused on enhancing cybersecurity and combating cybercrime. Both organizations play crucial roles in their respective domains, and their collaboration is essential for addressing the growing challenges posed by cyber threats. NITDA is a Nigerian government agency under the Federal Ministry of Communications and Digital Economy. Its primary mandate is to develop and regulate information technology in Nigeria. NITDA is responsible for promoting the use of IT in various sectors, ensuring cybersecurity, and implementing policies that foster the growth of the digital economy. One of its key roles is to enhance the country's cybersecurity posture and protect critical information infrastructure. INTERPOL provides a platform for NITDA to share information about cyber threats and incidents with other member countries. This collaboration allows Nigeria to benefit from global intelligence on emerging cyber threats and trends. For example, if INTERPOL identifies a new malware strain affecting multiple countries, it can alert NITDA and other Nigerian agencies to take preventive measures. NITDA has developed a Cybercrime Reporting Platform to facilitate the reporting of cyber incidents by citizens and organizations. INTERPOL has provided technical assistance and guidance in setting up this platform, ensuring it aligns with international standards for reporting and responding to cybercrime.

EXAMINATION OF INTERPOL'S ACTIVITIES IN NIGERIA

Operation Black Wrist is one of the operations of INTERPOL which focuses on combating online fraud, particularly in West Africa. It aimed to disrupt the activities of cybercriminals involved in various form of online scams. INTERPOL's Project Connect is another operation of INTERPOL in Nigeria. This project, initiated in collaboration with the Nigerian Police and other stakeholders, aimed to strengthen the capacity of law enforcement to deal with cybercrime effectively. It included training sessions, workshops, and the establishment of a dedicated cybercrime unit in Nigeria.

The arrest of 'Yahoo boys' in recent raids is another major operation of INTERPOL in Nigeria. Over the years, INTERPOL has supported Nigerian law enforcement in multiple operations targeting internet fraudsters, often referred to as 'Yahoo boys'. This includes incidents where INTERPOL provided resources and expertise that led to the arrests of numerous suspects engaged in various online fraud schemes. Partnerships with Nigerian financial institutions is another very potent operational strategy that has yielded great results. INTERPOL has worked with banks and financial organizations in Nigeria to combat cybercrime, focusing on sharing intelligence about fraudulent activities, enhancing cybersecurity measures, and ensuring swift responses to cyber threats.

Public awareness campaign is another major operational strategy that has also produced results. Although not a direct law enforcement operation, INTERPOL has engaged with Nigerian authorities to promote public awareness of cybercrimes, educating citizens on how to protect themselves from online scams, which indirectly supports law enforcement efforts by reducing the number of victims. These cases and operations highlight INTERPOL's ongoing commitment to combatting cybercrime in Nigeria, addressing both the operational and preventive aspects of the issue. Ibrahim, in a Master's thesis on the role of INTERPOL in enhancing Nigeria's security framework noted that INTERPOL plays a significant role in global law enforcement cooperation, and its activities in Nigeria encompass various objectives aimed at improving security and combating transnational crime (Bakari, 2020).

CHALLENGES FACED BY INTERPOL IN CURBING CYBERCRIMES IN NIGERIA

Abubakar, in a conference paper presented addressing cybercrime in Nigeria and policy recommendations, observed that curbing cybercrime in Nigeria poses several challenges for INTERPOL and local law enforcement agencies (Abubakar, 2021). The rapidly evolving nature of cyber threats, combined with the unique socio-political and economic circumstances in Nigeria, complicates efforts to address this issue. The challenges faced by INTERPOL in curbing cybercrime in Nigeria are multidimensional

and include limited technical capacity such as skill gaps and technological deficiencies. Legal and regulatory framework like jurisdictional issues and outdated laws. Others include underreporting, lack of awareness and cultural factors. Coordination and collaboration challenges like inter-agency coordination and international collaboration are also very key. Resource constraints, funding limitations, equipment and software issues as well as the evolving nature of cybercrime cannot be underestimated. Rapidly changing tactics, cryptocurrency and anonymity are equally serious factors to be considered. Public trust and engagement, distrust in authorities and engagement with private sector are also vital issues in this regard.

There is often a lack of skilled personnel who are trained in cybersecurity and cybercrime investigation techniques. This limits the effectiveness of local law enforcement agencies. Many agencies do not have adequate technological tools and infrastructure to investigate cybercrime effectively. Nigeria's legal framework regarding cybercrime is still developing. Existing laws may not adequately address the nuances of modern cyber threats, making prosecution challenging. Cybercrime often crosses borders, leading to complexities in jurisdiction and legal cooperation between countries. This makes it difficult to pursue offenders effectively.

Many victims of cybercrime do not report incidents due to a lack of understanding about the reporting process or fear of stigma. Cultural attitudes towards authority and law enforcement may discourage individuals or organizations from reporting cybercrimes. There can be challenges in coordination among various local agencies and INTERPOL due to bureaucratic processes and inefficiencies in communication. Although INTERPOL facilitates international cooperation, varying levels of commitment among member states can hinder prompt action against cybercriminals who operate across borders.

Local law enforcement agencies often struggle with budget constraints that limit their ability to invest in cybersecurity measures and training. The lack of access to advanced cybersecurity tools and software hampers the ability to detect and respond to cyber threats effectively. Cybercriminals continually adapt their techniques, making it challenging for law enforcement to keep up. Emerging threats such as ransomware, phishing attacks, and hacking require constant vigilance and updated strategies. The rise of cryptocurrencies poses additional challenges in tracking illicit financial transactions associated with cybercrime.

Many citizens may hesitate to report cybercrimes due to a lack of trust in law enforcement capabilities or the fear that their complaints will not be taken seriously. Insufficient collaboration with private companies that manage critical infrastructure and online services can limit information sharing and proactive measures against cyber threats. The challenges INTERPOL faces in curbing cybercrime in Nigeria are multifaceted and require comprehensive strategies addressing legal, technical, and operational deficiencies. Building local capacity, ensuring robust legal frameworks, enhancing inter-agency collaboration, and fostering public awareness are critical steps toward effectively tackling cybercrime in Nigeria. Additionally, there is a need for ongoing support and engagement from international partners, including INTERPOL, to create a more resilient cybersecurity environment.

Akinwunmi (2019), in his study of the role of INTERPOL in combating transnational crime in Nigeria noted that the institutional barriers to the efforts of INTERPOL in curbing cybercrimes in Nigeria rang from the weak legal framework, insufficient collaboration, corruption and lack of accountability, limited public awareness and education among others. Although Nigeria has made strides in establishing laws to combat cybercrime, such as the Cybercrime (Prohibition, Prevention, etc.) Act of 2015, there are gaps and ambiguities in the legal framework that hinder effective prosecution. Inconsistent application of laws and jurisdictional challenges can impede the ability of law enforcement agencies to act decisively.

Adeyemi, observes that in the fight against cybercrime, Nigeria faces several operational barriers that hinder effective law enforcement and prevention strategies. These challenges involve a combination of technological, institutional, legal, and societal factors. These operational barriers include weak cybersecurity infrastructure, lack of skilled personnel, legal and regulatory challenges, lack of coordination among agencies, public awareness and education, resource constraints among others. Inadequate security measures, insufficient investment and outdated technology constitute weakness in our cybersecurity infrastructure. Many organizations, both public and private, lack robust cybersecurity measures, making them vulnerable to attacks. The government and businesses often do not invest adequately in cybersecurity technologies and training. Many institutions rely on outdated systems that are not well equipped to handle modern cyber threats.

Skill shortages, training and development are very critical personnel issues that hinder INTERPOL's operations in Nigeria. There is a significant shortage of trained cybersecurity professionals in Nigeria, which limits the capacity to effectively combat cybercrime. Existing personnel may lack access to continuous education and training programs to keep up with evolving cyber threats. Inadequate legislation, jurisdictional issues and law enforcement gaps are some of the legal and regulatory challenges faced by INTERPOL in Nigeria. Existing laws may be outdated or not comprehensive enough to address the complexities of cybercrime. Cybercrime often transcends national borders, complicating enforcement and cooperation between countries. The existing legal frameworks can be slow to adapt to the rapidly changing nature of cyber threats.

Fragmented response and inadequate communication lead to discoordination among cyber security agencies and stakeholders. Different agencies may have overlapping mandates but lack coordination, leading to inefficiencies in tackling cybercrime. Poor communication between law enforcement agencies, government bodies, and private sector organizations hampers collaborative efforts. Limited awareness and cultural attitudes are also serious impediments to INTERPOL's efforts in Nigeria.

Many citizens and organizations are not fully aware of the risks associated with cybercrime or how to protect themselves. There may be cultural factors that prevent individuals from reporting cybercrime incidents due to fear of stigma or lack of trust in law enforcement. Funding Limitations include limited budgets for law enforcement agencies which has made it very difficult for INTERPOL to meet up with its set goals and targets with regard to curbing cybercrimes in Nigeria.

CONCLUSION

Transnational crime is daily increasing in the country, more worrisome is the rate at which young adults are actively engaged in the criminal craft. It has become a career for some, whereby young teens are being groomed by their peers and other adults in the act of cybercrime. Over the years, INTERPOL has made significant progress in the battle against cybercriminals.

REFERENCES

1) Abubakar, A. 2021. "Addressing Cybercrime in Nigeria: Policy Recommendations." Paper presented at the International Conference on Cybersecurity. Abuja, Nigeria.
2) Adebayo, A. 2020. Cybercrime in Nigeria: A Comprehensive Guide. Lagos: Nigerian Cybersecurity Press.
3) Adebayo, T. 2023. The Impact of INTERPOL on Cybercrime Prevention in Nigeria: A Policy Analysis. Master's Thesis, University of Lagos.
4) Adeyemi, T. INTERPOL's Struggles in Nigeria: A Look at Operational Challenges. *The Guardian* https://www.guardian.ng
5) Akanbi, O. 2023. "Reforming Nigeria's Law Enforcement: Lessons from INTERPOL's Engagement." *Journal of Law Enforcement and Public Safety.* Volume 15, Issue 1, 22-40.
6) Akinwunmi, O. 2019. "The Role of INTERPOL in Combatting Transnational Crime in Nigeria: Challenges and Prospects." *Journal of African Law.* Volume 63, Issue 2, 123-145.
7) Akinyemi, O. 2019. "The Role of Law Enforcement Agencies in Combating Cybercrime in Nigeria." *International Journal of Cyber Criminology.* Vol. 13, Issue 1, 123-135.
8) Akujuobi, C.A. and Nwanguma, E.T. 2019. "Cybercrime and Internet Fraud in Nigeria: Current Challenges and Solutions" *Journal of Computer Security*. Volume 7, Issue 2, 94-109.
9) ASP Orji. 2025. Oral Interview. NPF-NCCC Abuja, Tuesday 21 January.
10) Bakari, A. 2024. Oral Interview. National Information Technology Development Agency (NITDA) Abuja. Friday 13 December.
11) Brenner, S. 2011. Cybercrime and the Law: Challenges, Issues, and Outcomes. New York City: Springer.
12) Chukwuma, A. 2021. "The Rise of Internet Fraud in Nigeria: A Socio-Economic Perspective." *African Journal of Criminology and Justice Studies.* Volume 14, Issue 2, 23-40.
13) Chukwuma, O. 2021. "The Role of INTERPOL in Curbing Cybercrime in Africa: A Case Study of Nigeria." *African Journal of Criminology and Justice Studies*. Volume 14, Issue 1, 45-62.
14) CSEAN 2023 Annual Cyber Threat Reports www.CSEAN-Cyber-Threat-Forecast-2023 (1).pdf
15) David, W.S. 2007. Cybercrime: The Transformation of Crime in the Information Age. United Kingdom: Centre for Criminal Justice Studies, School of Law, University of Leeds.
16) Europol Report. 2021. Internet Organised Crime Threat Assessment (IOCTA).
17) Ezekiel, M., Abdullahi, S. and Abdulkarim R. 2021. "A Historical Assessment of Cybercrime in Nigeria: Implication for Schools and National Development." Journal of Research in Humanities and Social Science. Volume 9, Issue 9, 84-94.
18) Guinchard, A. 2008. "Cybercrime: The Transformation of Crime in the Information Age." Information, Communication and Society. Volume 11, Issue 7, 1030-1032.
19) Holt, T. J. and Adam, M.B. 2011. "Low Self-Control, Deviant Peer Associations, and Juvenile Cyber deviance." American Journal of Criminal Justice. Volume 37, Issue 3,1-18.
20) Holt, T.J. 2016. Cybercrime and Society. Washington DC: Sage Publications.
21) Ibrahim, M. 2022. The Impact of INTERPOL on Law Enforcement Collaboration in Nigeria. Master's Thesis, University of Nigeria Nsukka, Nigeria.
22) Kshetri, N. 2015. Cybercrime and Cybersecurity in the Global South. London: Palgrave Macmillan.
23) National Institute of Standards and Technology (NIST), Cybersecurity Framework, 2018.
24) Ogunleye, O. 2022. "Cybercrime in Nigeria: Trends, Challenges and INTERPOL's Response." Journal of Cyber Policy. Volume 7, Issue 2, 123-140.
25) Smith, B. 2018. The Effectiveness of Government Agencies in Combating Cybercrime: A Case Study of the United States. Master's thesis 2018.
26) Taylor, R.W. and Fritsch, E.J. 2015. Digital Crime and Digital Terrorism. London: Pearson.
27) The Director. 2024. Oral Interview. NSA-NG CERT Abuja, Friday 13 December.

28) United Nations Office on Drugs and Crime (UNODC): Report on Cybercrime. https://www.unodc.org/unodc/en/cybercrime/index.html.
29) Wall, D.S. and Williams, M.L. 2013. Cybercrime: The Transformation of Crime in the Information Age. United Kingdom: Polity Press.
30) Yahaya, T. 2024. Oral Interview, Research Officer I of the Department of Planning, Policy, Research and Statistics (DPPRS), 3 December.
31) Zaballos, A. G. and Herranz, F. G. 2013. From Cybersecurity to Cybercrime: A Framework for Analysis and Implementation. IDB Inter-American Development Bank http://www.iadb.org

There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non Commercial 4.0 International (CC BY-NC 4.0) (https://creativecommons.org/licenses/by-nc/4.0/), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.