THE ROLE OF LAW ENFORCEMENT AGENCIES IN COMBATING CYBERCRIME IN NIGERIA

Majebi Samuel Amune*

Abstract

Cybercrime has become a major threat to Nigeria's security and economic stability, with crimes such as internet fraud, identity theft, and ransomware increasingly undermining public trust in digital platforms. Although Nigeria enacted the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and related statutes to address these challenges, cybercriminals continue to exploit technological loopholes and jurisdictional gaps. This paper examines the role of law enforcement agencies in combating cybercrime in Nigeria, with emphasis on their mandates, strategies, achievements, and constraints. The study identifies the core problem as the widening gap between the improvements on cybercriminal activities and the limited technical, legal, and institutional capacity of Nigerian law enforcement agencies. Despite the involvement of key institutions such as the Economic and Financial Crimes Commission (EFCC), Nigeria Police Force (NPF), National Information Technology Development Agency (NITDA), and the Office of the National Security Adviser (ONSA), enforcement remains hampered by inadequate funding, insufficient manpower, slow judicial processes, and weak inter-agency coordination. Adopting a doctrinal research methodology, the study relies on statutory provisions, judicial decisions, and scholarly works to evaluate the effectiveness of Nigeria's legal and institutional response to cybercrime. Findings reveal notable successes, including high-profile arrests, asset recovery, and collaborative operations with international bodies such as INTERPOL and the FBI, but these remain insufficient given the scale of cyber threats. The paper recommends targeted capacity building, legislative reforms, stronger international cooperation, increased funding, and public-private partnerships to enhance Nigeria's cyber resilience. It concludes that a unified, proactive, and technology-driven national strategy is essential for securing Nigeria's cyberspace and protecting its digital economy.

Keywords: Cybercrime, Cybersecurity, Digital Economy, Law Enforcement, Tax Compliance

1.0 Introduction

As time evolves, technology advances, and the urges to commit crimes increase. As time goes by, different walks of life have decided to employ the use of technology – finance, commerce, entertainment, and even in governance. This, therefore, comes with a price - cybercrime. Although advancing in accompaniment with technology is a digital crime, which is identified as

LL.B. (University of Benin); LL.M., M.Phil., Ph.D (Obafemi Awolowo University) Senior Lecturer, College of Law, Joseph Ayo Babalola University, Ilesa, Osun State, Nigeria & Principal Partner, LawDigital Consult. Email: noble heirs@yahoo.com Tel: 08033724459

cybercrime. Cybercrime involves the use of computer networks and the internet to target a particular computer network or system as to gain unauthorized access in order to result to causing harm to the targeted network. Cybercrime goes deep into committing fraud, trafficking in child pornography and intellectual property, stealing identities, violating privacy, and many more.[1] The extent to which cybercrime reaches is not limited to any physical boundaries. The crime itself, the perpetrators, who are the cybercriminals, the victims of the crimes, and the technological tools used in committing the crime span across different jurisdictions. Through the use of technology in exploiting technological vulnerabilities on both a personal and an enterprise level, cybercrime continues to evolve in line with the advancements of technology. This, in consequence, has caused the ability to effectively investigate, prosecute, and prevent cyber-crimes to be an ever-trending fight posing many dynamic challenges. [2]

2.0 Types of Cybercrimes

Phishing: This is usually the most common type of cybercrime. In a phishing attack, cybercriminals imitate and impersonate legitimate organizations, which could include banks or government offices, via email, text, or phone calls, in order to persuade and trick individuals into sharing sensitive information. The sensitive information includes login credentials or financial details, which can then lead to identity theft and financial losses for the victims. Business Email Compromise (BEC) is a more targeted form of phishing where cybercriminals manipulate organization employees into making fraudulent transactions which could result in financial losses for the organization.[3]

Ransomware Attacks: it is a type of cyber threats that involves the attacker encrypting the victim's files and demands payment which is a ransom in exchange for regaining access back to the encrypted files. These attacks can paralyze entire organizations, from hospitals to financial institutions, and result in significant financial damage. There are many types of ransomware attack vectors, such as email attachments, website pop-ups, or text messages.

[1] Michael Aaron Dennis. "Cybercrime". Available at https://www.britannica.com/topic/cybercrime accessed on 2nd August, 2025.
[2] What Is Cyber Crime? Available at < https://www.proofpoint.com/au/threat-reference/cyber-crime> accessed on 2nd August, 2025.
[3] Bitsight Research Team. "Types of Cyber Crimes". Available at < https://www.bitsight.com/learn/cti/types-of-cyber-crimes> accessed on 2nd August, 2025.

Identify Theft: Identity theft happens when someone uses the personal information of a victim without the victim's permission. Information like Social Security number, bank account number, and credit card information are used to gain financial benefits or commit fraud. Thieves can use your information to access personal accounts, open up new accounts without the owner's permission, make unauthorized transactions, or commit crimes. [4]

3.0 Overview of Cybercrime in Nigeria

Due to the increasing need for Nigeria to accept the adoption of the use of technology in her system, although, this has caused an increase in social and economic opportunities, however, it does not go without saying that, the use of technology, coupled with vulnerabilities of Nigerians, the economic state in the country, and low level of exposure of Nigerians to the use of technology has served as a cause in increasing the rate of cyber related crimes like mail scams, identity theft, cryptocurrency fraud in Nigeria among many others.[5] While the use of technology may promote efficiency, increase productivity, and enhance workflows, a little glitch may cause a whole system draw-down for an individual, organization, or even a nation at large, resulting in loss of information, data, or even result in huge financial losses. The estimated annual financial loss in Nigeria due to cybercrime was N250 billion ($649 million) in 2017 and N288 billion ($800 million) in 2018. [6]

3.1 Causes of Cybercrimes

Several factors like unemployment, the quest for wealth, a lack of strong cybercrime laws, and incompetent security on personal devices amongst others – have combined to make cybercrime a significant problem for the country. These factors have through certain ways served as the drive pushing criminals to engage in the fraudulent acts.

A. Financial Gain

Usually, the foremost reason why cybercriminals engage in the act is for financial gains. Many cybercriminals find themselves convinced through the potential financial rewards that comes with it. They may decide to engage in stealing sensitive financial information, conduct ransomware

[4] Ali Hussain, Marguerita Cheng, Vikki Velasquez. "What Is Identity Theft? Types and Examples" available at https://www.investopedia.com/terms/i/identitytheft.asp accessed on 2nd August, 2025.
[5] Edward Olalekan and Mariam Yusuff. "The Evolution of Cybercrime in Nigeria: Trends and Countermeasures" available at https://www.researchgate.net/publication/388634325_The_Evolution_of_Cybercrime_in_Nigeria Trends __ and_Countermeasures accessed on 2nd August, 2025.
[6] Proshare. "*Cybercrime in Nigeria: Causes and Effects*". Available at https://proshare.co/articles/cybercrime-in-nigeria-causes-and-effects accessed on 2nd August, 2025.

attacks, or engage in fraud schemes to make money from victims, or through the information sold out to a third party. [7]

B. Parental Pressure

ometimes, the high expectations from parents cause youth to turn to cybercrime in order to meet up with expectations and achieve the expected success. This happens so, because while under intense pressure from parents, youths often find themselves stuck between the hard place of decision-making and challenging situations. Also, on the flip side, parents, whose duty it is, to discourage their children from engaging in crime, conversely facilitate, encourage and conceal their wards cybercriminal activities. [8]

C. Complexity of Code

The well-functioning of computer being dependent majorly on operating systems, in which operating system depends highly on code. Since codes are constructed by human, it makes it highly subjected to errors. The errors in these codes may be taken lightly by the user or even the manufacturer, and these may serve as loopholes for cybercriminals to exploit and gain access to information on such computer. [9]

D. **Negligence**

Human being are prone to neglecting things, which may even include things related to personal information. Negligence of the user may serve as a costly mistake which cyber criminals may take advantage of, in gaining access to exploit the victims. [10]

4.0 Legal Framework for Cybercrime in Nigeria

A. Cybercrimes (Prevention, Prohibition, etc.) Act 2015

Nigeria embarked on a crucial and important in combating cybercrimes by dedicating an act for it. The primary enactment for combating cybercrimes in Nigeria is the Cybercrimes (prevention, prohibition, etc) Act 2015 which was passed into law in May 2015 by the Nigerian National Assembly, under the President Muhammadu Buhari's administration, making the act serve as the first, and still the major enactment for regulating online activities of persons in the cyber space.

[7] Nusaiba Ibrahim. "Cybercrime: Understanding its Nature, Causes, and Effects" available at https://sun.edu.ng/5 838-2/ accessed on 2nd August, 2025.
[8] Ibid
[9] GeeksforGeeks "Cybercrime Causes and Measures to Prevent them" available at https://www.geeksforgeeks.org/ethical-hacking/cybercrime-causes-and-measures-to-prevent-it/ accessed on 2nd August, 2025.
[10] Ibid

[11]In the Act, there are 59 sections, 8 Parts and two schedules. The First Schedule of the Act provides for members of the Cybercrime Advisory Council while the Second Schedule on the other hand provides for businesses to be levied for the purpose of cyber-security Fund.

The Act provides an effective, and well-detailed comprehensive legal regulatory framework for prohibiting, preventing, prosecuting and punishing cyber related crimes, and cyber criminals in Nigeria. In addition to that, the act also protects guards infrastructure which are key to national information, and promotes cybersecurity and the protection of computer systems and networks, electronic communications, data and computer program, intellectual property and privacy rights.[12] The Act serves as a legislative response to cybercrimes for which there had not been a specific act covering the area, considering the advancement of technology. The Act therefore serves to prevent crimes like *Identity theft and impersonation,[13] Child pornography and related offences,[14] Cyberstalking,[15] Cybersquatting,[16] Racist and xenophobic offences,[17] Attempt, conspiracy, aiding and abetting,[18] Importation and fabrication of e-tools,[19] Breach of confidence by service providers,[20] Manipulation of ATM/POS Terminals[21] and many more related cybercrimes.* With the Act providing punishments like monetary fines, imprisonment terms as provided by the Act. However, prior to the enactment of the act, there had been an act covering the area of fee fraud in Nigeria. The Advance Fee Fraud and other related Offences Act, 2006, the Economic and Financial Crimes Commission (EFCC) Act, 2004 and the Money Laundering Act, 2012 regulated cybercrimes in Nigeria. The inadequacy of these legislations became a major reason why the Cybercrimes (Prohibition, Prevention, etc) Act, 2015 was made. In the case of *Harrison Odiawa (alias Abu Belgore) v. Federal Republic of Nigeria*,**[22]** Between March 2003 and January 2004, Odiawa and his syndicate used deceptive emails and forged documents to convince Mr. Blick to

[11]Olanrewaju Adesola Onadeko, Abraham Femi Afolayan. "A Critical Appraisal of the Cybercrimes Act, 2015 in Nigeria". Available at https://www.isrcl.com/wp-content/uploads/2021/05/Onadeko-Afolaya-A-critical-appraisal-of-the-cybercrimes-act-in-Nigeria.pdf accessed on 2nd August, 2025.
[12] Cybercrimes (prevention, prohibition, etc) Act 2015
[13] *Ibid* Section 22.
[14] *Ibid* Section 23.
[15] *Ibid* Section 24.
[16] *Ibid* Section 25.
[17] *Ibid* Section 26.
[18] *Ibid* Section 27.
[19] *Ibid* Section 28.
[20] *Ibid* Section 29.
[21] *Ibid* Section 30.
[22] [2008] 57 WRN 83

transfer funds under the guise of a lucrative business opportunity. Following a report to the Economic and Financial Crimes Commission (EFCC), an investigation led authorities to Odiawa's cybercafe, where evidence was recovered, including documents and a mobile phone used for communication with the victim. The offenders were tried under the Advance Fee Fraud and Other Related Offences Act, 2006. The first defendant was sentenced to twelve years imprisonment on each of the four counts without an option of fine while the second defendant was sentenced to ten years imprisonment on each of the three counts without an option of fine. That is to serve an indication that prior to the Cybercrime Act, 2015, Nigeria had legislation in place, although inadequate to cover wise range of cyber activities.

5.0 Other Related Acts

A. The Constitution

Although the *Cybercrimes (Prevention, Prohibition, etc) Act 2015* identifies as the primary statutory authority serving as the backbone to cybercrimes in Nigeria, the 1999 Constitution of the Federal Republic of Nigeria, 1999, however is not ruled out to address these cyber threats. The Constitution, although not intended to cover these parts in its making, however serves to prevent these crimes by guaranteeing and securing the right to privacy of Nigerians, their telephone calls, and so on. Consequently, when law enforcement authorities require information from a person's cell phone, e-mail, or other electronic devices as part of a telecom service provider investigation into cybercrime, the Nigerian Constitutional right to privacy must be taken into account. In *Independent Television/Radio v. Edo State Board of Internal Revenue*, the Court of Appeal held that "by virtue of the provisions of sections 37, 43 And 44(1), (a) and (b) of the Constitution of the Federal Republic of Nigeria, 1999, the privacy of citizens, their homes, correspondence, telegraphic communication is guaranteed and protected." [23] Also, the Supreme Court in *Ransome Kuti v. Attorney General of the Federation* held that "A Fundamental Right is a right that stands above the ordinary laws of the land and which is antecedent to the political society itself. It is a primary condition for a civilized existence." [24] Flowing from the above, it is no gainsaying that the Nigerian Constitution protects people from unnecessary searches and seizures by law enforcement agencies. It also enjoins officers to obtain a search warrant before accessing a place where a person is guaranteed to have a reasonable degree of privacy. Computers, records, and/or information on

[23] (2015) 12 NWLR (Pt. 1474) 442
[24] (1985) 2 NWLR (Pt. 6) 211

individual computers are covered by the Nigerian Constitution from searches by law enforcement agents. [25]

B. International treaties and obligations (e.g., Budapest Convention)

Domestic or national laws are the domestic law within a city or a country, which is binding on all forces within such state. [26] National laws, however, do not have force outside the territory where they are enacted. Due to the increasingly growth of cybercrimes, this results in the need for an international instrument that would be binding on states that are signatory to it, and have it ratified as their local laws. This then could be seen as a rationale behind the Council of Europe Convention on Cybercrime.[27] The convention, famously referred to as the Budapest Convention, is a collective response by members of the European Union and non member states in guarding and combatting against the spread of cybercrimes. The Convention is the first binding multinational treaty to comprehensively address cybercrime, and it has had a profound impact on the international anti-cybercrime legislation.[28] Since been open for signature in November 2001, twenty-four years later, it still remains the most relevant international agreement on cybercrime and electronic evidence. Since then, they have also made them highly vulnerable to security risks such as cybercrime, mis- and disinformation, foreign influence and more. While there is recognition of the need to strengthen security, confidence and trust in ICT and to reinforce the rule of law and the protection of human rights in cyberspace, all things "cyber" have become more important as they touch upon the fundamental rights of individuals as well as the national security interests of states.

C. Major Law Enforcement Agencies Involved

Due to the rapid surge in cybercrimes, it has become a necessity to create more agencies in combating cybercrimes. This then has served for many jurisdictions to create dedicated enforcement agencies in tackling cyber related crimes.

---

[25] The Editorial Board, Wigwe and Partners. *The Legal Framework For Cyber Crimes In Nigeria.* Available at https://wigweandpartners.com/the-legal-framework-for-cyber-crimes-in-nigeria/ accessed on 2nd August, 2025.

[26] Susan Buckner, J.D. Melissa Bender, Esq. "*What Is Municipal Law?".* Available at https://www.findlaw.com/hirealawyer/choosing-the-right-lawyer/municipal-law.html accessed on 2nd August, 2025.

[27] CoE, Convention on Cybercrime – ETS No. 185 (2001).

[28] Dr. Chat Le Nguyen, Dr. Wilfred Golman. "*Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action*'. " available at https://www.sciencedirect.com/science/article/abs/pii/S0267364920301266#:~:text=The%20Budapest%20Convention%20as%20a,The%20Council%20of accessed on 2nd August, 2025.

D. The Federal Bureau of Investigation

Established in 2002, the Federal Bureau of Investigation is the lead domestic intelligence service and a leading federal agency engaged in combating cyberattacks by criminals both in the United States and the international sphere.[29] The FBI through different means, gather intelligence, disrupt malicious cyber activity, identify perpetrators, and then declare costs on adversaries. The FBI fosters this team approach through unique organizations where different sectors come to establish a long-term trusted relationships to fight the spread of cybercrime. [30]

E. The Nigeria Police Force

Nigeria Police Force – National Cybercrime Centre (NPF-NCCC), a subsidiary of the general law enforcement agency, the Nigeria Police Force in Nigeria, serves as a premier and leading body in fights against different forms of cyber related offenses in Nigeri. The NPF-NCCC investigates cybercrimes, analyzes digital evidence, coordinates national cybersecurity policies, and enlightens the public in order to protect citizens from online criminal activities. The Centre makes use of advanced forensic tools and comprises of detectives who are well versed, and have strong IT backgrounds. [31]

The NPF-NCCC is recognized as a leading body in fights against cybercrimes, not just through proclamations, but with the involvement of actions, in which the force recorded an impressive achievement in the year 2024 in combating cybercrimes. In 2024, the Nigeria Police Force National Cybercrime Center (NPF-NCCC) successfully recovered a staggering N8,821,001, 881. 80 (Eight Billion, Eight Hundred and Twenty-One Million, One Thousand, Eight Hundred and Eighty-One Naira, Eighty Kobo), 115,237.91 USDT, and $84,000 (Eighty-Four Thousand Dollars). In which the amounts were restituted to the victims in order to ensure justice to the victims of the fraudulent activities.[32] Also, similarly in the past year, the Cybercrime Unit has actively engaged in strategic operations, resulting in the arrests and prosecutions of over 751 individuals involved in cybercrime. The unit has successfully recovered a total of 685 devices that were used in these nefarious activities, which include 467 mobile phones, 137 laptops and computers, 46 routers, 4 servers, 1 drone, and 4 Starlink devices. Additionally, the operations led

[29] FBI. "What We Investigate". Available at https://www.fbi.gov/investigate/cyber accessed on 16th August, 2025.
[30] Ibid
[31] The NPF. Available at https://nccc.npf.gov.ng/?utm accessed on 16th August, 2025.
[32] https://x.com/PoliceNG/status/1876666816832938407?t=Q6hr-iOCrUggKwwPGG_WGQ&s=19

to the confiscation of 16 houses, 39 plots of land, 14 land documents, and 26 vehicles, further dismantling the infrastructure supporting cybercriminal activities.[33] These efforts further have been recognized as the NPF-NCCC was awarded the title of the Best Cybercrime Unit in Africa for 2024 by the INTERPOL Cybercrime Directorate based in Singapore, securing the top position among 54 participating African countries. [34]

F. The Economic Financial Crime Commission

Economic and Financial Crimes Commission, popularly regarded as the EFCC, is a body responsible for investigating and prosecuting economic and financial crimes activities generally in Nigeria. The EFCC, primarily established to go after different forms of deceptions for financial gains, has extended its scope into going after cyber-enabled fraud and internet scams. EFCC also works on legislative reforms, fraud detection, and public enlightenment campaigns to combat cybercrime. [35] With the determination of the EFCC in combating cybercrimes in Nigeria can be seen as a major justification for introducing a 24-hour Cybercrime Rapid Response Desk on Tuesday, October 22, 2024 which was meant to provide both local and international telephone numbers in reaching the body anywhere across the globe.[36]

The EFCC, through their rigorous fights against cyber related crimes through October 2023, and September 2024, secured 3455 convictions and made monetary recoveries of N 248,750,049,365.52 (Two Hundred and Forty-Eight Billion, Seven Hundred and Fifty Million, Forty-Nine Thousand, Three Hundred and Sixty-Five Naira, Fifty-Two Kobo); $105,423,190.39 (One Hundred and Five Million, Four Hundred and Twenty-Three Thousand, One Hundred and Ninety Dollars, Thirty-Nine Cents); £ 53,133.64 (Fifty-Three Thousand, One Hundred and Thirty-Three Pound Sterling, Sixty-Four Pence;€172,547.10 (One Hundred and Seventy-Two Thousand, Five Hundred and Forty-Seven Euros, Ten Cents); T1,300.00 (One Thousand, Three Hundred Indian Rupees); CAD $ 3,400.00 (Three Thousand, Four Hundred Canadian Dollars); ¥74,859:00 (Seventy-Four Thousand, Eight Hundred and Fifty-Nine Chinese Yuan); AUS $ 740:00 (Seven

[33] Ibid
[34] Ayomikunle Daramola. "Police: Cybercrime unit recovered N8bn, $115k in 2024 — rated best in Africa. " available at https://www.thecable.ng/police-cybercrime-unit-recovered-n8bn-115k-in-2024-rated-best-in-africa/ accessed on 16th August, 2025.
[35] EFCC. Available at https://www.efcc.gov.ng/efcc/ accessed on 16th August, 2025.
[36] Media and Publicity Team, EFCC. "EFCC Unveils Cybercrime Rapid Response Service". Available at https://www.efcc.gov.ng/efcc/news-and-information/news-release/10471-efcc-unveils-cybercrime-rapid-response-service accessed on 4th August, 2025.

Hundred and Forty Australian Dollars); 170:00 UAE DIRHAM (One Hundred and Seventy United Arab Emirates Dirham); 73,000:00 KOREAN WON (Seventy-Three Thousand Korean Won); CFA 7,821,375:00 (Seven Million, Eight Hundred and Twenty-One Thousand, Three Hundred and Seventy-Five West African CFA) to R 50:00 (Fifty South Africa Rands). [37]

5.0 Strategies and Tools Employed by Law Enforcement

As time goes by, cybercriminals grow in various ways of making attacks, this, therefore, has necessitated the needs for law enforcement agencies to step up their ways of combatting cybercrimes. Through performing their functions, law enforcement agencies have also come up with different strategies in combatting the threats put forward by these data sucking thieves.

A. Digital forensics and investigative techniques

Serving as a key strategy in combating cybercrime, digital forensic expands itself way across different spheres in the digital world. Digital forensics sits itself as a branch under cybersecurity, which focuses on the recovery and investigation of material found in digital devices and cybercrimes.[38] Digital forensic becomes necessitated in order to present evidence in a court of law when required.[39]Digital forensics underpins virtually all cybercrime investigations by enabling law enforcement to identify, preserve, analyze, and present electronic evidence in court.[40]

Law enforcement agencies increasingly integrate AI/ML–enabled tools to automate pattern detection, anomaly flagging, and large-scale data correlation, accelerating lead generation and threat attribution.[41] Digital forensics play a significant role in fighting cybercrimes as it provides powerful tools and techniques which are core to aiding investigations of cyber crime cases. Through digital forensic, it is feasible to recover the deleted, modified, hidden and corrupted data and to collect the evidence using tools and techniques. Digital forensic can help us to track the

[37] Ibid

[38] Abi Tyas Tunggal. "What is Digital Forensics?" available at https://www.upguard.com/blog/digital-forensics accessed on 4th August, 2025.

[39] Computer Forensic. "What is Digital Forensics? Phases of Digital Forensics in Cybersecurity". Available at https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-digital-forensics/ accessed on 4th August, 2025.

[40] Zenarmor Content team. "An Introduction to Digital Forensics: Types and Techniques". Available at https://www.zenarmor.com/docs/network-security-tutorials/what-is-digital-forensics?utm accessed on 4th August, 2025.

[41] Gilad Ben Ziv. "Emerging Trends and Technologies in Digital Forensics Investigations". Available at https://www.cognyte.com/blog/digital-forensics-investigations/?utm accessed on 4th August, 2025.

attackers place by analyzing network traffic and logs and it also help us to find weakness and loop hole which later we can patch and improve the security. [42]

B. Cyber Patrol and Surveillance Operations

A society watch on the digital space that monitors activities engaged in by people on the internet space. It involves making use of technology to monitors of Internet users. Digital surveillance is the use of technology in monitoring, tracking, and making checks of activities carried on, within the virtual space. [43] This method encompasses several key ways it could be carried out. A notable key one is the use of Open Source Intelligence (OSINT). Through, Open-Source Intelligence (OSINT), surveillance is carried out through automated monitoring of public forums, marketplaces, and social media for indicators of trafficking, hate speech, or fraud. [44] Another way in which this could be done is through proactive cyber patrols, often termed Internet Patrol Units or digital community policing, which allow agencies to detect illicit online activity before formal complaints. [45]

Undercover Online Investigations: Covert profiles on encrypted platforms to infiltrate criminal networks; augmented by threat-specific task forces.[46]

C. Use of Artificial Intelligence and Data Analytics

AI and advanced analytics transform law enforcement's ability to detect, predict, and respond to cybercrime. Artificial Intelligence (AI) involves the use of intelligent algorithms and machine learning techniques to make efficient, the detection, prevention, and response to cyber threats. AI supports cybersecurity systems to analyze large information and data, identify certain key patterns, and make quick decisions, which functions far beyond human capabilities. [47] The use of Artificial Intelligence in cybersecurity revolutionizes threat detection, and strengthens vulnerability

[42] GeeksforGeeks Content Team. "Digital Forensics in Cyber Security". Available at https://www.geeksforgeeks.org/computer-networks/digital-forensics-in-cyber-security/ accessed on 4th August, 2025.
[43] Paul Hawkes. "Digital Surveillance Explained". Available at https://researchassociates.com/digital-surveillance-explained/ accessed on 4th August, 2025.
[44] Prithwish Ganguli. "*Digital Policing: Using Social Media Surveillance to Tackle Cybercrime."* Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5124657 accessed on 5th August, 2025.
[45] Group 2 (Mr. Elcio Ricardo de Carvalho (Brazil), Mr. Mirza Abdullahel Baqui (Bangladesh), Ms. Rita Chun-fa Lam (Hong Kong), Mr. Yoichi Omura (Japan), Mr. Hiroyuki Ito (Japan), Mr. Takuya Matsunaga (Japan), Mr. Gilbert Caasi Sosa (Philippines), Mr. Napoleon Bonaparte (Indonesia), Mr. Jesus Rodriguez Almeida (Mexico)). "Challenges and Best Practices in Cybercrime Investigation". Available at https://www.unafei.or.jp/publications/pdf/RS_No79/No79_15RC_Group2.pdf?utm accessed on 5th August, 2025.
[46] Ibid
[47] Fortinet. "AI in Cybersecurity: Key Benefits, Defense Strategies, & Future Trends" available at https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity accessed on 5th August, 2025.

management. Through analyzing behaviors, detecting phishing, and adapting to new threats, AI empowers cybersecurity strategies, enabling proactive defense and safeguarding sensitive data. [48] AI-driven systems learn from experience, allowing them to predict, detect, and respond more effectively to known and unknown threats which makes it an advanced distinction to the conventional cybersecurity tools, which rely on established rules to detect threats,. Through that, AI safeguards organizations' cyber measures protect against breaches. [49]

6.0 Challenges Facing Law Enforcement Agencies

Law enforcement agencies worldwide face an unprecedented convergence of challenges that significantly serve as a barrier and hinder their ability to effectively serve and protect communities. These challenges, ranging from resource constraints to technological hurdles and internal integrity issues, threaten the fundamental operations of policing in the 21st century.

A. Inadequate Funding and Technological Tools

Law enforcement agencies are struggling with high budget constraints that significantly limit their operational capacity. Through research, it has been shown that law enforcement and corrections funding is spent on operational costs (salaries and benefits, administrative expenses), leaving only a little amount being directed for other important things like facilities, equipment, and technology. [50]This imbalance creates a critical gap between essential needs and available resources.

The financial pressures are quite much for smaller departments. Lots of these agencies do not have specific budget lines tailored to cater for technology costs and must rely on other entities such as domestic or regional agencies for technological support. This dependency creates vulnerabilities in operational capability and leaves departments unable to independently invest in critical technological infrastructure. [51]

[48] Ibid
[49] Courtney Goodman. "AI in Cybersecurity: Transforming Threat Detection and Prevention." Available at https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/ accessed on 5th August, 2025.
[50] National Public Safety Partnership. Understanding Technology Cost Considerations in Law Enforcement. Available at https://vrnclearinghousefiles.blob.core.windows.net/documents/PSP_PoliceTechnologyCost_v5.pdf?utm accessed on 13th August, 2025.
[51] Ibid

B. Technology Investment Challenges

Despite the challenges, technology investments can provide little to no significant returns. Modern technological tools enable departments to quickly identify suspects, locate stolen vehicles, and close cases faster. [52]

Police departments face significant obstacles in modernizing their technological capabilities. It has been revealed that the police IT spend goes toward maintaining legacy systems, with most technology budgets focused on "keeping the lights on" rather than innovation or transformation.[53]This maintenance-focused approach prevents agencies from investing in cutting-edge tools that could enhance operational efficiency and public safety outcomes.

The procurement process itself, presents additional barriers. Complicated procurement procedures make it difficult for suppliers, especially smaller firms, to work with law enforcement agencies.[54] These bureaucratic obstacles, combined with unstable funding and short-term planning, often result in projects that begin with initial funding but lack resources for scaling up or effective post-implementation support.[55]

C. Training and Development Challenges

Insufficient staffing directly impacts training capacity and professional development. With 95% of officers reporting direct impacts of low staffing at their agencies, many officers have less time for training and policy review. [56]This training deficit occurs precisely when law enforcement faces increasingly complex challenges requiring specialized knowledge and skills.

The recruiting challenges are compounded by high failure rates during the screening process. Some agencies report disqualification rates as high as 98.5% during the law enforcement screening process.[57] This combination of high standards and limited qualified applicants creates a mathematical impossibility for filling available positions in many jurisdictions.

---

[52] Why Police Technology Is a Must for Small Departments. Available at https://www.flocksafety.com/blog/why-police-technology-is-a-must-for-small-departments?utm accessed on 13th August, 2025.

[53] How are funding issues holding back the deployment of new police tech? Available at https://www.virginmediao2business.co.uk/insights/funding-issues-new-police-tech/?utm accessed on 13th August, 2025.

[54] Ibid

[55] Ibid

[56] Laura Neitzel. "Staffing shortages are having a negative impact on policing, but technology can help". Available at https://www.police1.com/police-products/investigation/cameras/articles/staffing-shortages-are-having-a-negative-impact-on-policing-but-technology-can-help-a7y5LsOctxs1QwV7/?utm accessed on 15th August, 2025.

[57] Sid Smith. "A Crisis Facing Law Enforcement: Recruiting in the 21st Century". Available at https://www.policechiefmagazine.org/a-crisis-facing-law-enforcement-recruiting-in-the-21st-century/?utm accessed on 15th August, 2025.

D. Jurisdictional Issues and Internet Anonymity

A key feature of the internet is how the usage is not confined in a particular physical boundary. This makes it so for cybercrime as well, as cybercriminals, victims, and the tools used spread across boundaries and different jurisdictions. Due borderless nature of the internet, law enforcement agencies often experience key challenges in jurisdictional issues, and its enforcement. More than half of all criminal investigations now require access to cross-border electronic evidence, however, traditional legal frameworks remain anchored and focused on particular geographical boundaries that are meaningless and non-enforceable in the cyberspace.[58]

Key jurisdictional complications include:

Territoriality principle challenges: The traditional principle granting states authority over activities within geographic boundaries becomes "anachronistic and unable to accommodate the fluid and ubiquitous nature of cyber activities" [59]

Effects doctrine complexity: While the effect doctrine principle allows states to assert jurisdiction based on cybercrime effects within their territory, this approach "risks jurisdictional overreach, leading to conflicts between sovereign states". [60]

Double criminality requirements: The principle requiring crimes to be recognized in both requesting and requested jurisdictions "often impedes the extradition of cybercriminals" when national laws differ significantly which may cause national conflict between states. [61]

7.0 Success Stories and Notable Cases

Operation HAECHI IV[62]

Operation HAECHI IV (July–December 2023) was a six-month long international criminal operation which was led by the International Criminal Police Organization, **INTERPOL,** which

[58] Fran Casino, Claudia Pina, Pablo López-Aguilar, Edgar Batista, Agusti Solanas, Constantinos Patsakis. "SoK: cross-border criminal investigations and digital evidence Open Access". Available at https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060?utm accessed on 16th August, 2025.

[59] Hayden Coupla. "Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them". Available at https://www.york.ac.uk/media/law/documents/eventsandnewsdocs/2.%20Investigating%20Cybercrime_The%20Key%20Jurisdictional%20and%20Technical%20Challenges%20Faced%20by%20Law%20Enforcement%20and%20Ways%20to%20Address%20Them.pdf?utm accessed 16th August, 2025.

[60] Ibid

[61] Ibid

[62] Interpol intl News. "USD 300 million seized and 3,500 suspects arrested in international financial crime operation". Available at https://www.interpol.int/en/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation accessed on 16th August, 2025.

was aimed at targeting several fraudulent activities such as voice phishing, romance scams, investment fraud, business email compromise and related cyber-enabled crimes. According to the press release published by Interpol, a joint activity was conducted against a prominent online gambling criminal in Manila. The law enforcement agencies seized a total of USD 199 million in hard currency and USD 101 million in virtual assets. The operation resulted in 3,500 arrests across 34 countries, blocking 82,112 suspicious bank accounts and 367 virtual asset accounts via I-GRIP. "Cooperation between Filipino and Korean authorities led to the arrest in Manila of a high-profile online gambling criminal after a two-year manhunt by Korea's National Police Agency." "The seizure of USD 300 million represents a staggering sum and clearly illustrates the incentive behind today's explosive growth of transnational organized crime. This represents the savings and hard-earned cash of victims. This vast accumulation of unlawful wealth is a serious threat to global security and weakens the economic stability of nations worldwide." revealed, **Stephen Kavanagh**, *INTERPOL's Executive Director of Police Services*. [63]

Operation Red Card (Nov 2024**–Feb 2025).** [64]

The operation was a three month operation aimed at targeting international cyberattacks and cyber enabled scams which led to the arrest of 306 suspects, and the seizure of 1842 devices. The operation spanned across 7 nations in the African continent, including Nigeria, South Africa, Rwanda, Zambia etc. [65]

The Nigerian police made a total of 130 arrests, including 113 foreign nationals who were allegedly involved in cyber scams, like online casino and investment fraud. The South African authority, on the other hand, arrested 40 individuals including the seizure of over 1,000 sim cards, along with 53 desktops and towers linked to a sim card related fraud. The Zambian made an arrest of 14 individuals who were alleged to be members of a criminal syndicate involved in cyber related fraud. [66] According to Neal Jetton, INTERPOL's Director of the Cybercrime Directorate, "The success of Operation Red Card demonstrates the power of International cooperation in combating cybercrime, which knows no borders and can have devastating effects on individuals and

[63] Pierluigi Paganini. "Law enforcement Operation HAECHI IV led to the seizure of $300 Million". Available at https://securityaffairs.com/156209/cyber-crime/haechi-iv-operation-interpol.html accessed on 16th August, 2025.
[64] Interpol News. "More than 300 arrests as African countries clamp down on cyber threats" available at https://www.interpol.int/en/News-and-Events/News/2025/More-than-300-arrests-as-African-countries-clamp-down-on-cyber-threats accessed on 16th August, 2025.
[65] Ibid
[66] Ibid

communities. The recovery of significant assets and devices, as well as the arrest of key suspects, sends a strong message to cybercriminals that their activities will not go unpunished."

"Kaspersky is proud to be part of this collaborative effort led by INTERPOL. The evolving threat landscape in Africa requires a multi-stakeholder dialogue and joint efforts of public and private organizations to address the cybersecurity challenges the region faces today. The Red Card operation is a notable example of such cooperation, showcasing how the expertise of private companies coupled with extensive investigative capacities of law enforcers can foster a more cyber-resilient environment," comments Yuliya Shlychkova, Vice President, Global Public Affairs, Kaspersky.

Operation Artemis (2023)

This was a joint operation jointly conducted by the Federal Bureau of Investigation (FBI) and the Economic Financial Crime Commission (EFCC) [67] which led to the apprehension of 22 Nigerians who were accused of running sextortion, a crime that led to the increasing suicide of teenagers in the United States, for financial gains. The FBI reported that half of the suspects were connected to the victims who took their lives.

"*Once the content was obtained, the victims were blackmailed with threats of public exposure unless they paid ransom often through gift cards, mobile money, or cryptocurrency.*

"The harassment frequently continued even after payments were made", FBI revealed. [68]

Oluwadamilare Samuel (Aug 2025): *Conviction under the Cybercrime Act*

Lawal Oluwadamilare Samuel was sentenced to jailed on a cybercrime related offence at a Federal High Court sitting in Ikoyi, Lagos State. Lawal was reported to have created a fake facebook account acting under a female profile, identifying as Sandra Brooks, a female in Virginia, United States of State, to one Keith based in the USA, later fraudulently obtaining up to Seven Hundred United States Dollars, $700. The accused was eventually convicted and sentenced to six months imprisonment, with an option of fine of N3,000,000.00 (Three Million Naira). The accused was

[67] EFCC. Available at https://www.efcc.gov.ng/efcc/ accessed on 16th August, 2025.

[68] Ojochenemi Onje "How FBI and EFCC arrested 22 Nigerians for sextortion in operation Artemis". Available at https://businessday.ng/news/article/how-fbi-and-efcc-arrested-22-nigerians-for-sextortion-in-operation-artemis/ accessed on 16th August, 2025.

also ordered to forfeit the Samsung Galaxy S9, HP laptop, Samsung tab, Mercedes Benz C300 2008 model and N500,000.00. [69]

Conclusion

In the time where technology becomes an integral part of man's day to day activities, and where easy and effective solutions are brought through the use of technology, businesses have been stuck in between the choice of adopt the use of technology or be seen lagging in areas where competitors have gone past, in their daily activities. This has even prompted financial institutions to adopt the use of technology in replacing manpower where possible.

The adoption of technology, therefore, now has served as a magnet attracting different forms of cyber related crimes like phishing, email scam, advanced fee fraud, and many other cybercrime activities for the purpose of gaining unauthorized access to information and data for financial gains. Hardly a time goes without increase in cyber related crimes being reported. As time goes by, technology improves, cybercriminals continue to explore different methods of attack. This efforts by cybercriminals have not gone without the notice of the government that has been charged with the duty of enacting an act, serving as the cornerstone in combating cybercrimes, particularly, in Nigeria – Cybercrimes (prevention, prohibition, etc) Act 2015. [70]

The Cybercrime Act, passed into law in 2015 has been the major enactment serving to guide and regulate activities carried on, on the cyberspace in Nigeria. The act provides an effective, and well-detailed comprehensive legal regulatory framework for prohibiting, preventing, prosecuting and punishing cyber related crimes, and cyber criminals in Nigeria. In addition to that, the act also protects guards infrastructure which are key to national information, and promotes cybersecurity and the protection of computer systems and networks, electronic communications, data and computer program, intellectual property and privacy rights.[71] However, despite having a primary enactment serving to address the issues of cybercrimes, as well as having other acts addressing the threats posed by cybercrimes, it begs the question of *how have cybercrimes reduced in Nigeria?* On an objective look is the discovery that it is only ideal to say that the act is without its loopholes,

[69] EFCC Media & Publicity Team. "Court Jails Man Six Months for Internet Fraud in Lagos" . Available at https://www.efcc.gov.ng/efcc/news-and-information/news-release/11339-court-jails-man-six-months-for-internet-fraud-in-lagos-2?utm accessed on 16th August, 2025.

[70] Cybercrimes (prevention, prohibition, etc) Act 2015

[71] See the preamble of the Cybercrimes (Prevention, Prohibition) Act, 2015.

and lack of Enforcement posed by the act serves as a way to manipulate its provisions by potential cybercriminals.

The continuous increase in cybercrime has imposed the duty of addressing and moving from combatting traditional financial crimes, and crimes generally to addressing cybercrimes on law enforcement agencies like the Economic Financial Crime Commission (EFCC), the Federal Bureau of Investigation (FBI), the Nigeria Police Force creating a cybercrime department identified as the Nigeria Police Force – National Cybercrime Centre, which consists of officers who have a very strong IT background and are well versed in the aspect of technology. Another notable efforts taken by these law enforcement agencies include the creation of a 24- hour Cybercrime Rapid Response Desk which was meant to provide both local and international telephone numbers in reaching the body anywhere across the globe. [72] Ideally, it is will only be fair to recognize the continuous efforts of these law enforcement agencies who have since it became a task, engaged in rigorous fights against cybercrimes and cybercriminals. The participation of law enforcement agencies in several key operations has witnessed the capture of cybercriminals, recovery of stolen funds and recovery of stolen items. Notable operations which have been participated in include the transcontinental **Operation HAECHI IV[73]** by the INTERPOL, **Operation Red Card,[74]** an African Continental operation, **Operation Artemis (2023)[75]** jointly operated by the FBI and EFCC. These operations have witnessed "clamp down" of several cyber threats, cybercriminals, seizure of bank accounts, and recovery of several items including phones, laptops, among many others.

[72] Media and Publicity Team, EFCC. "EFCC Unveils Cybercrime Rapid Response Service". Available at https://www.efcc.gov.ng/efcc/news-and-information/news-release/10471-efcc-unveils-cybercrime-rapid-response-service accessed on 4th August, 2025.

[73] Interpol intl News. "USD 300 million seized and 3,500 suspects arrested in international financial crime operation". Available at https://www.interpol.int/en/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation accessed on 16th August, 2025.

[74] Interpol News. "More than 300 arrests as African countries clamp down on cyber threats" available at https://www.interpol.int/en/News-and-Events/News/2025/More-than-300-arrests-as-African-countries-clamp-down-on-cyber-threats accessed on 16th August, 2025.

[75] Ojochenemi Onje "How FBI and EFCC arrested 22 Nigerians for sextortion in operation Artemis". Available at https://businessday.ng/news/article/how-fbi-and-efcc-arrested-22-nigerians-for-sextortion-in-operation-artemis/ accessed on 16th August, 2025.