DIGITAL CRIME AND POLICE RESPONSE IN NIGERIA: INSTITUTIONAL CHALLENGES AND SECURITY IMPLICATIONS

Osaretin Akinola Osho

Command Finance Office, the Nigeria Police Force, State Command Headquarters, Diamond Hill, Calabar. Cross River State.

oshoosaretin@gmail.com

ABSTRACT: This study examines the intersection of digital transformation and the challenges facing the Nigeria Police Force (NPF) in addressing digital-related crimes and their broader implications for national security. The study employed the qualitative approach. Data for the study was collected through primary sources, including key informant interviews (KIIs) and in-depth interviews (IDIs) and other secondary sources such as books, journals and media reports. Based on the Situational Crime Prevention (SCP) theoretical framework, findings show that the NPF's limitations stem from inadequate funding, poor digital infrastructure and equipment, institutional decay, and insufficient training. Although government efforts such as establishing digital literacy centres, initiating training and retraining programs, and partnering with local and international agencies represent steps in the right direction, their effectiveness is often undermined by systemic corruption and institutional weaknesses. These challenges have serious implications for national security. The study emphasises the urgent need to address these barriers, with particular attention to sustained political will and increased investment in the sector.

Keywords: Policing, Digital, Yahoo-Yahoo, Crime, Technology, CBEX

INTRODUCTION

Technology plays a multifaceted role in both facilitating and combating crime. Innovations in information and communication technology (ICT)—such as closed-circuit television (CCTV), Geographic Information Systems (GIS), and biometric identification— are not new, and they have enhanced crime detection and prevention capabilities (Grabosky, 1989). However, these same advancements have also paved the way for new forms of criminal activity, including cybercrime and identity theft (Brey, 2017). The digital transformation of the 21st century is reshaping the landscape of national security and internal policing. National security now entails safeguarding a nation from internal and external threats that could jeopardise its peace, stability, and development.

As criminal tactics increasingly rely on digital tools—ranging from cyber fraud and online radicalisation to digital surveillance and the spread of misinformation—law enforcement agencies must adapt to these evolving threats. Both national and international organizations, including INTERPOL and the United Nations Office on Drugs and Crime (UNODC), have taken steps to address these challenges. Nonetheless, cybercrime and related offenses continue to rise.

While developed countries have responded with advanced technological solutions to detect and deter crime, many developing nations continue to struggle to confront or fully understand the implications of the digital era. In Nigeria, law enforcement agencies have made some progress, but substantial work remains. At the forefront of these efforts is the Nigeria Police Force (NPF), which traces its origins back to 1820. The Royal Niger Company established the Royal Niger Company Constabulary in 1888, with its headquarters in Lokoja. Around the same time, the Hausa Constabulary, a paramilitary force comprising approximately 1,200 men, was established. In 1894, the Niger Coast Constabulary was founded in Calabar under the Niger Coast Protectorate, and the Lagos Police Force was formed in 1896 to maintain order in the Lagos Colony (NPF, 2024a). Since colonial times, the NPF has undergone various reforms. According to the 1999 Constitution, the Nigeria Police is the national police force with exclusive jurisdiction across the entire country. The Constitution also allows for the creation of specialised branches within the NPF for the protection of strategic national infrastructures such as harbours, waterways, railways, and airfields.

Although significant research has explored technology use (Isman, 2012) and the Nigeria Police Force (Alemika, 2000; Osho, 2025a; 2025b), insufficient focus has been placed on the challenges posed by an increasingly digital crime landscape. Hindered by institutional decline, underfunding, corruption, inadequate training, and low morale, the Nigeria Police Force struggles to adapt to digital transformations. This study examines these challenges and their impact on Nigeria's national security in a rapidly digitising world. The research questions are: What obstacles do the Nigeria Police Force face in addressing digital crime? What measures is the government taking to address these issues? What implication do these challenges have on national security? The answers to these questions will be of immense significance to crime prevention, security, and policing.

LITERATURE REVIEW

It is trite to understand the difference between digital and cybercrime. Cybercrime: Refers specifically to crimes committed using the internet or targeting computers, networks, or online systems. Examples: Hacking, phishing, and ransomware attacks. On the other hand, Digital Crime is a broader term that includes any crime involving digital devices or technologies, whether or not the internet is involved. Some examples are the use of Universal Serial Bus (USB) to steal files from a computer, tampering with a CCTV system, or altering data on a local machine.

Table 1: Difference between Cybercrime and Digital Crime

Feature	Cybercrime	Digital Crime
Involves internet?	Yes	Not always
Broader category?	No	Yes
Examples	Phishing, hacking	Data theft via USB, modifying digital records
Relationship	Subset of digital crime	Encompasses cybercrime and more

Source: Author compilation

The transformation of crime in the digital era has demanded a corresponding shift in crime prevention and law enforcement approaches. Technology has become an essential asset in modern policing and the global criminal justice system. From surveillance tools and biometric identification to artificial intelligence (AI), data analytics, and cyber forensics, these innovations are reshaping how crimes are detected, prevented, and prosecuted. Closed-circuit television (CCTV) is among the earliest and most widely utilised technologies in policing. Research has shown that surveillance systems significantly deter crime in urban environments, especially in areas prone to property-related offences. For instance, a meta-analysis by Welsh and Farrington (2009) found that CCTV systems led to a moderate but statistically significant 16% reduction in crime in experimental areas compared to control groups. The greatest impact was seen in car parks, with crime dropping by 51%, while the effects in residential neighbourhoods and city centres were minimal or statistically insignificant. Their analysis, which focused on 44 methodologically rigorous studies, revealed that CCTV was most effective when clearly identified as the primary intervention, particularly in UK-based initiatives.

Further advancing urban crime analysis, Ristea and Leitner (2020) underscored the importance of interdisciplinary, GIS-based frameworks. By combining theoretical insights with geospatial analysis and advanced data techniques, they propose a proactive and strategic approach to policing, moving beyond passive data collection to spatially informed enforcement strategies. Another breakthrough in crime prevention is the use of big data and predictive analytics. Predictive policing involves algorithmic analysis of historical crime data to forecast future criminal activity and deploy law enforcement resources accordingly. An example is the "PredPol" software, used in several U.S. cities, which identifies potential crime hotspots (Perry et al., 2013). While results have shown moderate effectiveness, critics like Lum and Isaac (2016) warn that such systems may perpetuate racial bias and deepen existing inequalities in policing. Despite these concerns, predictive analytics remains a valuable supplement to conventional crime-fighting methods.

In today’s digital crime landscape, offenses such as cybercrime and cryptocurrency-related fraud are on the rise. These include a broad spectrum of illicit activities—from identity theft and online scams to cyberterrorism. To combat these threats, law enforcement agencies are investing in digital forensic laboratories and specialised cybercrime units. According to Casey (2011), digital forensics is vital for tracing criminal activity through tools like email analysis, IP tracking, and metadata interpretation.

In developing countries such as Nigeria, agencies like the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force Cybercrime Unit have made efforts to address internet-based crimes, including the notorious “Yahoo Yahoo” scams. These efforts often involve collaboration with international agencies such as INTERPOL and Europol. Nevertheless, significant challenges persist, particularly regarding technological infrastructure and workforce training (Ojedokun & Eraye, 2012; Egieleva, 2022).

Artificial Intelligence (AI) is increasingly used in facial recognition, voice analysis, and behavioural analytics. AI applications in law enforcement include crime pattern recognition, automatic number plate recognition (ANPR), and intelligent CCTV systems (Garvie, Bedoya & Frankle, 2016). Similarly, biometric systems, such as fingerprint databases (e.g., AFIS), iris scanners, and DNA profiling, have transformed criminal investigations, enabling faster and more accurate suspect identification (Wayman et al., 2005). In many parts of Africa, including Nigeria, mobile technology is being harnessed for community policing. Initiatives such as the use of mobile apps for crime reporting (e.g., the "NPF Rescue Me" app) aim to bridge the communication gap between citizens and police authorities. Ajayi and Adebayo (2020) note that while these tools improve responsiveness and trust, their effectiveness is often undermined by poor infrastructure, low digital literacy, and a lack of political will to act on reports. While technology offers vast potential in fighting crime, several limitations exist such as Infrastructural deficits in developing nations limit implementation., The high cost of equipment and training makes adoption difficult; Cyber threats are constantly evolving, outpacing enforcement capabilities; ethical concerns over surveillance, profiling, and data misuse raise questions about democratic accountability (Zuboff, 2019).

The integration of technology into policing and crime prevention is both inevitable and indispensable in the digital age. For countries like Nigeria, the strategic deployment of technological tools accompanied by investment in infrastructure, capacity building, and legal frameworks can significantly enhance the effectiveness of law enforcement. However, these efforts must be balanced with considerations of ethics, human rights, and systemic reform.

Theoretical Framework

The study adopts the Situational Crime Prevention (SCP) Theory. The SCP is a criminological approach that focuses on reducing the opportunities for crime by making it more difficult, risky, or less rewarding for offenders. Developed in the late 20th century, particularly by British criminologist Ronald V. Clarke, this theory is grounded in the idea that crime can be prevented by altering the immediate environment in which it occurs rather than solely focusing on offenders' motivations or social conditions (Clarke, 1997). The key assumptions of the SCP are crime is opportunistic, rational choice perspective, focus on specific crimes and not criminals, and environmental design matters (Clarke, 1997). The five main strategies of situational crime prevention are to increase the effort needed to commit a crime, increase the risks of being caught, reduce the rewards of crime, reduce provocations or triggers, and remove excuses for committing a crime.

While the theory was criticised for the following reasons: the displacement effect, limited focus on root causes, and overreliance on surveillance, it still remains relevant to crime prevention. Situational Crime Prevention is a practical, immediate, and often cost-effective method of reducing crime, especially in settings where long-term social reforms may be slow. In the context of the Nigeria Police Force, Situational Crime Prevention can be used to, among other things, Improve cybersecurity infrastructure to raise the effort and risk associated with committing cybercrimes, Introduce digital surveillance and data tracking systems to deter internet-based fraud and terrorism, Deploy public education campaigns to reduce the "excuses" or justifications often used by online scammers (e.g., blaming poverty or government failure) and Develop digital reporting channels that allow quick reporting and response to crimes, increasing the risk of detection for perpetrators. For Nigeria, especially in an era of increasing digital threats, SCP offers a valuable toolset for the Nigerian Police Force to adapt to contemporary security challenges.

METHODS

The study employed a qualitative research approach, drawing on both primary and secondary sources of data. The qualitative methodology becomes imperative in institutional researches as it helps unveil lived experiences of the actors which may not ordinarily be captured in quantitative methodology. Thus, Qualitative research creates an in-depth understanding of the attitudes, behaviours, interactions, events, and social processes that comprise everyday life which makes it sufficiently fit into the context of social researchers (Creswell, 2007; Lune & Berg, 2017; Muzari, Shava, & Shonhiwa, 2022; Oranga, & Matere, 2023) Primary data were obtained through Key Informant Interviews (KIIs) and In-Depth Interviews (IDIs). The KIIs were conducted with members of the Nigeria Police Force in Southwest Nigeria, while the IDIs involved members of the public, including university lecturers, IT professionals, and civil servants. Participants were purposively selected based on three main criteria: geographic spread across the southwestern states, relevant experience, and willingness to participate. Language for the interview was in both English and pidgin depending on the one that is convenient for the interviewees or respondents.

A total of 19 participants were interviewed—12 KIIs and 7 IDIs. Interview questions were shared with participants in advance, and responses were collected via phone calls, WhatsApp calls, and voice notes. The guiding questions included: “What do you think are the obstacles facing the police in a digital age?” “In what ways has the government responded?” and “What are the implications of the police’s inability to combat 21st-century digital crime in the country?” Each interview lasted between 15 and 27 minutes, and informed consent was obtained from all participants. For data confidentiality, they were assured that their names would be coded as (KII and IDI) without exposing their identities.

Secondary data were used to support and enrich the primary findings. These included books, academic journals, and media reports. The collected data were analysed using content analysis and are presented thematically in a descriptive narrative format.

RESULTS

Obstacles of the Nigeria Police Force (NPF) in Addressing Digital Crimes

i. Traditional Policing vs. Modern Threats

There is a growing disconnect between traditional policing methods and modern security threats. Many serving officers in the Nigeria Police Force remain anchored in outdated policing models that are ill-suited to the complexities of 21st-century crime. As one KII said

> Since the colonial government left and the new Nigerian elite has taken over, much has not been done to remove the mentality or orientation of the police from prevention to arrest. The police today still believe in arresting and prosecution rather than preventive. They want to order obeisance rather than become friendly. All these is affecting our way of fighting crime (KII. Inspector, Abeokuta. 12.5.2025.

> Another was of the view that the police today have not purged themselves from manual to digital. That is why you see them asking youths to open their phones, and when they see a white man, white woman, or anything foreign or which they lack knowledge of, they quickly tag the person Yahoo boy or criminal (IDI, tech industry, male, Lagos, 11.5.2025).

ii. Lack of Digital Infrastructure/ equipment and Institutional decay

A respondent narrated how they are even taught some skills in the police college but that the equipment is not sophisticated to combat modern crimes. He went further to state that the computers and the rooms are not modern and there are not many to go around as each personnel is not entitled to a computer (KII. Police sergeant. Lagos command. 12.5.2025). Another puts it this way:

Our stations and commands do not have modern equipment for detecting and preventing digital crimes, such as lie detectors, DNA testing, etc. Even to track phones, we don’t have as we either go to Lagos or Abuja or a few stations or commands. This is something that should be available at all stations in Nigeria, from rural areas to cities (KII, Superintendent of Police, Osogbo, 28/5/2025).

One respondent observed that the Nigeria Police Force is grappling with numerous challenges, primarily stemming from institutional decay. He explained that this decay affects critical aspects such as recruitment, training, promotions, conditions of service, welfare, and other associated benefits (KII. Inspector. Ibadan. 14.5.2025).

Another respondent said this digital infrastructure or equipment is not produced in Nigeria, and since they are expensive, it is always a big change to get them cheap; thus, the Nigeria government only appropriates very small amount for this, and even if they appropriate big money, these monies are insufficient as a result of the unequal exchange rate (KII. Sergeant Major. Ekiti State Command. 1.6.2025).

iii. Lack of adequate training and inclusiveness

A respondent narrated how shabby or haphazard the training can be in police college and that even if one is now out of police college, one may need to seek permission to go for further studies and that is if your superior allows you. He furthered that in a system where training and re-training are allowed, staff may want to take such programs and get reimbursed back, but where this is not so, it may be hard for personnel to go for such training (KII, Deputy Superintendent of Police, state command, Abeokuta. Similarly, another respondent said:

> The Nigeria Police Force is increasingly perceived as ineffective due to the government's lack of tangible commitment to training and capacity building. Although there is frequent rhetoric about training and re-training, little is done in practice. Funding for training is grossly inadequate, and allocations for ICT-related capacity building are virtually non-existent. This

> raises critical concerns about how officers are expected to grow professionally or effectively prevent and respond to emerging digital crimes (IDI. Tech entrepreneur. Lagos. 1.6.2025).

Another stated that apart from lack of adequate training, there is ethnicity and religiosity in the selection of trainees or prospective candidates to be trained and that at times, they can select police officers based on relationship, nepotism, ethnicity, religion and other features and not on merit or competence or zeal (KII, Asst. Superintendent of Police, Ibadan, 2.6.2025).

Another respondent noted that women are underrepresented in the Force and are often excluded from key training opportunities, which hinders their career advancement and progression within the ranks (KII, DSP. Lagos. Female. 2.6.2025).

iv. Recruitment Process and Level of Education

One of the respondents noted that the calibre of people recruited in the Nigeria Police Force, as well as their level of education and exposure, may also affect how they embrace or rebuke digital literacy so as to combat 21st-century digital crime. In his words, as reported in Pidgin language:

> No be say our men no gallant, but most of the recruitment wey government dey do these days na based on man-know man so majority no sabi write, read or even use internet. Some of our men self no like anything internet and because some of them local, they no one sabi am (KII. Sergent. Ibadan Police command. 10.6.2025).

It is not that our officers lack courage or dedication, but recent recruitment exercises by the government have often been influenced by patronage and clientelism. As a result, some individuals without adequate educational or professional qualifications have found their way into the Nigeria Police Force. Additionally, a number of officers exhibit resistance to digital innovation and institutional reforms, making it difficult for the Force to fully adapt to modern policing standards

A retired officer who now lectures said it is hard for many police officers because the recruitment is bad, porous and shallow and again, the so-called minimum requirement is usually forged by a few while the ones who do not even forge theirs are still living in the past as a result of culture (IDI. Retired ASP. Lecturer, Lagos. 5.6.2025).

vi. Poor funding and Lack of political will

A respondent noted that the obstacle to improving the lot of the NPF in terms of digital know-how is also linked to the lack of commitment or political will from the government as they prefer to allocate millions of dollars so as to corruptly enrich themselves. The lack of commitment also plays out in terms of the appointment of the police inspector general (IGP). He went further to state that poor funding, which is sometimes deliberate in order not to make the police effective, traces its roots to the military era, where the military thought that improving the police may bring them stronger than every other force in the country, including it (IDI. University lecturer. Akure.

2.6.2025). Another KII noted that the money allocated to the NPF is still very small compared to other law enforcement agencies and this affects the integration of digital literacy in fighting modern crimes (KII. The Asst. Superintendent of Police. Ibadan. 3.6.2025).

vii. Poor or lack of legal framework

There is also a lack of legal framework as a result of the archaic and unequal laws in the land. A respondent noted that the law applicable in the North is a penal code based on Islamic traditions, while the South uses criminal law based on Western tradition, which affects the way cases of digital crime are addressed in the courts of laws on both sides of the country. He furthered that, at times, the use of forensic evidence is lacking in so many cases, which, in the end, makes a mockery of the efforts of the police and other prosecutors (KII. Lawyer. Lagos. 11.6.2025). Another respondent held that, "the law makers across the sates of the federation must make laws to ensure that digital evidences are collected and admissible in the court of law if not, many cases will remain unresolved or inconclusive. He further gave instances of many alleged suspects such as an Abuja big boy who has been going in and out of EFCC custody, citing one Ismaila Mustapha, also known as Mompha, was arrested by the Economic and Financial Crimes Commission (EFCC) on allegations of money laundering and cyber fraud but that the cases have been there since 2019 (IDI. Civil servant. Ekiti. 20.5.2025).

viii. Indiscipline and Corruption

A respondent also said one of the problems is indiscipline and corruption because even when some officers can operate within the digital space, they will still prefer to take advantage of civilians and the public in order to make more illegitimate money despite their increase in pay by successive governments (IDI, lecturer. Abeokuta. 5.6.2025). Another stated that the country needs disciplined police officers and men of integrity and that until this is done, then the challenge will continue.

Government Responses and Hindrances

i. Creation of an ICT department

The Nigerian government is actively investing in Information and Communication Technology (ICT) training for the Nigeria Police Force (NPF) to enhance operational efficiency and improve service delivery. This includes equipping officers with digital literacy skills and tools, such as GPS and GIS, to track crime, respond to emergencies, and manage resources effectively. Even the Nigeria Police Force acknowledged this as it stated,

> As it is known globally, technology plays a significant role in modern law enforcement to enhance the efficiency and effectiveness of the agencies. Thus, modern law enforcement agencies must have the capability to manage electronic databases and communication systems as global crime has become more sophisticated (NPF, 2024b).

The department also has different sections. This includes Force Communication, INFOTECH Section from 'F' Department, Police Computer College, Abeokuta, 'F' Department, Communications Training Schools in Kaduna & Ikeja, Police Biometric Central Motor Registry (BCMR) from 'B' Department, Automatic Fingerprint Identification System from 'D' Department and Tracking & Intercepting Device Unit from 'D' Department. The objectives of the department are not limited to:

i. To develop an ICT Policy for the Nigeria Police Force in line with National ICT Policies, such as policies on procurement, use, and maintenance of ICT equipment
ii. To develop and empower the Nigeria Police personnel with ICT skills for operation efficiency and improved service delivery
iii. To provide tools that will help accomplish efficient modern policing.
iv. To introduce ICT innovative solutions centred on strategic policing that will facilitate public participation in policing
v. To develop a technologically driven Citizen and Law Enforcement Analysis and Reporting (CLEAR) program that is designed within the context of police-community-partnership for efficient and effective law enforcement
vi. To provide and maintain a system for data collection, input analysis, and necessary output
vii. To provide and maintain security for all levels of access and privilege to information systems and technology in all Police Formation
viii. To ensure that Nigeria Police acquire the best ICT equipment that complies with global law enforcement standards
ix. To evolve law enforcement technological solutions that will set the pace for other security agencies globally
x. To periodically conduct ICT-related need assessments and advise the Force accordingly (NPF, n.d. [b])

ii. Training of Officers

In 2023, Dr. Nasir Sani-Gwarzo, the Permanent Secretary of the Ministry of Police Affairs, called on senior officials at the directorate level to strengthen their skills in Information and Communication Technology (ICT), particularly in tools like PowerPoint and Excel, to enhance service delivery. Speaking at a capacity-building workshop at the Ministry's headquarters in Abuja—centred on boosting work efficiency through digital tools—Dr. Gwarzo highlighted the need for officers on Grade Levels 15 to 17 to gain hands-on experience with ICT applications. He noted that the training was intended to expose directors to various PowerPoint functions that can support project monitoring, evaluation, and day-to-day administrative duties. He stressed that consistent use of these digital tools would not only improve their productivity but also help them remain adaptable in an increasingly technology-driven work environment. Commenting further, Dr. Gwarzo stated that once current police reforms are fully implemented, operations would become more streamlined, adding that the Ministry remains committed to supporting the Nigeria Police Force and its medical unit in achieving optimal service outcomes.

> The worst thing we can do to ourselves as a nation is to assume that we cannot change the status quo ante, but the best thing to happen is not a

> journey to ultimate designation but the planning and setting the foundation stone of that journey. This is the best alignment I have seen in a long time; the President is ready, the Ministry and Nigeria Police Force are ready and all Nigerians believe that NPF is seriously understaffed/underserved however, if NPF is supported to an optimum level, Nigeria will be a better place to live in (Kazeem, 2023)

In April 2025, President Bola Ahmed Tinubu reaffirmed his administration's commitment to developing a Nigeria Police Force that is professionally trained, adequately motivated, and fully equipped with modern tools and technology to tackle crime effectively across the country. He announced that April 7 would henceforth be observed as National Police Day. The President, represented by Vice President Kashim Shettima, also pledged continuous training and retraining of police personnel, particularly in Information and Communication Technology (ICT), to enable them to respond effectively to emerging forms of crime. In his words:

> As President, I reaffirm this administration's steadfast dedication to the welfare and empowerment of the Nigeria Police Force. A secure Nigeria is vital for our collective prosperity, and this vision begins with ensuring that our police force is well-equipped, well-trained, and well-motivated. We are resolute in our commitment to police welfare and comprehensive reform. To that end, let me assure you that the Federal Government of Nigeria will institutionalise 7th April as an annual celebration of National Police Day, cementing its place in our national calendar and demonstrating our enduring appreciation for the Nigeria Police Force (Nkwocha, 2025)

The Inspector General of Police (IGP), Kayode Egbetokun stated that the occasion serves as an opportunity to reaffirm the commitment to excellence, professionalism, and the protection of human rights core values guiding the redefined identity of the Nigeria Police Force. He outlined his administration's reform agenda, emphasizing efforts to build a trustworthy and professional police institution dedicated to justice and contributing to national development through improved security and law enforcement.

Highlights of the event included the Vice President's inspection of the guard, a ceremonial parade by tactical units and other security agencies, as well as a silent drill performance by officers of the Nigeria Police Force.

iii. Partnering with sister and foreign agencies

In 2016, The Zone 2 Police Command, Onikan, Lagos, partnered with stakeholders in Information and Communication Technology (ICT) to enhance police officer's use of technology in combating crime in the zone. The then Assistant-Inspector General of Police (AIG), Mr Bala Hassan, made the assertion at the flag-off of "On the Need to be ICT Compliant'' at the Zonal Headquarters. The AIG, represented by a Deputy Commissioner of Police in the zone, Isaac Akinboyede, added that the use of ICT would improve the ways the officers were tackling criminal investigations. In his words:

> I am aware that they have organised similar training in this zone for officers, now we are here because our partners want to give us a proper insight into the ICT world. We know that the world is growing in ICT, and everything is growing with it; what we used to do 10 to 15 years ago is different from what we have now in terms of ICT. The Nigeria Police cannot afford to be left behind in the society (The Government Business Journal, 2016).

Contributing, the Zonal Police Public Relations Officer, CSP Adebowale Lawal, said that the development would enhance the operational activities of the officers and men. Lawal emphasised the importance of keeping police personnel informed about global advancements in technology, particularly in the area of investigation. He noted that international partners frequently assist in training officers in ICT-related skills and stressed the need for continued collaboration with such stakeholders. Highlighting ongoing efforts, he pointed to the establishment of an ICT College in Kobape, along the Sagamu Road in Ogun State, where officers are being trained to ensure they are not left behind in the digital era. According to him, the goal is to promote technological adoption within the Force at an affordable cost. He added that this initiative would not be limited to Ogun but would be extended to other police commands and zones across the country (The Government Business Journal, 2016).

In 2024, the government also trained senior civil servants, including police officers. The Federal Government, in collaboration with Huawei Technologies Company Nigeria Limited, has trained 100 Federal Civil Servants at the directorate level on Information and Communication Technology (ICT) under its ICT for Change Training programme and awarded prizes to outstanding participants. While presenting prizes to 16 outstanding participants at the closing ceremony of the fourth phase of ICT for Change programme, the Secretary to the Government of the Federation, Sen. George Akume, CON thanked the Company for training more than 3,000 civil servants from different Ministries, Departments and Agencies (MDAs) on ICT since the commencement of the collaboration. Speaking on behalf of the awardees, the Director ICT in the Federal Ministry of Science, Technology and Innovation, Adebayo Adeyemi, expressed gratitude to the Federal Government and Huawei Technologies for their collaborative efforts in building the capacity of Civil servants in ICT, which have helped to broaden their horizons on e-governance and other relevant subjects. He assured that the knowledge they acquired during the training would be harnessed in discharging their duties (Imohiosen, 2024).

Despite these initiatives or responses, several challenges persist. These are largely rooted in Nigeria's digital divide, which impacts the Nigeria Police Force (NPF) just as much as it affects the general population. The NPF grapples with issues such as inadequate data systems and lack of digitised records, insufficient forensic and cybercrime laboratories, limited ICT training and awareness among officers, systemic corruption, weak institutions and institutional decay, manpower shortages, and poor inter-agency data-sharing mechanisms.

Implications for National Security

The growing digital crime has significant implications for national security. First, it leads to increased vulnerability to digital threats. The inability of the Nigeria Police Force (NPF) to effectively counteract cybercrime, online fraud, and other digital offences emboldens both domestic and transnational criminal networks. This not only undermines investor confidence, especially in key sectors like fintech, telecommunications, and e-commerce, but also erodes public trust in state institutions. As digital threats evolve in complexity, the lack of adequate training, personnel, and digital infrastructure within the NPF hampers swift detection and response. Additionally, the proliferation of online black markets, identity theft, phishing schemes, and politically motivated cyberattacks further exposes national systems, including banking, communication, electoral processes, and critical infrastructure, to exploitation. In the long term, such unchecked digital vulnerabilities can destabilise governance, deepen insecurity, and create fertile ground for terrorism, misinformation, and organised crime.

Second, it leads to the rise of alternative security actors. The persistent inefficiency and incapacity of the Nigeria Police Force in addressing digital and conventional crimes have created a security vacuum. This has prompted the emergence of non-state security actors such as vigilante groups, ethnic militias, and even online hacktivist networks who step in to fill the gap. While some of these actors may initially provide localised or community-based protection, their operations are often unregulated, lack accountability, and may operate outside the bounds of the law. In many cases, they exacerbate insecurity by engaging in human rights abuses, extortion, or pursuing ethnic and political agendas, thereby undermining state authority and contributing to a fragmented and unstable security landscape.

Also, it erodes trust and civic cooperation. Public distrust in the Nigeria Police Force significantly diminishes citizen willingness to report crimes, share intelligence, or collaborate with law enforcement. In an era where effective policing increasingly depends on community partnerships, crowdsourced information, and digital surveillance cooperation, this lack of trust weakens the very foundation of modern security practice. When people view the police as corrupt, incompetent, or disconnected from their concerns, they are less likely to engage in proactive crime prevention efforts, thereby hampering early detection and response to both physical and digital threats.

Ultimately, it has a negative impact on global perception and exacerbates regional threats. Nigeria’s persistent inability to effectively police its cyberspace undermines its international image as a secure and stable state. This perceived weakness in cybersecurity governance diminishes foreign confidence in Nigeria’s digital economy, discourages foreign investment, and raises concerns among international partners. Moreover, the country's porous digital space creates a safe haven for transnational criminal networks involved in human trafficking, money laundering, drug smuggling, and online terrorism. These threats often spill across borders, posing significant security challenges not only to Nigeria but also to the broader West African sub-region. Inadequate digital policing capacity, therefore, makes Nigeria both a target and a conduit for cyber-enabled crimes with global implications.

DISCUSSION OF FINDINGS

Findings show obstacles to include traditional policing vs. modern threats, lack of digital infrastructure/ equipment and institutional decay, lack of adequate training and inclusiveness, poor recruitment process and level of education, poor funding and lack of political will, poor or lack of legal framework, indiscipline and corruption. With limited exposure to digital technologies and minimal training in cybercrime detection, data analysis, and surveillance tools, officers are often ill-equipped to confront evolving threats such as internet fraud, cyberstalking, digital financial crimes, and online radicalisation. This gap in knowledge and skills has become a critical challenge as the Force struggles to adapt its strategies, tools, and operational frameworks to the demands of the digital age. Without a deliberate and sustained investment in modern training and technological integration, the NPF risks becoming obsolete in the face of rapidly advancing criminal networks. This is in line with Ismail and Abdullahi (2023) who affirmed the poor exposure to NPF members in Jigawa state.

The second finding shows that the government has responded in various ways, from creating a department in the NPF to training and retraining as well as partnering with other sister agencies. This is no doubt consistent with the Situational Crime Prevention (SCP) Theory which is a criminological approach that focuses on reducing the opportunities for crime by making it more difficult, risky, or less rewarding for offenders (Adeniji & Emekayi, 2022; Ismail & Abdullahi, 2023). However, it also shows that these interventions have been hindered by some other factors, such as corruption, systemic issues, etc. These appear to be the same issues confronting the NPF entirely (Osho, 2025a; 2025b).

The findings also show that the situation has heightened exposure to digital threats and contributed to the emergence of alternative security actors. It has also undermined public trust and reduced civic engagement. Additionally, it damages international reputation and intensifies regional security risks. The recent China Beijing Equity Exchange (CBEX) incident illustrates the shortcomings of digital crime prevention had the syndicate been intercepted earlier, it could have prevented significant financial losses and preserved investor confidence. This case reflects a broader pattern of government indifference toward addressing cybercrime effectively (Awolaja, 2025). Consequently, situational crime prevention becomes crucial (Clarke, 1997; Hayward, 2007).

Conclusion

The emergence of digital crime has fundamentally redefined the landscape of law enforcement, demanding agile, tech-savvy, and well-resourced policing institutions. In Nigeria, however, the Nigeria Police Force (NPF) remains constrained by deeply rooted institutional challenges, including poor digital infrastructure, outdated recruitment practices, low digital literacy among officers, inadequate training, and a general resistance to technological innovation. These challenges are further compounded by systemic corruption, poor funding, and a fragmented legal framework, all of which severely undermine the Force's capacity to combat 21st-century crimes.

Although commendable efforts have been made by the Nigerian government—including the establishment of ICT departments, training programs, and inter-agency collaborations—these initiatives have not yielded optimal results due to persistent structural and governance deficits. As a result, Nigeria remains vulnerable to digital crimes such as cyber fraud, digital scams, identity theft, and transnational online crimes. The erosion of public trust, rise of alternative security actors, and weakening of national and regional security underscore the urgent need for comprehensive reform. If Nigeria is to safeguard its digital future and ensure internal stability, reforming the NPF to meet modern demands must be treated as a national security priority.

The recommendations of the study are:

1 Comprehensive Digital Policing Reform

There is an urgent need for a holistic reform of the NPF that integrates digital crime-fighting strategies. This should include digitisation of records, development of forensic laboratories, deployment of crime-mapping technologies, and real-time data-sharing systems.

2. Merit-Based and Transparent Recruitment

Recruitment into the NPF must prioritise digital competence, education, and merit. Patronage-based recruitment should be phased out in favour of standardised and transparent entry processes that reflect the digital realities of modern policing.

3. Mandatory and Continuous Training

Training in ICT, cyber forensics, digital surveillance, and emerging tech tools must be made mandatory for both new and existing officers. Structured refresher courses and certifications should be incentivized and linked to career progression.

4. Legislative Overhaul and Harmonization

National and sub-national legislators must reform existing laws to support digital policing. This includes legal recognition and admissibility of digital evidence, harmonization of penal codes across regions, and development of robust cybersecurity laws.

5. Investment in Infrastructure and Welfare

The government must prioritize increased budgetary allocations for the procurement of advanced equipment and the modernization of police stations. This should be accompanied by improved welfare packages to reduce corruption and enhance motivation.

6. Gender and Inclusion Policy

Special efforts should be made to promote gender equity in training and leadership roles within the Force. Inclusion policies must address barriers faced by women and marginalized groups in digital policing careers.

7. Public-Private Partnerships (PPP)

Collaboration with private tech companies, cybersecurity firms, and academic institutions should be institutionalized to provide training, mentorship, and technological support to the police.

8. Community and Digital Engagement

Leveraging mobile apps and digital platforms for crime reporting, whistle-blowing, and feedback mechanisms can help rebuild trust between the public and the police. Efforts must be made to improve responsiveness and digital literacy among the populace.

9. Establishment of Oversight and Accountability Mechanisms

Independent digital crime oversight bodies should be established to monitor NPF activities, ensure accountability in the use of surveillance tools, and prevent abuse of citizens' digital rights.

REFERENCES

Adeniji, A.S and Emekayi, M (2022) Information Technology and Crime Detection and Fighting in Nigeria and India: A Comparative Analysis. *Journal of Global South Research on Security and Development* 1(1), 124-144

Ajayi, L. A., & Adebayo, O. R. (2020). Mobile Technology and Crime Reporting in Nigeria: Challenges and Prospects. *African Journal of Criminology and Justice Studies*, 13(1), 142–160.

Awolaja, A (2025, April 19). The government's CBEX hypocrisy. *Tribune*. https://tribuneonlineng.com/the-governments-cbex-hypocrisy/

Brey, P. (2017). Theorizing Technology and Its Role in Crime and Law Enforcement. In M. McGuire and T. Holt (Ed.), *The Routledge International Handbook of Technology, Crime and Justice* (pp. 17-34). New York: Routledge.

Casey, E. (Ed.) (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. USA: Academic Press.

Clarke, R. V. (1997) *Situational Crime Prevention Successful Case Studies*. New York: harrow and Heston

Creswell , J. W. (2007). *Qualitative Inquiry and Research Design: Choosing Among five designs*. London: Sage.

Egielewa, Peter Eshioke. 2022. "Yahooism or Internet Fraud in the Nigerian Higher Education System. *Journal of Ethics in Higher Education* 1: 75–101. DOI: 10.26034/fr.jehe.2022.3378

Garvie, C., Bedoya, A., & Frankle, J. (2016). The Perpetual Line-Up: Unregulated Police Face Recognition in America. Georgetown Law Center on Privacy & Technology.

Grabosky, P (1989) Technology & Crime Control. Technology & Crime Control No. 78: 1-6. https://www.aic.gov.au/sites/default/files/2020-05/tandi078.pdf

Imohiosen, S (2024, October 10). FG, HUAWEI TRAINS DIRECTORATE LEVEL OFFICERS ON ICT…Presents Awards to outstanding participants. Ministry of Defense. https://defence.gov.ng/2024/10/11/fg-huawei-trains-directorate-level-officers-on-ictpresents-awards-to-outstanding-participants/#:~:text=The%20Federal%20Government%20in%20collaboration,and%20welfare%20of%20its%20citizens.

Ismail, U., & Abdullahi, A. S. (2023). Digital policing in Nigeria: A study of Jigawa State Police Command. *International Journal of Police Science & Management*, 26(1), 67-77. https://doi.org/10.1177/14613557231198701

Isman, A (2012) Technology and Technique: An Educational Perspective. *TOJET: The Turkish Online Journal of Educational Technology*, 11(2), 207-213.

Keith Hayward, K (2007) Situational Crime Prevention and its Discontents: Rational Choice Theory versus the 'Culture of Now' Social Policy & Administration, Vol. 41(3), 232–250

Lum, K., & Isaac, W. (2016). To predict and serve? Significance, 13(5), 14–19.

Lune, H., & Berg, B. L. (2017). Qualitative Research Methods for the Social Science. Essex: Pearson Education Limited.

Muzari, T., Shava, G. N., & Shonhiwa, S. (2022). Qualitative Research Paradigm, a Key Research Design for Educational Researchers, Processes and A Theoretical Overview. Indiana Journal of Humanities and Social Sciences, 3(1), 14-20.

Nkwocha, S (2025, April 7) President Tinubu: We Will Engender Well-trained, Tech-driven, Modern Police Force. Press release, state House. https://statehouse.gov.ng/news/president-tinubu-we-will-engender-well-trained-tech-driven-modern-police-force/ accessed 12.6.2025

Nigeria Police Force. (2024). *History of the Nigeria Police Force*. https://www.npf.gov.ng/history/display

Nigeria Police Force. (2024). *Department of Information and Communication Technology*. https://www.npf.gov.ng/home/department/4

Ojedokun, U. A., & Eraye, C. M. (2012). Socioeconomic Lifestyles of the Yahoo-Boys: A Study of Perceptions of University Students in Nigeria. International Journal of Cyber Criminology, 6(2), 1001–1013.

Oranga, J. and Matere, A. (2023) Qualitative Research: Essence, Types and Advantages. Open Access Library Journal, 10: e11001. https://doi.org/10.4236/oalib.1111001

Osho, O. A (2025a) Has Anything Changed? Impact Of the Nigeria Police Force Act 2020 On Police Practices and Reforms. *IKR Journal of Arts, Humanities & Social Science (IKRJAHSS)*. Vol. 1 (1), 16-20. https://ikrpublishers.com/wp-content/uploads/2025/03/IKRJAHSS0225-2025.pdf

Osho, O. A (2025b) From Resource Control To Oil Theft: Evolving Crime In The Niger-Delta And The Nigeria Police Force's Role In Mitigation And Enforcement. Ochendo, Vol 6, (3): 1-13. https://acjol.org/index.php/ochendo/article/view/6681/6468

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. RAND Corporation.

Ristea, A., & Leitner, M. (2020). Urban Crime Mapping and Analysis Using GIS. *ISPRS International Journal of Geo-Information*, *9*(9), 511. https://doi.org/10.3390/ijgi9090511

The Government Business Journa (2016, June 22) Zone 2 Police Command trains officers in ICT. https://govbusinessjournal.com/zone-2-police-command-trains-officers-in-ict/

Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). Biometric Systems: Technology, Design and Performance Evaluation. Springer.

Welsh, B. C., & Farrington, D. P. (2009). Public area CCTV and crime prevention: An updated systematic review and meta-analysis. Justice Quarterly, 26(4), 716–745.

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. Public Affairs.