web of semantic

Journal of Interdisciplinary Science | ISSN: 2960-9550

Research Article Peer-review, Open Access

Cybercrime Regulation in Nigeria: a Comparative Analysis with International Best Practices

Dr Kalada [1]
D.S. Nonju [2]
Agent Benjamin Ihua-Maduenyi [3]

Abstract: Cybercrime is in the increase and becoming a growing concern in Nigeria. Rapid digitalization has exposed vulnerabilities to various cyber threats, including fraud, identity theft, and ransom ware attacks. In response to this trend, Nigerian Government has enacted the Cybercrimes (Prohibition, Prevention, etc.) Act in 2015, aimed at providing a legal framework to combat cybercrime. However, the effectiveness of this regulation remains a subject of scrutiny, with concerns about enforcement capacity, resource allocation, and alignment with international standards. This paper undertakes a comparative analysis of Nigeria's cybercrime regulation against global best practices, drawing on legal frameworks from the European Union's General Data Protection Regulation (GDPR), the Council of Europe's Convention on Cybercrime (Budapest Convention), and the United States' cyber security strategies.

While Nigeria's legal framework criminalizes cyber offenses and provides guidelines for digital evidence, there are challenges in the areas of international cooperation, data privacy, and technical capacity for cyber investigation and prosecution. Unlike the Budapest Convention, which facilitates cross-border cooperation, Nigeria's law lacks robust provisions for mutual legal assistance and data-sharing agreements with other nations. Furthermore, Nigeria's enforcement mechanisms are hindered by limited resources and technical expertise, leading to low conviction rates. This study recommends reforms to align and synergize Nigeria's cybercrime legislation with international standards, including provisions for improved collaboration, investigations, specialized training, and greater data protection measures. Such reforms are essential for Nigeria to mitigate cyber risks effectively and foster trust in its digital economy. This analysis emphasizes the need for harmonized, adaptive legal frameworks that balance cyber security imperatives with individual rights and align with evolving global cyber norms.

Keywords: cyber, crime, regulation, comparative, analysis, international

1.0 Introduction

Cybercrime presents an increasingly pervasive threat to global security, economic stability, and individual privacy. In the digital age, cyber threats have evolved to encompass a range of sophisticated

activities, from hacking and financial fraud to ransom ware, data theft, and cyber espionage. This growth in cyber threats has compelled nations to develop legal frameworks to mitigate risks and enforce penalties for cyber-related offenses. For Nigeria, a rapidly digitalizing economy, the stakes are particularly high [1], [2]. Despite being one of Africa's largest economies, Nigeria has faced significant challenges in combating cybercrime effectively, with high-profile cases of financial fraud and data breaches highlighting vulnerabilities in its cyber infrastructure. The Nigerian government took a significant step toward addressing these challenges with the Cybercrimes (Prohibition, Prevention, etc.) Act in 2015, which aimed to regulate cyber activities and establish deterrents for cybercriminals. However, while this Act represents progress, questions remain about its effectiveness and alignment with international standards [3].

This paper examines Nigeria's cybercrime regulatory framework through a comparative analysis with international best practices, specifically evaluating how it measures against the standards set by the European Union's General Data Protection Regulation (GDPR), the Council of Europe's Convention on Cybercrime (Budapest Convention), and the United States' cyber security policies [4]. These frameworks provide essential benchmarks as they represent some of the most comprehensive legal responses to cyber threats, with provisions that promote cross-border cooperation, data protection, and clear penalties for cyber offenses.Nigeria's Cybercrimes Act is structured to address a wide spectrum of cyber threats, including hacking, identity theft, and cyber terrorism. It includes provisions for offenses such as unauthorized access, computer-related fraud, and data interference, along with penalties aimed at deterring cybercriminals [5], [6]. However, enforcement has proven difficult, largely due to resource constraints and the complexity of tracing cybercriminals across borders. In contrast, the Budapest Convention on Cybercrime, which Nigeria has not yet ratified, promotes international collaboration by encouraging member states to adopt standardized definitions and procedures for cybercrime offenses. This treaty also provides a framework for mutual legal assistance and facilitates cooperation among law enforcement agencies worldwide in combating cross-border cybercrime. Ratifying and implementing principles of the Budapest Convention could offer Nigeria an enhanced legal toolkit for addressing the transnational nature of cyber threats [7], [8]. However, Nigeria's reluctance to adopt the Convention may be attributed to concerns about data sovereignty and the perceived limitations on its legislative independence.

Another critical area where Nigeria's framework diverges from international standards is in data protection and privacy. The European Union's GDPR has become a benchmark for data protection, mandating strict regulations on data processing, user consent, and breach notification, with severe penalties for non-compliance [9]. In Nigeria, data protection laws are in a relatively nascent stage. The Nigeria Data Protection Regulation (NDPR), introduced in 2019, aims to enhance data privacy and security, yet it lacks the rigorous enforcement mechanisms and comprehensive reach of the GDPR.The absence of robust data protection standards undermines Nigeria's cybercrime regulatory framework, as data security is central to preventing identity theft, fraud, and other cybercrimes. Strengthening data protection laws in line with the GDPR could enhance Nigeria's ability to mitigate cyber risks and safeguard user privacy [10].

Moreover, enforcement remains a considerable challenge within Nigeria's cybercrime framework. While the Cybercrimes Act criminalizes a range of offenses and assigns responsibilities to specific agencies, including the Economic and Financial Crimes Commission (EFCC) and the Nigerian Police Force, these agencies often lack the resources and technical expertise necessary to enforce cyber laws effectively. By contrast, the United States has adopted a more comprehensive approach, involving both federal and state agencies in cybercrime enforcement, as well as partnerships with the private sector [11]. The United States also emphasizes capacity building and public-private partnerships, which have proven essential in addressing complex cyber threats. Adopting a similar multi-stakeholder approach could strengthen Nigeria's enforcement capabilities by fostering collaboration and resource sharing among government agencies, private companies, and international partners [12].

International cooperation is another vital component of effective cybercrime regulation, as cyber threats often transcend national borders. However, Nigeria's regulatory framework lacks provisions that promote cross-border collaboration. This gap hinders Nigeria's ability to respond effectively to transnational cybercrime, as cybercriminals frequently exploit jurisdictional challenges to avoid detection and prosecution [13]. Encouraging international collaboration, whether through ratifying the Budapest Convention or forming bilateral agreements with other nations, could provide Nigeria with valuable resources and support in combating cybercrime.In conclusion, while Nigeria's Cybercrimes Act represents a positive step toward addressing the country's cybercrime challenges, gaps remain in terms of enforcement capacity, data protection, and international cooperation. Aligning Nigeria's framework with international standards, such as those established by the Budapest Convention and GDPR, could enhance its ability to respond to cyber threats effectively. Such alignment would not only improve Nigeria's cyber resilience but also build trust in its digital economy, fostering a safer environment for businesses and individuals alike . Achieving this, however, will require concerted efforts to strengthen regulatory enforcement, bolster data protection laws, and embrace international cooperation [14], [15]. As Nigeria continues to navigate the challenges posed by digital transformation, aligning with global cyber governance standards will be essential to ensuring its cybercrime framework remains robust, adaptable, and capable of safeguarding its citizens and economy in the face of evolving cyber threats.

Methodology

2.1 An Overview of Cyber Crime Regulations in Nigeria

Cybercrime regulation in Nigeria has gained urgency as the country's digital landscape expands rapidly. The proliferation of internet connectivity, digital financial services, and mobile technology has facilitated economic growth but also introduced significant vulnerabilities to cyber threats such as hacking, identity theft, and financial fraud. To address these risks, Nigeria enacted the *Cybercrimes (Prohibition, Prevention, etc.) Act* in 2015, which provides the primary legal framework for combating cybercrime. However, Nigeria's regulatory framework has faced criticisms regarding its enforcement capacity, alignment with international standards, and effectiveness in mitigating cyber risks.

The *Cybercrimes Act 2015* is Nigeria's first comprehensive legislation on cybercrime. It criminalizes various offenses, including unauthorized access to computer systems, identity theft, cyber stalking, child pornography, and online fraud.The Act also establishes penalties for financial institutions that fail to implement adequate cyber security measures and grants law enforcement agencies the authority to investigate cyber offenses.Furthermore, it mandates the protection of critical national infrastructure (CNI), such as telecommunications and banking systems, which are considered essential to national security. These provisions aim to create a robust framework for preventing, detecting, and prosecuting cybercrime in Nigeria.

Despite these advancements, the Act has encountered challenges in implementation, largely due to resource constraints and limited technical capacity among law enforcement agencies. While the Act assigns enforcement responsibilities to the Nigerian Police Force, the Economic and Financial Crimes Commission (EFCC), and the National Security Adviser, these agencies often lack the expertise and technology needed to conduct complex cybercrime investigations effectively. The EFCC, for example, has a Cybercrime Section focused on handling internet fraud cases, but the scope of its resources remains insufficient to tackle the scale and sophistication of cyber threats in Nigeria. This lack of technical capacity hampers enforcement efforts, leading to low prosecution rates and a limited deterrent effect.

Another challenge is the absence of comprehensive data protection laws. Although the *Nigeria Data Protection Regulation* (NDPR) was introduced by the National Information Technology Development Agency (NITDA) in 2019, it is not as robust as international standards like the European Union's *General Data Protection Regulation* (GDPR). The NDPR sets guidelines for data processing, breach notification, and user consent but lacks the enforceability and depth of protections seen in the GDPR. Without strong data protection standards, Nigeria remains vulnerable to data breaches and identity theft,

which are central issues in cybercrime. Strengthening data protection would not only bolster cyber security but also build public trust in digital services, which is crucial for the continued growth of Nigeria's digital economy.

Nigeria's cybercrime regulation also lacks provisions for international cooperation, which is essential in combating cybercrime due to its cross-border nature. Cybercriminals often operate across multiple jurisdictions, exploiting legal and regulatory differences to evade detection and prosecution. The Council of Europe's *Convention on Cybercrime*, also known as the Budapest Convention, is a widely adopted treaty that facilitates cross-border cooperation and harmonizes cybercrime laws among member states. However, Nigeria has yet to ratify the Budapest Convention, a gap that limits its ability to collaborate with international partners effectively. Ratifying the Convention could improve Nigeria's capacity to handle transnational cybercrime cases by allowing it to participate in mutual legal assistance arrangements and information-sharing mechanisms with other countries.

Furthermore, the private sector's role in cyber security is relatively underdeveloped within Nigeria's regulatory framework. The *Cybercrimes Act 2015* mandates certain cyber security obligations for financial institutions, but there is limited regulatory guidance for other industries critical to national infrastructure, such as energy, healthcare, and transportation. By contrast, countries like the United States and the European Union emphasize public-private partnerships in cyber security efforts, recognizing that effective cyber security requires collaboration between government, private sector entities, and civil society. Establishing partnerships with private sector stakeholders and implementing industry-specific cyber security standards could strengthen Nigeria's resilience to cyber threats.

Another issue with the *Cybercrimes Act* is the absence of a dedicated regulatory body solely focused on cyber security. While several agencies share cyber security responsibilities, including NITDA, the Central Bank of Nigeria, and the Office of the National Security Adviser, there is no single entity with overarching authority for cyber security policy, implementation, and coordination. This fragmentation can result in overlaps, inefficiencies, and a lack of cohesive strategy, ultimately weakening Nigeria's overall cyber resilience. A centralized cyber security agency, similar to the U.S. *Cyber security and Infrastructure Security Agency* (CISA), could address these coordination issues by streamlining cyber security efforts across different sectors and ensuring consistent enforcement of regulations.

There are also concerns about civil liberties within Nigeria's cybercrime regulation. The *Cybercrimes Act 2015* includes provisions for the interception of communications and the collection of digital evidence, which have raised privacy concerns among civil society organizations. Critics argue that some sections of the Act grant law enforcement agencies broad surveillance powers without sufficient judicial oversight, potentially infringing on individuals' right to privacy. Balancing cyber security with privacy and civil liberties is a delicate task, as overly invasive regulations could undermine trust in digital services and discourage innovation. Adopting clearer legal safeguards, such as judicial authorization for communication interception, would help protect individuals' rights while still allowing law enforcement agencies to perform their duties.In conclusion, Nigeria's *Cybercrimes (Prohibition, Prevention, etc.) Act 2015* represents a foundational step toward regulating cybercrime, yet significant gaps remain. Addressing challenges in enforcement, data protection, international cooperation, private sector engagement, and civil liberties will be crucial for Nigeria to enhance its cyber resilience. Aligning its regulatory framework with international standards, such as those established by the Budapest Convention and GDPR, could offer Nigeria a more effective and globally compatible approach to cyber security. With Nigeria's digital economy continuing to expand, adopting these improvements is essential not only to protect the nation's critical infrastructure but also to foster trust in its digital transformation journey. Strengthening cybercrime regulation through a multi-stakeholder approach that includes government agencies, private sector entities, and international partners will be key to securing Nigeria's digital future.

2.2 Institutional Framework: Roles of Law Enforcement, Judiciary and Regulatory Agencies.

The institutional framework for cybercrime regulation in Nigeria involves a range of stakeholders, including law enforcement agencies, the judiciary, and various regulatory bodies. Each institution plays a critical role in enforcing cyber laws, ensuring compliance, and prosecuting offenders. Despite these efforts, the framework faces challenges in coordination, resource allocation, and technical capacity. This section examines the roles of law enforcement, the judiciary, and regulatory agencies in Nigeria's cybercrime regulatory structure, analyzing their effectiveness and limitations within the context of the *Cybercrimes (Prohibition, Prevention, etc.) Act* 2015.

2.2.1. Law Enforcement Agencies

Law enforcement agencies are the primary executors of cybercrime regulation in Nigeria. Under the *Cybercrimes Act 2015*, the Nigerian Police Force, Economic and Financial Crimes Commission (EFCC), and Department of State Services (DSS) are tasked with investigating cyber offenses, arresting suspects, and supporting prosecution efforts.

2.2.1.1. The Nigerian Police Force is authorized to investigate various forms of cybercrime, including identity theft, cyber stalking, and hacking. The Cybercrime Unit within the Nigerian Police Force handles cybercrime cases and works to improve the digital forensics capabilities required to track online offenders. However, the police often lack advanced technology and specialized training to handle sophisticated cyber threats, which limits their ability to enforce the law effectively.

2.2.1.2. The Economic and Financial Crimes Commission (EFCC) plays a critical role in investigating financial cybercrimes, particularly those involving online fraud, phishing scams, and money laundering. The EFCC's Cybercrime Section focuses on preventing internet-based financial crimes, and it has had notable success in tracking down and arresting perpetrators involved in high-profile fraud cases. However, the EFCC faces significant challenges, including resource constraints and an overwhelming number of cyber fraud cases, which hinder its effectiveness.

2.2.1.3. The Department of State Services (DSS) is primarily responsible for national security-related cyber threats, including cyber terrorism and espionage. The DSS collaborates with other intelligence agencies and law enforcement bodies to monitor potential cyber threats that could impact Nigeria's critical infrastructure and national security. Although the DSS has some technical expertise, its activities are often constrained by limited resources and a lack of collaboration with other stakeholders, which can reduce its overall impact on cybercrime regulation.

2.2.2. The Judiciary

The judiciary plays an essential role in interpreting and applying cybercrime laws, ensuring justice in cyber-related cases, and upholding due process. The *Cybercrimes Act 2015* grants Nigerian courts the authority to hear cases involving cyber offenses, determine appropriate penalties, and enforce judgments. The Federal High Court has exclusive jurisdiction over cybercrime cases, as cyber offenses are considered federal crimes under the Act.Judges in Nigeria's judiciary face the challenge of adjudicating cybercrime cases that involve complex technical details and require specialized knowledge. Many judges lack training in digital forensics, cyber security, and technology law, which can result in inconsistent judgments and delays in case processing.To address this issue, some judicial training programs have been initiated to familiarize judges with digital evidence and the nuances of cyber law. However, these efforts are still in their early stages and require greater investment to ensure that the judiciary can effectively handle the growing number of cybercrime cases.

Additionally, the judiciary is often faced with procedural challenges related to digital evidence. Digital evidence is inherently different from traditional evidence, as it is more susceptible to tampering and requires stringent handling protocols to maintain its integrity. Nigerian courts have developed some guidelines for the admissibility of digital evidence, but these are not as robust as international standards, leading to potential gaps in prosecuting cybercrime effectively.

2. 2.3. Regulatory Agencies

Nigeria's cybercrime regulatory framework includes several regulatory bodies, each tasked with specific responsibilities for policy development, oversight, and compliance. Key regulatory agencies include the National Information Technology Development Agency (NITDA), the Central Bank of Nigeria (CBN), and the Nigerian Communications Commission (NCC). These agencies collectively contribute to Nigeria's cyber security and data protection strategies.

2.2.3.1. The National Information Technology Development Agency (NITDA) is responsible for overseeing data protection and ensuring compliance with cyber security regulations in the private sector. In 2019, NITDA introduced the Nigeria Data Protection Regulation (NDPR), which sets standards for data processing, user consent, and breach notification. However, NITDA's enforcement capacity is limited, as it lacks the technical resources and manpower required to conduct widespread inspections and compliance audits. Strengthening NITDA's resources and authority would enhance its ability to monitor and enforce data protection standards effectively.

2.2.3.2. The Central Bank of Nigeria (CBN) regulates cyber security standards within the financial sector, mandating that financial institutions implement robust cyber security measures to protect customer data and prevent cyber fraud.The CBN has issued guidelines on electronic banking and cyber security, requiring banks to conduct regular risk assessments, implement anti-fraud measures, and report breaches promptly. While these regulations help protect Nigeria's financial infrastructure, enforcement remains inconsistent, as many banks lack the resources to fully comply with the CBN's cyber security requirements. Strengthening oversight within the financial sector would be crucial to mitigating cyber risks and enhancing the resilience of Nigeria's banking system.

2.2.3.3. The Nigerian Communications Commission (NCC) oversees cyber security within the telecommunications industry, which forms the backbone of Nigeria's digital infrastructure. The NCC ensures that telecom providers comply with cyber security standards, protect customer data, and collaborate with law enforcement in cyber investigations. The NCC has issued guidelines on network security and incident reporting, but it faces challenges in enforcing these regulations due to the complexity and size of the telecommunications sector. Improving the NCC's regulatory reach and fostering greater collaboration between telecom providers and law enforcement would be beneficial for Nigeria's overall cyber security posture.

2.2.3.4. Challenges and Recommendations

The effectiveness of Nigeria's institutional framework for cybercrime regulation is constrained by several factors. First, there is limited coordination among law enforcement agencies, the judiciary, and regulatory bodies, which results in inefficiencies and reduces the overall effectiveness of cybercrime enforcement. A centralized cyber security agency, similar to the U.S. *Cyber security and Infrastructure Security Agency* (CISA), could enhance coordination, streamline enforcement, and improve the nation's cyber security resilience.

Second, Nigeria's law enforcement agencies and judiciary require additional training in cyber security and digital forensics to effectively handle cybercrime cases. Providing specialized training programs for law enforcement officers and judges would enhance their capacity to investigate, prosecute, and adjudicate cyber offenses effectively.

Lastly, there is a need to strengthen data protection and cyber security regulations. The Nigeria Data Protection Regulation (NDPR) needs to be aligned with international standards, such as the EU's General Data Protection Regulation (GDPR), to provide robust protections for individuals' personal data. Implementing stricter cyber security requirements for critical infrastructure sectors, including finance and telecommunications, would also improve Nigeria's resilience to cyber threats.

The roles of law enforcement, judiciary, and regulatory agencies in Nigeria's cybercrime regulation framework are critical yet challenged by resource limitations, fragmented responsibilities, and a lack of

technical expertise. Addressing these issues through improved coordination, enhanced training, and stronger data protection standards would significantly bolster Nigeria's cyber security posture and enable more effective enforcement of cybercrime laws.

Results and Discussion

2.3 Challenges: Enforcement, Capacity Building and Public Awareness

Challenges in enforcing cybercrime regulation in Nigeria are multifaceted, encompassing enforcement gaps, capacity-building limitations, and public awareness deficiencies. These issues hinder the effective implementation of the *Cybercrimes (Prohibition, Prevention, etc.) Act* 2015 and other regulatory measures, impacting Nigeria's resilience against growing cyber threats. This section discusses the challenges of enforcement, capacity building, and public awareness within Nigeria's cybercrime regulatory framework, highlighting potential solutions to address these issues.

2.3.1. Enforcement Challenges

Enforcing cybercrime regulation in Nigeria is complex due to resource constraints, technical limitations, and coordination issues among enforcement agencies. The *Cybercrimes Act 2015* designates the Nigerian Police Force, the Economic and Financial Crimes Commission (EFCC), and the Department of State Services (DSS) as primary enforcers, but these agencies often struggle with the technical demands of cybercrime investigations.

2.3.1.1. The Nigerian Police Force faces significant enforcement difficulties as it lacks the advanced digital forensic tools and expertise needed to handle sophisticated cybercrime cases. Many local police departments are unable to conduct in-depth cyber investigations, resulting in low prosecution rates and a limited deterrent effect against cyber offenders. Moreover, the police force often prioritizes physical crime over cybercrime due to resource limitations and a lack of specialized personnel, which diverts attention from enforcing cybercrime laws.

2.3.1.2. The Economic and Financial Crimes Commission (EFCC), tasked with investigating financial cybercrimes, also encounters enforcement barriers due to inadequate funding and an overwhelming number of cyber fraud cases. Although the EFCC has achieved some success in prosecuting high-profile cyber fraud cases, the sheer volume of internet fraud in Nigeria, coupled with limited resources, prevents it from effectively addressing the scale of cyber threats. Enhancing funding and equipping the EFCC with the necessary technology and training would strengthen its enforcement capacity.

Coordination challenges further hinder enforcement efforts. The *Cybercrimes Act* outlines roles for multiple agencies, but the lack of a centralized cyber security agency leads to overlapping responsibilities and inefficiencies. Enhanced coordination between the Nigerian Police Force, EFCC, and DSS, potentially through a centralized cyber security body, could streamline enforcement and improve Nigeria's response to cybercrime.

2.3.2. Capacity-Building Challenges

Capacity building is essential for the successful enforcement of cybercrime laws, but Nigeria faces significant challenges in this area. Capacity-building initiatives are needed to enhance the skills and resources of law enforcement agencies, judiciary, and regulatory bodies to effectively address cyber threats. Currently, these institutions lack sufficient training, technical expertise, and modern equipment.

2.3.2.1. Law enforcement personnel often lack specialized training in digital forensics, cyber law, and investigative techniques required to handle cybercrime cases. Many cyber offenses involve complex digital evidence that requires specialized handling, analysis, and preservation skills. Without sufficient training, law enforcement officers are unable to conduct proper investigations, leading to weak cases and low conviction rates. To address this, the Nigerian government has started to implement training programs, but these efforts remain limited in scope and impact. Expanding these programs to cover a broader range of law enforcement personnel and ensuring access to up-to-date forensic tools would

significantly improve Nigeria's capacity to enforce cyber laws.

2.3.2.2. The judiciary also faces capacity-building challenges. Judges often lack knowledge of cyber laws and digital evidence, which can affect their ability to adjudicate cybercrime cases fairly and effectively. Digital evidence, such as data stored in computers, smartphones, or the cloud, poses unique challenges in terms of admissibility and interpretation in court. Nigerian judges, who are generally trained in conventional evidence rules, may find it difficult to assess and interpret digital evidence without specialized training. Implementing continuous professional development programs on cyber law and digital forensics for members of the judiciary could help bridge this gap.

2.3.2.3. Regulatory bodies such as the National Information Technology Development Agency (NITDA) and the Central Bank of Nigeria (CBN) also face capacity-building challenges. These agencies are tasked with ensuring compliance with cyber security standards and data protection regulations. However, they often lack the resources and technical expertise to conduct rigorous audits and enforce compliance effectively. For example, NITDA's enforcement of the Nigeria Data Protection Regulation (NDPR) is limited by its lack of adequate staff and technology for compliance monitoring. Strengthening the capacity of regulatory agencies through funding, staff training, and partnerships with international cyber security organizations would enhance their ability to enforce regulations and support Nigeria's cyber security framework.

2.3.3. Public Awareness Challenges

Public awareness is critical to combating cybercrime, as an informed population is better equipped to protect itself against cyber threats. In Nigeria, however, public awareness about cybercrime risks and preventive measures remains low. The general population, businesses, and even some government institutions lack adequate knowledge of cyber hygiene practices, making them vulnerable to phishing, ransom ware, identity theft, and other forms of cyber-attacks.

2.3.3.1. Individual awareness about online security risks is limited, partly due to low digital literacy rates and insufficient educational initiatives. Many Nigerians are unaware of basic cyber security practices, such as using strong passwords, avoiding suspicious links, and recognizing phishing attempts. This lack of awareness increases susceptibility to cyber-attacks, as individuals may unknowingly expose personal and financial information to cybercriminals.Public education campaigns and community outreach programs focused on basic cyber hygiene could significantly reduce individual vulnerabilities to cybercrime.

2.3.3.2. Business awareness is also lacking, particularly among small and medium-sized enterprises (SMEs), which are often targeted by cybercriminals due to their limited cyber security measures. Many Nigerian businesses do not prioritize cyber security, viewing it as an unnecessary expense rather than an essential investment. This lack of prioritization leaves businesses vulnerable to data breaches and financial losses. Educating businesses about the economic and reputational impact of cyber-attacks, and encouraging them to implement cyber security best practices, would bolster Nigeria's overall cyber security posture.

2.3.3.3. Governmental awareness of cyber risks has improved in recent years, but challenges remain, particularly at the local level. Many local government offices lack sufficient cyber security measures, exposing them to potential attacks that could compromise sensitive data and disrupt public services.Enhancing cyber security awareness and training at all levels of government would help protect public sector institutions from cyber threats.

2.3.4. Recommendations for Addressing Challenges

Addressing Nigeria's enforcement, capacity-building, and public awareness challenges requires a multi-faceted approach. **Strengthening enforcement** would benefit from the creation of a centralized cyber security agency, similar to the U.S. *Cyber security and Infrastructure Security Agency* (CISA), which could improve coordination and streamline enforcement efforts. Additionally, increased funding for law

enforcement agencies, particularly the EFCC and Nigerian Police Force, would help address resource constraints and enable them to acquire advanced forensic tools and technology.

2.3.4.1. **For capacity building**, expanding training programs for law enforcement, judiciary, and regulatory agencies is essential. Specialized training in digital forensics, cyber law, and data protection should be mandatory for relevant personnel. **Public-private partnerships** with technology firms and international cyber security organizations could provide additional expertise and resources to enhance capacity-building initiatives.

2.3.4.2. Improving public awareness will require a coordinated national strategy that involves both government and private sector stakeholders. Implementing **public education campaigns** on cyber security practices and conducting workshops targeting individuals, businesses, and government institutions would raise awareness and reduce vulnerabilities. Schools could also integrate cyber security into digital literacy curricula to ensure that young people develop good cyber security habits from an early age.

Enforcement, capacity building, and public awareness challenges significantly impact Nigeria's ability to effectively regulate cybercrime. Addressing these issues through increased funding, targeted training, improved coordination, and enhanced public awareness initiatives would strengthen Nigeria's cyber resilience. By developing a more robust cyber security infrastructure and promoting a culture of cyber awareness, Nigeria can mitigate cybercrime threats and secure its growing digital economy.

3.0 International Best Practices in Cybercrime Regulations

International best practices in cybercrime regulation offer valuable frameworks that can strengthen a country's ability to prevent, detect, and respond to cyber threats. This section explores three major models: the *Budapest Convention on Cybercrime (2001)*, the *European Union's Directive on Security of Network and Information Systems (NIS Directive)*, and the *United States Cyber security and Infrastructure Security Agency (CISA) regulations*. Each of these frameworks provides structured approaches that Nigeria could consider for enhancing its own cybercrime regulatory mechanisms.

3.1. The Budapest Convention on Cybercrime (2001)

The *Budapest Convention on Cybercrime* is the first international treaty that seeks to combat cybercrime through harmonized legislation, procedural law tools, and international cooperation.Drafted by the Council of Europe and effective in 2004, it remains the most comprehensive international standard for cybercrime law. Although a European-led initiative, the Budapest Convention has been signed by non-European countries, including the United States, Canada, and Japan, thereby establishing itself as a global standard.

The primary aim of the Budapest Convention is to harmonize national laws by criminalizing acts such as illegal access, data interference, system interference, and misuse of devices. It also stipulates that signatories should implement investigative procedures that respect human rights and the rule of law. A distinctive feature of the Convention is its focus on international cooperation. Signatory countries are required to cooperate with each other in cybercrime investigations, expediting processes like evidence-sharing across borders.

While Nigeria is not yet a signatory to the Budapest Convention, adopting similar principles could enhance Nigeria's efforts to tackle cybercrime. The Convention's focus on harmonization and international cooperation could facilitate more robust enforcement capabilities and improve Nigeria's alignment with international standards.Additionally, the Convention serves as a foundation for technical and legal capacity-building, helping nations develop more effective responses to evolving cyber threats.

3.2. The European Union's Directive on Security of Network and Information Systems (NIS Directive)

The *NIS Directive* was adopted by the European Union in 2016 as a strategic response to the growing

threats posed to critical infrastructure through cyber-attacks. It represents the EU's first overarching cyber security law, aimed at ensuring a high common level of security for network and information systems across member states.The Directive establishes requirements for both public and private entities that are deemed "operators of essential services" (OES) and "digital service providers" (DSP).Under the NIS Directive, these entities are required to take appropriate security measures and to notify national authorities of incidents that significantly impact their services. Member states, in turn, must designate national competent authorities, establish a cyber-security strategy, and create Computer Security Incident Response Teams (CSIRTs) to facilitate swift responses to incidents. The Directive also promotes information-sharing and cooperation among member states, both within the EU and with external parties.The NIS Directive has prompted member states to bolster their cyber security infrastructure, improve risk management strategies, and prioritize the protection of critical infrastructure.While Nigeria is not subject to EU laws, aspects of the NIS Directive could serve as a model for the country's own approach to protecting essential services from cyber threats. By implementing similar measures—such as mandatory reporting for significant incidents and establishing CSIRTs—Nigeria could strengthen its cyber resilience and more effectively manage cyber risks.

3.3 United States Cyber security and Infrastructure Security Agency (CISA) Regulations

The United States' *Cyber security and Infrastructure Security Agency (CISA)* is a leading federal agency dedicated to enhancing cyber security across both public and private sectors. Established in 2018, CISA is part of the Department of Homeland Security (DHS) and is responsible for defending the nation's critical infrastructure from cyber threats. The agency collaborates with government bodies, businesses, and international partners to secure essential networks and prevent cyber-attacks.

CISA's approach to cyber security includes a strong emphasis on public-private partnerships, information-sharing, and proactive risk management. The agency works with critical infrastructure operators to implement frameworks like the National Institute of Standards and Technology's (NIST) Cyber security Framework, which outlines risk assessment and mitigation strategies. CISA also coordinates responses to cyber incidents, provides resources for cyber security awareness, and offers technical support for incident recovery. Through the *Cyber Incident Reporting for Critical Infrastructure Act of 2022,* CISA mandates that operators report significant cyber incidents, improving situational awareness and response capabilities.

Nigeria could benefit from incorporating CISA's focus on public-private collaboration and mandatory incident reporting into its cyber security framework. CISA's model highlights the importance of building relationships with industry stakeholders, as many cyber threats target private infrastructure. By creating a similar regulatory body, Nigeria could foster an environment of shared responsibility for cyber security, encourage voluntary adoption of best practices, and enhance resilience to cyber threats. International best practices such as the Budapest Convention, the EU's NIS Directive, and CISA regulations represent valuable models for addressing cyber threats. Each framework emphasizes critical elements like harmonized legislation, mandatory reporting, information-sharing, and public-private partnerships, offering Nigeria adaptable tools for strengthening its cybercrime regulatory framework. By integrating aspects of these established international standards, Nigeria could advance its capabilities in detecting, preventing, and responding to cybercrime in a rapidly evolving digital landscape.

4.0 Comparative Analysis of Cybercrime regulation between Nigeria and International Standards.

A comparative analysis of cybercrime regulation between Nigeria and international standards reveals both strengths and areas for growth within Nigeria's regulatory framework. By examining key elements such as legislative definitions, enforcement mechanisms, international cooperation, and institutional support, this section evaluates Nigeria's cybercrime framework against major international models such as the *Budapest Convention on Cybercrime (2001),* the *European Union's NIS Directive*, and the *United States Cyber security and Infrastructure Security Agency (CISA)* standards.

4.1. Legislative Framework and Definitions of Cybercrime

One of the critical steps in any cybercrime regulation framework is the clear definition of cyber offenses, which is foundational for legal consistency and enforcement. The *Budapest Convention on Cybercrime*, as the first international treaty on cybercrime, offers comprehensive definitions of offenses such as illegal access, data interference, and system interference. These definitions have been widely adopted and adapted by various jurisdictions.In Nigeria, the *Cybercrimes (Prohibition, Prevention, etc.) Act 2015* outlines various cyber offenses, including unauthorized access, cyber stalking, and identity theft, reflecting a degree of alignment with the Budapest Convention. However, some experts argue that Nigeria's definitions lack the specificity seen in the Budapest Convention and often face challenges in their applicability to emerging technologies, which may create enforcement ambiguities. Aligning Nigeria's legal definitions more closely with internationally recognized standards could provide greater clarity for enforcement agencies and increase prosecutorial success rates.

4.2. Enforcement Mechanisms and Procedural Law

The effective enforcement of cybercrime laws relies on robust procedural provisions that enable authorities to investigate, prosecute, and prevent cybercrimes. The Budapest Convention emphasizes the use of specialized investigative techniques, such as the preservation of electronic evidence and the production of subscriber information. These procedural measures are essential for tackling the cross-border nature of cybercrime.

Nigeria's *Cybercrimes Act 2015* provides some procedural tools for law enforcement, including search and seizure powers for electronic devices and preservation orders. However, enforcement remains constrained by limited resources, technological capabilities, and training among Nigerian law enforcement agencies. In contrast, CISA in the United States has implemented a well-funded framework for cyber incident response and a structured information-sharing network, fostering a more proactive approach to cybercrime management. Adopting similar resources and specialized training in Nigeria could significantly improve the nation's cybercrime enforcement capacity.

4.3. International Cooperation

Given the borderless nature of cybercrime, international cooperation is crucial. The *Budapest Convention* provides a formalized framework for international collaboration, requiring signatories to assist one another in cybercrime investigations through expedited mutual legal assistance and data-sharing channels. This mechanism allows law enforcement agencies to access evidence and conduct investigations across borders more efficiently.

Nigeria is not currently a signatory to the Budapest Convention, which limits its access to these established channels for international cooperation. Instead, Nigeria has forged bilateral agreements and participates in regional forums, but these initiatives often lack the streamlined processes and mutual legal assistance capabilities provided by the Budapest Convention.Adopting international cooperation practices from the Budapest framework could enhance Nigeria's capacity to investigate and prosecute transnational cyber offenses effectively.

4.4. Institutional and Regulatory Support

The institutional framework for cybercrime regulation plays a significant role in ensuring effective governance, policy implementation, and public-private cooperation. In the EU, the *NIS Directive* mandates that member states establish competent authorities and create Computer Security Incident Response Teams (CSIRTs) to facilitate cyber incident management. This structured approach enables EU countries to maintain national-level readiness and collaborate with one another on cyber security matters. In Nigeria, several institutions play roles in cybercrime regulation, including the *National Information Technology Development Agency (NITDA)* and the *Nigerian Communications Commission (NCC)*.While these agencies provide policy direction and support, their roles often overlap, leading to jurisdictional ambiguities and less efficient responses to cyber incidents. In comparison, CISA in the United States acts

as a centralized authority for cyber security, coordinating efforts across federal, state, and private sectors.A unified institutional framework similar to CISA could help Nigeria streamline its response to cyber incidents and improve coordination among stakeholders.

4.5. Public Awareness and Capacity Building

International models emphasize the role of public awareness and capacity-building initiatives in reducing cybercrime risk. CISA in the United States, for example, undertakes extensive public awareness campaigns and collaborates with private sector entities to enhance cyber security literacy. Similarly, the NIS Directive in the EU requires member states to implement cyber security awareness programs to educate both the public and critical infrastructure operators.

Nigeria has made efforts in this area, particularly through NITDA's public awareness programs and the NCC's initiatives to promote safe digital practices. However, these campaigns are often limited in reach and impact due to resource constraints and competing national priorities.Increasing investment in cyber security awareness and skills development could improve Nigeria's overall cyber resilience, aligning it more closely with international best practices. The comparative analysis indicates that Nigeria has made substantial progress in establishing a legal and institutional framework for cybercrime regulation. However, alignment with international standards such as the Budapest Convention, the EU's NIS Directive, and CISA regulations could further enhance Nigeria's capabilities. Specifically, adopting internationally recognized legal definitions, enhancing enforcement mechanisms, formalizing international cooperation, and investing in institutional capacity and public awareness would strengthen Nigeria's position in combatting cybercrime. By integrating these best practices, Nigeria can improve its ability to address evolving cyber threats and contribute more effectively to global cyber security efforts.

5.0 Gaps and Challenges in Nigeria's Cybercrime Regulation

Despite notable strides, Nigeria's framework for combating cybercrime has critical gaps and challenges that impact its efficacy. The *Cybercrimes (Prohibition, Prevention, etc.) Act 2015* provides the foundational legal framework, but limitations remain in enforcement, interagency collaboration, capacity-building, international cooperation, and public awareness.

5.1. Enforcement Challenges

A fundamental challenge lies in enforcing Nigeria's cybercrime laws. Law enforcement agencies often lack adequate resources, technical expertise, and forensic tools to investigate complex cybercrime cases. While the Act grants certain powers for evidence preservation and prosecution, these provisions are often undermined by logistical constraints, such as insufficient funding and outdated infrastructure. Cybercriminals frequently operate with sophisticated tactics, which require a level of forensic technology that is beyond the reach of many Nigerian agencies. Furthermore, training deficits in cyber security among law enforcement personnel hinder effective enforcement.

5.2. Capacity-Building and Training

The lack of adequate capacity-building within law enforcement and judiciary bodies presents a serious challenge. Cybercrime investigations require specialized knowledge in areas like digital forensics, network security, and cyber intelligence, yet these skills remain scarce in Nigeria.Limited investment in cyber security training and development programs results in a knowledge gap, which compromises the ability of agencies to identify, track, and prosecute cybercriminals effectively. By contrast, countries with advanced cybercrime frameworks, such as the United States and EU members, invest in continuous training and skill enhancement for their cyber law enforcement teams, enabling them to stay ahead of cyber threats.

5.3. Regulatory Overlap and Fragmentation

Nigeria's regulatory structure for cyber security and cybercrime is fragmented, creating overlap and ambiguity in roles and responsibilities. Several agencies, including the *National Information Technology*

Development Agency (NITDA), the *Nigerian Communications Commission (NCC)*, and the *Economic and Financial Crimes Commission (EFCC)*, are involved in cybercrime regulation. This multiplicity of agencies leads to jurisdictional conflicts and inconsistencies in enforcement, as each agency operates under different mandates and regulations. The lack of a cohesive, centralized agency to oversee cyber security and cybercrime regulation reduces the overall effectiveness of the framework and leads to delays in response to cyber incidents.

5.4. Limited International Cooperation

Cybercrime is inherently transnational, often requiring cross-border cooperation to gather evidence and apprehend suspects. The Budapest Convention on Cybercrime provides a structured framework for international collaboration in cybercrime investigations, but Nigeria is not a signatory. Consequently, Nigerian authorities face obstacles in obtaining assistance from foreign jurisdictions, which hampers the investigation of international cybercrime cases.Instead, Nigeria relies on regional agreements and bilateral arrangements, which lack the streamlined processes and broad mutual legal assistance available through international conventions like the Budapest Convention.

5.5. Public Awareness and Education

A significant challenge to Nigeria's cybercrime regulation is the limited public awareness of cyber security practices and cybercrime risks. Many individuals and businesses lack a strong understanding of safe online behaviors, making them vulnerable to cyber threats such as phishing, identity theft, and ransom ware attacks. Public awareness campaigns are minimal, and there are limited government-led initiatives to educate citizens on cybercrime prevention and reporting. In contrast, countries with well-developed cybercrime frameworks often invest in extensive awareness campaigns aimed at educating the public and promoting cyber security best practices. Expanding awareness and cyber security education in Nigeria would help to reduce vulnerabilities and foster a culture of proactive cyber safety.

5.6. Inadequate Legal Provisions for Emerging Threats

While the *Cybercrimes (Prohibition, Prevention, etc.) Act 2015* addresses a range of cyber offenses, it does not fully account for new and emerging cyber threats, such as those posed by artificial intelligence (AI), the Internet of Things (IoT), and advanced ransom ware attacks.Technology evolves rapidly, and legal provisions must adapt to effectively regulate these emerging cyber threats. For instance, IoT devices are increasingly targeted by cybercriminals due to their often limited security measures, yet Nigeria's laws do not specifically address IoT-related vulnerabilities. Similarly, advances in AI have facilitated the creation of "deep fake" content, which can be used for extortion, defamation, or election interference, and Nigerian law lacks specific provisions to address such offenses. Updating the legal framework to address these emerging technologies would better equip Nigeria to combat the latest forms of cybercrime.

5.7. Insufficient Data Protection Standards

Effective cyber security regulation is closely tied to robust data protection laws, as safeguarding personal data is integral to preventing cybercrimes like identity theft and fraud.24 Nigeria's *Nigeria Data Protection Regulation (NDPR) 2019* provides some degree of data protection, but enforcement is weak, and compliance among businesses remains low. Furthermore, the NDPR lacks the stringent requirements seen in frameworks like the EU's *General Data Protection Regulation (GDPR)*, which mandates high standards for data handling, storage, and breach notification. Enhancing Nigeria's data protection framework would improve privacy protections and support overall cybercrime prevention efforts.

Nigeria's cybercrime regulatory framework has established an essential foundation for addressing cyber offenses; however, significant gaps and challenges persist. To build a more resilient cyber infrastructure, Nigeria must enhance its enforcement capabilities, streamline its regulatory institutions, invest in capacity-building and training, improve public awareness, and expand legal provisions for emerging threats. Additionally, joining international conventions like the *Budapest Convention on Cybercrime* and strengthening data protection laws would position Nigeria to more effectively combat both domestic and

transnational cyber threats.

6.1. Conclusion

Nigeria's cybercrime regulation has established foundational mechanisms to address cyber threats; however, critical challenges undermine its effectiveness. The *Cybercrimes (Prohibition, Prevention, etc.) Act 2015* and the *Nigeria Data Protection Regulation (NDPR) 2019* represent commendable efforts, yet gaps in enforcement, international cooperation, regulatory coordination, and public awareness remain significant obstacles. Addressing these issues is crucial for creating a robust cyber security framework that aligns with international standards and protects Nigeria's digital economy and national security.

6.2 Summary of Findings

The examination of Nigeria's cybercrime regulation reveals several core issues:

6.2.1. Enforcement Gaps: Limited resources, outdated technology, and lack of trained personnel hinder the effectiveness of Nigerian law enforcement agencies in combating cybercrime.While the legal framework provides for evidence gathering and prosecution, these provisions are often undermined by practical enforcement barriers.

6.2.2. Fragmented Regulatory Structure: Overlapping mandates among agencies such as the *Economic and Financial Crimes Commission (EFCC), National Information Technology Development Agency (NITDA),* and *Nigerian Communications Commission (NCC)* create jurisdictional conflicts, leading to inefficiencies in cybercrime response and prevention.

6.2.3. Lack of International Cooperation: Cybercrime is transnational, necessitating collaboration across borders. However, Nigeria's absence from key international frameworks, such as the *Budapest Convention on Cybercrime,* limits its ability to engage in effective cross-border enforcement.

6.2.4. Public Awareness Deficiencies: A low level of cyber security awareness among the public and businesses increases susceptibility to cyber threats, undermining regulatory efforts.Countries with robust cyber frameworks invest heavily in public awareness and digital literacy, a gap that Nigeria must address to foster a cyber-safe environment.

6.2.5. Inadequate Provisions for Emerging Threats: The existing framework does not comprehensively address modern cyber threats, such as those related to artificial intelligence, the Internet of Things (IoT), and ransom ware. Legal reforms are required to keep pace with technological advancements and evolving cyber risks.

6.3 Implications for Policy and Practice

Based on these findings, several policy and practical recommendations emerge to strengthen Nigeria's cybercrime regulation

6.3.1. Strengthening Capacity-Building Initiatives: There is a pressing need for investments in cyber security training for law enforcement and judicial personnel to enhance the technical capacity required to investigate and prosecute cybercrimes effectively. Establishing partnerships with international cyber security organizations can support skill-building and resource-sharing.

6.3.2. Creating a Centralized Cyber security Agency: Streamlining Nigeria's cyber security regulation under a single, centralized agency could reduce regulatory fragmentation and jurisdictional conflicts, thereby improving overall coordination and responsiveness. Lessons from countries with centralized cyber security frameworks, such as the US's *Cyber security and Infrastructure Security Agency (CISA),* underscore the advantages of a unified approach.

6.3.3. Joining the Budapest Convention on Cybercrime: Becoming a signatory to the Budapest Convention would enable Nigeria to collaborate effectively with other nations on cybercrime cases. This would enhance Nigeria's ability to engage in mutual legal assistance, expedite evidence sharing, and improve cooperation in transnational investigations.

6.3.4. Enhancing Public Awareness Campaigns: Government-led cyber security awareness campaigns targeting individuals, businesses, and public institutions can play a pivotal role in reducing vulnerabilities. Public education on safe online practices and cyber hygiene would mitigate risks and build a culture of cyber security consciousness across Nigeria.

6.3.5. Updating Cybercrime Legislation for Emerging Threats: Legal reforms should address new cyber threats, particularly those related to AI-driven crimes, IoT vulnerabilities, and ransom ware.Introducing specific legal provisions that account for these emerging technologies would help Nigeria stay ahead of sophisticated cybercriminal tactics.

6.3.6. Improving Data Protection Standards: Strengthening the enforcement of the NDPR and introducing provisions similar to the EU's *General Data Protection Regulation (GDPR)* would enhance data privacy and contribute to preventing cybercrimes that exploit personal data.Rigorous data protection is fundamental to cybercrime regulation, as it deters data breaches and strengthens trust in digital infrastructure.

Reference

1. United Nations, *Universal Declaration of Human Rights*, 1948. [Online]. Available: https://www.un.org/en/about-us/universal-declaration-of-human-rights
2. United Nations, *International Covenant on Civil and Political Rights*, 1966. [Online]. Available: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
3. U.N. Human Rights Committee, *General Comment No. 34 on Article 19: Freedoms of opinion and expression*, CCPR/C/GC/34, 2011.
4. European Court of Human Rights, *Handyside v. The United Kingdom*, App. No. 5493/72, judgment of Dec. 7, 1976.
5. European Court of Human Rights, *Delfi AS v. Estonia*, App. No. 64569/09, judgment of June 16, 2015.
6. Economic Community of West African States (ECOWAS) Court of Justice, *SERAP v. Federal Republic of Nigeria*, Judgment No. ECW/CCJ/APP/09/17, 2020.
7. Council of Europe, *Convention on Cybercrime (Budapest Convention)*, ETS No. 185, Budapest, 2001.
8. Federal Republic of Nigeria, *Cybercrimes (Prohibition, Prevention, etc.) Act*, 2015.
9. Supreme Court of the United States, *Elonis v. United States*, 575 U.S. 723, 2015.
10. United Kingdom, *Protection from Harassment Act 1997*, amended by *Protection of Freedoms Act 2012*.
11. Government of India, *Information Technology Act*, 2000.
12. Supreme Court of India, *Shreya Singhal v. Union of India*, Writ Petition (Criminal) No. 167 of 2012, March 24, 2015.
13. European Commission, "Proposal for a Directive on combating violence against women and domestic violence," COM (2022) 105 final, Mar. 8, 2022.
14. Australian Government, *Enhancing Online Safety Act*, 2015. [Online]. Available: https://www.legislation.gov.au/Details/C2015A00024
15. German Bundestag, *Network Enforcement Act (NetzDG)*, 2017. [Online]. Available: https://www.bmj.de/EN/Ministry/NetworkEnforcementAct/NetworkEnforcementAct_node.html