

# Exploring the Intersection between Nigeria's Cyber policy and National Security: An Examination of International Cooperation, Legal Frameworks and Regulatory Compliance

Amaefule I. A<sup>1</sup>, Henry C. Alisigwe<sup>2</sup>, Ubochi C.I<sup>3</sup>

<sup>1&3</sup>*Department of Computer Science, Imo State University, Owerri, Imo State Nigeria.*

<sup>2</sup>*Faculty of Law, Imo State University, Owerri, Imo State Nigeria*

## Abstract

Nigeria's cybersecurity landscape is a pressing concern, with significant implications for national security and economic stability. This study provides an in-depth analysis of the intersection of Nigeria's cyber policy and national security, focusing on international cooperation, legal frameworks, and regulatory compliance. The country's increasing reliance on digital technologies has exposed it to a range of cyber threats, including AI-driven phishing, ransomware attacks, and data breaches, resulting in estimated losses of \$500 million (N250 billion) in the last two years. The study examines Nigeria's efforts to combat cyber threats, protect critical infrastructure, and promote a secure digital environment. The National Cybersecurity Policy and Strategy (NCPS) and the Cybercrime Prevention Act are key initiatives, but gaps in legislative frameworks, insufficient public awareness, and inadequate infrastructure hinder their effectiveness. This research highlights the importance of robust cybersecurity measures, effective law enforcement, and public-private partnerships in safeguarding national interests. It identifies key threats, including AI-driven phishing (increased by over 70%), ransomware attacks (12-15% of incidents), and data breaches (government systems accounted for 8-10% of incidents). The study offers insights into the challenges and opportunities in enhancing cybersecurity and promoting national security in the digital age. It recommends capacity building, research and development, and public awareness to mitigate cyber risks and ensure economic stability. International cooperation, leveraging emerging technologies, and regulatory compliance are also crucial for protecting Nigeria's critical infrastructure and promoting a secure digital environment.

**Keywords:** Cybersecurity, Legal framework, Regulatory compliance, Cyber policy, National security, International cooperation.

## A. INTRODUCTION

Nigeria's increasing reliance on digital technologies has created new opportunities for economic growth, social development and governance. However, this digital transformation has also exposed the country to a range of cyber threat, including hacking, phishing, ransomware attacks and identify theft. These threats have significant implications for national security, economic stability and the privacy and security of citizens data. [1]. In the digital age, the security of a nation is no longer solely dependent on its military prowess or territorial integrity. The rapid evolution of technology has introduced new dimensions to national security with cyber threat emerging as a significant concern for government worldwide [2]. Nigeria like many other countries, is grappling with the challenges of protecting its digital infrastructure, ensuring the privacy and security of its citizens' data and safeguarding its national interest in the face of an ever-evolving cyber threat landscape. [3].

The Intersection between cyber policy and national security is complex and multifaceted. Effective cybersecurity measures are essential for protecting critical infrastructure, preventing economic espionage and ensuring the continuity of government services. However, the development and implementation of cyber policies that balance security needs with the protection of individual rights and freedoms pose significant challenges.

The rapid evolution of technology has brought about significant benefits to Nigeria but it has also exposed the country to a myriad of cyber threats that impact its national security and economic stability. As a result, the Nigerian government has formulated various policies and strategies to address these challenges, including the National Cybersecurity policy and strategy [4]. However, despite these efforts, Nigeria's cybersecurity landscape remains growing concerns with numerous cyber threats posing significant risks to the country's critical infrastructure, economy and citizens.

The study seeks to examine the current state of cybersecurity in Nigeria, analyze the country's cyber policy framework and identify areas for improvement. By exploring the intersection of cyber policy and national security, this research aims to contribute to the development of effective strategies for enhancing Nigeria's Cybersecurity posture and protecting its national interest in the digital age.

## B. LITERATURE REVIEW

The Nigeria's cybersecurity landscape is characterized by numerous challenges, including an inadequate legislative framework, insufficient public awareness and training, corruption and inadequate infrastructure [5]. These challenges are further compounded by the rapidly evolving nature of cyber threats, which requires a proactive and coordinated response from government agencies, private sector organizations, and civil society.

Nigeria's cyber policy intersects with national security through the cybercrime Act 2015; the National Cybersecurity Policy and Strategy and data protection regulations, but faces flaws such as inconsistent implementation, insufficient skilled personnel, inadequate infrastructure and so on. These shortcomings leave critical sector vulnerable to increasingly sophisticated threat like AI-powered attacks and crypto scams which undermine national security and hinder digital development efforts.

International cooperation is crucial in combating cyber threats, as cyber attacks can originate from anywhere in the world. Collaboration between countries can facilitates information sharing, capacity building and joint investigations. Microsoft's operation against Raccoon 0365 in September 2025, where Microsoft seized 340 websites linked to a Nigeria-base phishing services, Raccoon 0365, which had generated over \$100.000 in cryptocurrency payments since July 2024. This operation demonstrates the importance of international cooperation in disrupting cybercrime operation [6].

Nigeria's legal framework for cybersecurity and national security is primarily governed by the Cybercrime (Prohibition, Prevention and Punishment) Amendment Act. Which was signed into law on 28<sup>th</sup> February 2024. This Act provides a comprehensive framework for prohibiting, preventing, detecting, prosecuting and punishing cybercrimes, but comes with a lot of challenges. The Act was designed to combat cybercrime, but its effectiveness is hindered by lack of sufficient manpower by security agencies, equipment and funding which hinders their ability to respond effectively to security threats. Also, corruption in security agencies undermines the enforcement of laws and erodes public trust, leading to compromised investigation and lack of accountability [7].

The National Cybersecurity Policy and Strategy 2014; aims to safeguard critical information infrastructure but its implementation is affected by poor coordination among security agencies, resulting in disjointed approaches to law enforcement, leading to gaps in intelligence sharing and hindering of comprehensive responses to security challenges. Again, Nigeria Data Protection Regulation (NDPR) 2019; emphasizes data protection, but organization struggles to comply due to inadequate resources, lack of necessary training and capacity-building programs to deal with modern security challenges such as cybercrimes and terrorism [8].

Nigeria's regulatory compliance frameworks for cybersecurity faces several challenges that hinder effective enforcement of security measures. Many organization and individuals underestimate the scale of potential cyber threat, resulting in insufficient investment in protective measures. Again, outdated technology and legacy systems leave vulnerabilities that malicious actor can exploit, undermining regulatory compliance. Budgetary constraints hamper regulatory bodies ability to conduct thorough inspections or provide necessary training and resources. Finally, small and medium sized enterprise (SMEs) struggle to allocate budget for cybersecurity, unaware that compliance can safeguard their operation and reputation [7].

### C. INTERNATIONAL COOPERATION

Cooperation with international organization and countries can facilitate information sharing, capacity building and joint investigation which plays a vital role in enhancing Nigeria cyber policy and national security [9]. Engaging various stakeholders, such as industry expert, academia, private sector and civil society can enhance cybersecurity awareness, training and incident response and foster a comprehensive approach to cybersecurity; like the operation which involved the collaboration of US District court in Manhattan, the Health Information Sharing and Analysis Center (Health- ISAC) and Cloudflare, that disrupt cybercrime operation where 340 websites linked to a Nigeria-based phishing service were seized; demonstrating the importance of international cooperation [6].

- a. **Global Partnership:** The Nigeria's cybersecurity efforts can be enhanced through global partnerships. The National Cybersecurity Policy and Strategy emphasizes the importance of partnership to combat threat and protect national interest. Collaboration with international organizations and countries to share best practices, intelligence, awareness, expertise in incident response and facilitate capacity building can enable Nigerians to take proactive measures to protect themselves and their organization from cyber threats. This collaboration facilitates the development of robust cybersecurity ecosystem that can support Nigeria's economic and national development goals [9].
- b. **Treaties and Conventions:** Treaties and conventions play a crucial role in shaping global cybersecurity standard and practices. Nigeria cyber policy and national security are influenced by various international treaties and conventions; these agreements provide a framework for cooperation and information sharing to combat cyber threats. Nigeria is involved in several key treaties and convention related to cybersecurity; some of the notable ones include Africa Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention). Adopted in 2014, this Convention aims to address regulatory challenges posed by increasing cybercrime on the continent. Although, Nigeria has not ratified it yet, but the country has taken steps to enact data protection regulations such as the Nigeria Data Protection Regulation (NDPR) in 2019 and Nigeria Data Protection Act 2023. Another convention is United Nations Convention against Transnational Organized Crime adopted by General Assembly Resolution 55/25 of 15 November 2000; which Nigeria ratified in 2001. It includes provisions against cybercrime [10]. However, the rapidly evolving nature of cyber threats requires treaties and conventions to be regularly updated and adapted.
- c. **Information Sharing:** Nigeria's cyber policy and national security are significantly influenced by its involvement in international information sharing with global communities. This cooperation is crucial in combating cyber threat and enhancing the country's cybersecurity capabilities. Nigeria has developed a comprehensive policy and strategy to address cybersecurity challenges which include collaboration with international partners. The Cybercrime (Prohibition, Prevention and Punishment) Amendment Act 2014; establishes a framework for preventing, detecting and prosecuting cybercrime in Nigeria with international cooperation. Nigeria engages with international organizations and communities to share knowledge, best practices and threat intelligence to combat cyber threats. This international cooperation enables Nigeria to stay informed about emerging threats and vulnerabilities, improved incident response and facilitates training and capacity-building initiatives. However, the office of the National Security Adviser; serves as the coordinating body for cybersecurity and cybercrime issues; working closely with international partners to share information and best practices. Although, Nigeria faces challenges in terms of resources, expertise and infrastructure to effectively combat cyber threats; but by leveraging international information sharing and cooperation, Nigeria can strengthen its cybersecurity posture and contribute to global efforts to combat cyber threats [11], [9].

### D. LEGAL FRAMEWORKS

Nigeria aligns its cybersecurity regulations with international standards, such as the NIST Cybersecurity Framework, to enhance its national security and promote a secure digital environment. The country is also a signatory to various treaties and conventions that promote cooperative action against cyber threats. Nigeria's legal framework for cybersecurity is comprehensive with several key laws and regulation in place to combat cybercrime and protect personal data. The Nigeria's cyber policy and national security are governed by several key legal frameworks which includes [12], [13], [7].

- i. Cybercrime (Prohibition, Prevention and Punishment) Act 2015;** This Act was amended by the Cybercrime (Prohibition, Prevention and Punishment) Amendment Act 2024. This Act is the primary legal framework for prosecuting cyber-related offences including's unauthorized access to computer systems, identity theft, and cyber stalling. It bolsters efforts to prevent and respond to cyber threats affecting individual, businesses and government entities. The Act also provides for international cooperation in combating cybercrime [7]. The Cybercrime (Prohibition, Prevention, etc.) Act 2015 is a landmark legislation in Nigeria, establishing a comprehensive framework for governing cybercrimes and promoting cybersecurity. This Act is the first of its kind in Nigeria, specifically addressing the growing concerns of cybercrimes and cybersecurity threats. The Act provides a robust framework for protecting computer systems, networks, electronic communications, data, and intellectual property. It outlines stringent penalties for various cybercrimes, including cyber-terrorism, unlawful access to computer systems, and sales of preregistered SIM cards, among others. Despite its significance, experts have expressed mixed views on the effectiveness of the Act. Some of the limitations include ambiguity in certain provisions, lack of decisive roles for implementing agencies, and inadequate modern tools of surveillance. These shortcomings have hindered the Act's ability to prevent cybercrimes, highlighting the need for further reforms and improvements [14].
- ii. National Cybersecurity Policy and Strategy 2014;** This policy outlines the broader framework for cybersecurity governance in Nigeria, aiming to safeguard the nation's critical information infrastructure, promote awareness and foster a collaboration approach among stakeholders [12], [13], [7]. Another version of the National Cybersecurity Policy and Strategy Unveiled in February 2021; represents a significant milestone in Nigeria's pursuit of a secure and resilient digital landscape. This comprehensive policy serves as the overarching framework guiding Nigeria's cybersecurity efforts towards achieving its national objectives. The policy is a meticulously crafted, living document that outlines a clear roadmap for realizing Nigeria's cybersecurity vision. This vision is ambitious yet straightforward: "a safe and secure digital community that provides opportunities for its citizenry and promotes peaceful and proactive engagements in cyberspace for enhanced national prosperity." To achieve this vision, the policy sets forth a mission to "foster a trusted cyber environment that optimizes Nigeria's cybersecurity readiness and coordination capacities towards addressing the nation's cyber risk exposure." At its core, the National Cybersecurity Policy and Strategy 2021 is a convergence of goals, approaches, and resources, articulating the collective efforts of all stakeholders involved in Nigeria's cybersecurity landscape. The policy establishes a robust foundation for the Nigeria National Cybersecurity Programme, anchoring it on eight critical pillars. These pillars are designed to provide a structured approach to addressing the multifaceted challenges of cybersecurity, ensuring that Nigeria is well-equipped to navigate the complexities of the digital age and safeguard its national interests.



National Cybersecurity Policy and Strategy 2021 [15].

**Figure 1:** Eight 8 Pillars to form the support for National Cybersecurity Programme

The National Cybersecurity Policy and Strategy 2021 also places significant emphasis on enhancing incident response capabilities, recognizing that timely and effective responses are crucial in mitigating the impact of cyber threats. Furthermore, the policy underscores the importance of fostering international cooperation, acknowledging that cyber threats transcend national borders and require collaborative efforts to combat. Despite these commendable efforts, the study reveals that Nigeria's cybersecurity posture remains vulnerable due to several challenges. One of the major concerns is the restricted enforcement of cybersecurity regulations, which undermines the effectiveness of the policy. Additionally, there is a pressing need for increased cybersecurity awareness among citizens and organizations, as a lack of awareness can lead to unintentional vulnerabilities and security breaches. Moreover, the study highlights a significant scarcity of trained cybersecurity professionals, which hampers Nigeria's ability to respond to and manage cyber threats effectively. The shortage of skilled personnel is a critical issue that needs to be addressed to strengthen the country's cybersecurity capabilities. The study also identifies deficiencies in cooperation among critical agencies, which can lead to fragmented responses to cyber threats and compromise the overall security posture. Inadequate information sharing and coordination among agencies can result in delayed responses, allowing threats to escalate and cause more damage. Lastly, unreliable reporting of cyberattacks is another challenge that undermines Nigeria's cybersecurity efforts. Underreporting or inaccurate reporting of cyber incidents can lead to a lack of understanding of the threat landscape, making it difficult to develop effective countermeasures. Addressing these challenges will be crucial to strengthening Nigeria's cybersecurity posture and protecting its digital infrastructure from evolving cyber threats [16].

- iii. **Nigeria Data Protection Act (NDPA – 2023);** Is a comprehensive law that safeguard personal data and promotes a culture of transparency and accountability in handling sensitive information. This Act establishes a framework for data protection and introduces changes to the existing regulatory framework, including the creation of the Nigeria Data Protection Commission which oversees data protection and privacy issues [17]. As Nigeria solidifies its position in the global digital economy and expands its tech ecosystem, the Nigeria Data Protection Act (NDPA) 2023 underscores the country's commitment to safeguarding citizens' personal data, aligning with international data protection standards. This Act introduces notable provisions, including a new classification system for data controllers and processors deemed "of major importance," which come with specific obligations. Additionally, it provides broader protections for certain exempt processing activities, striking a balance between data protection and

operational needs. A significant achievement of the NDPA is resolving the long-standing uncertainty around Nigeria's primary data protection regulator, clarifying institutional authority and paving the way for more effective data protection practices. Overall, the Act marks a major milestone in Nigeria's data protection journey, enhancing trust in the country's digital economy [18].

- iv. **Nigeria Data protection Regulations (NDPR – 2019);** This regulation seamlessly incorporates key elements of the General Data Protection Regulation (GDPR), a gold standard in data protection, to bolster the safeguarding of personal information within Nigeria's digital landscape. At its core, the regulation underscores the importance of upholding fundamental data protection principles, ensuring that personal data is handled in a manner that respects individuals' rights and maintains transparency. A cornerstone of this regulation is the emphasis on consent, recognizing that individuals must be empowered to make informed decisions about their data. It meticulously outlines the rights of data subjects, providing them with greater control over their personal information and how it is used. To ensure these protections are more than theoretical, the regulation establishes robust enforcement mechanisms. These mechanisms are designed to hold accountable those who fail to comply with the stipulated data protection standards, thereby fostering a culture of accountability and respect for data privacy. By integrating these GDPR-inspired provisions, Nigeria strengthens its data protection framework, aligning itself with global best practices and enhancing trust in its digital ecosystem.

#### E. REGULATING BODIES

Regulating bodies play a crucial role in protecting individuals, organizations and nations from cyber threat. The primary purpose is to establish guidelines, regulation and standards for cybersecurity practices ensuring consistency and best practices across industries. They monitor and enforce compliance with cybersecurity regulation, investigating incidents and imposing penalties for non-compliance. Some of this regulatory bodies includes.

- a. Nigeria Computer Emergency Response Team (ngCERT); which responds to cybersecurity incidents, offers guidance on best practices and provides resources for capacity building.
- b. National Information Technology Development Agency (NITDA); which regulates and develops information technology in Nigeria and also promote cybersecurity awareness and best practices
- c. Nigerian Communication Commission (NCC); It regulate the telecommunication sector, securing telecommunication networks against cyber threats.
- d. Cybercrime Advisory Council: - Coordinates efforts to prevent and combat cybercrimes, and promoting cybersecurity in Nigeria [19].

These regulatory bodies play a vital role in ensuring the security and integrity of digital system environment, enhanced cybersecurity, ensuring consistency and trust, improved incident response and promotes cybersecurity awareness and education; which helps individuals and organization understand and mitigate cyber risks.

#### F. REGULATORY COMPLIANCE

Regulatory compliance is critical to ensure the protection of sensitive information and critical infrastructure. It refers to the process of ensuring that an organization adheres to relevant laws, regulations and standard that govern its operations. These include familiarizing oneself with relevant laws, regulation and standards, implementing policies and procedures, training and awareness, monitoring and reporting, and continuous improvement. Regulatory compliance is essential for organizations to avoid legal and financial penalties, protect reputation and brand, ensure business continuity and build trust with stakeholders. Relevant regulations and frameworks for Nigeria includes

- Nigeria Data protection Act (NDPA)
- Cybercrime (Prohibition and Prevention) Act
- NIST Cybersecurity Framework
- ISO 27001
- Payment Card Industry Data Security Standards (PCI DSS)

- a. **Required Security Measures:** To ensure regulatory compliance for cyber policy and national security in Nigeria, organizations should implement the following security measures [20], [21], [22].
- i. **Data Protection:** implementing robust data protection protocols to safeguard sensitive information from unauthorized access. Ensuring encryption of personal data, both at rest and transit and also conducting regular data protection impacts assessments to identify potential risks.
  - ii. **Access Control:** Establishing strict access controls, including multi-factor authentication and least privilege principles; limit access to sensitive data and systems to authorized person only; and equally reviewing and updating access controls to reflect changes in personnel or roles regularly.
  - iii. **Incident Response:** Develop and implement a comprehensive incident response plan to manage cybersecurity incidents. Also establishing procedures for prompt incident reporting to relevant authorities such as the National Computer Emergency Response Teams (CERT) Coordination Centre and conducting regular training and exercises to ensure effective incident response.
  - iv. **Risk Management:** Conducting regular risk assessments to identify vulnerabilities and potential threats and implementing measures to mitigate identified risk and monitor their effectiveness. Additionally, review and update risk management plan to address emerging threats continuously.
  - v. **Compliance and Audits:** Engage with external auditors to assess the effectiveness of security measures and identify areas for improvement; conduct regular compliance audits to ensure adherence to relevant regulations and standards and equally maintaining detailed records of compliance activities and audit findings.
  - vi. **Security Awareness and Training:** Provide regular security awareness training for employees and stakeholders, ensuring that personnel understand their roles and responsibilities in maintaining cybersecurity. Organization should conduct phishing simulations and other training exercises to test employee's awareness and response.
  - vii. **Network Security:** Organization should implement robust network security measures, including firewalls, intrusion detection systems and secure network protocols. They should also conduct regular network vulnerability assessments and penetration testing to identify potential weaknesses and ensure that network security measures are aligned with relevant regulations and standards.

By implementing these security measures and adhering to relevant regulations, organization can ensure regulatory compliance and maintain a robust cybersecurity posture to protect against emerging threats [23], [24].

- b. **Breach Reporting Obligations:** Breach reporting obligation for regulatory compliance in cyber policy and national security involve notifying the relevant authorities about security incidents. They are governed by various laws and regulations which include: **Nigeria Data Protection Act (NDPA)**, which mandates breach reporting and imposes fines for non-compliance; **Nigeria Data Protection Regulation (NDPR)**, which provides guidelines for data protection and beach reporting and **Cybercrimes (Prohibition and Prevention) Act**, that requires reporting of cyber incidents to the National CERT within 72 hours of detection.
- i. **Data Breach Notification:** Data controllers or processors must notify the Nigeria Data Protection Commission (NDPC) within 72 hours of becoming aware of a breach, as stipulated in Section 40 of the Nigeria Data Protection Act [25], [20].
  - ii. **Notification Contents:** The report should include details about the breach, such as the nature of the breach, data affected and measures taken to address the breach [7].

- iii. **Notification to Data Subjects:** If the breach poses a high risk to data subjects right and freedoms, they must be notified promptly in clear and straight forward language.
- c. **Penalties for Non-Compliance:** Penalties for non-compliance with regulatory requirement for cyber policy and national security includes [20], [25].
- i. **Financial Penalties**
    - **Data Protection:** 2% of annual gross revenue or 10 million naira, whichever is greater, for data controllers or processors of major importance who fail to comply with data protection regulations
    - **Cybercrime Act:** fine ranges from 1million naira to 7 million naira and imprisonment terms of up to 7 years for various cyber-related offenses.
  - ii. **Denial of Internet Services:** Organizations or individuals who fail to report cyber incidents to the National CERT within 72 hours of detection may be denied internet services and fined 2 million naira.
  - iii. **Reputational Damage:** Non-compliance can lead to reputational damage, loss of trust and potential legal action.
  - iv. **Other Consequences:** Organization may also face corrective actions such as rectification of non-compliant practices, payment of compensation to affected data subjects and accounting for profits realized from non-compliant activities.

## G. ESSENTIAL CONSIDERATION

Critical consideration organizations should adhere to, in ensuring national security includes

- a. **Capacity Building:** Establishing a dedicated cybersecurity institution such as the National Computer Forensics Laboratory, to enhance the country's capacity to respond to cyber threats; also enhancing the capacity of regulatory bodies, law enforcement agencies and organizations to implement and enforce cybersecurity regulations effectively through: -
  - i. **Cybersecurity Skill Development:** Integrating cybersecurity education into school curricula and provide training programs for professionals, focusing on developing skills in threat analysis, incident response and cybersecurity governance is very crucial in enhancing national security, economic stability and protection against cyber threats.
  - ii. **Public Awareness:** Conducting consumer sensitization campaigns to promote cybersecurity awareness and best practices among citizens, businesses and government agencies is also a vital consideration.
  - iii. **Research and Development:** Encourage research and development in cybersecurity to stay ahead of emerging threats with focus on areas like AI-Powered threat detection and automated security solutions [26], [9], [27].
- b. **Public – Private Partnership:** Fostering collaboration between government agencies, private sector and academia to develop cybersecurity capacity, promote information sharing by facilitating the exchange of threat intelligence and best practices between government and private sector entities drive innovations. Collaborating on research and development initiatives to develop new cybersecurity technologies and coordinating incidents response effort; creating more resilient and secure cyber environment ensures national security and economic stability. [28], [29]
- c. **Emerging Technologies:** Are transforming cyber policy and national security landscape [30].

- i. **Artificial Intelligence (AI):** AI is being used to detect and respond to cyber threat in real-time with nations integrating AI into their cybersecurity strategies.
- ii. **Quantum Computing:** poses significant risk to current encryption methods and countries are working to develop quantum-resistant cryptography.
- iii. **Blockchain:** Blockchain technology is being explored to enhance cybersecurity, particularly in financial transactions and data protection.
- iv. **Internet of Things (IoT):** IoT devices increase the attack surface and countries are developing policies to ensure secure IoT deployment.
- v. **5G Networks:** 5G networks offers high-speed connectivity but also introduce new cybersecurity risk and nations are working to ensures robust security protocol.

## H. NATIONAL SECURITY IMPLICATIONS

Cyber security threats are major concern for Nigeria's national security. This is moreso given the recent claims of tapping into the phone conversation of the National Security Adviser by an opposition party stalwart during a live TV interview; with the country experiencing an average of 4,200 cyber attacks per week; higher than the continental average of 3,153 and 60% above the global baseline of 1,963 attacks per organization per weeks. These attacks target critical national infrastructure including oil pipelines, communication installation, hospitals and military facilities, posing a significant threat to economic stability and national defense. This alarming trend, highlights the need for robust cybersecurity measures to protect the country's digital infrastructure. [31]

- a. **Threat Landscape:** Nigeria cyber threat landscape is quite concerning with 37 – 42% increase in reported cyber incidents in 2025 compared to the previous year, driven by AI-scaled threats and digitalization of enterprise systems. The financial sector is hardest hit, accounting for 55-60% of total national cyber losses mainly due to unauthorized transfer, card-not-present fraud and API compromise. Key threats include
  - i. **AI-driven Phishing:** Increased by over 70% with convincing emails, voice clone and deep fake video impersonation.
  - ii. **Ransomware Attacks:** Represented 12-15% of incidents, with energy and logistics assets experiencing a 62% year-on-year increase.
  - iii. **Data Breaches:** Government systems accounted for 8-10% of incidents with weak identity management and outdated systems being primary drivers.
  - iv. **Insider Threats:** Represented 10-12% of incidents with malicious insider collusion linked to financial fraud and resale on the dark web. [32]
- b. **Critical Infrastructure Protection:** is a top priority for Nigeria's national security and cyber policy. The country's digital economy and essential services rely heavily on secure and resilient infrastructure, making it a prime target for cyber threats. Critical infrastructure protection is crucial for Nigeria's economic stability, national security and public safety. [33]; why critical infrastructure protection matters
  - i. **Economic Stability:** protect financial institutions, power grids and transportation system, ensuring uninterrupted economic activity. Cyber attacks can disrupt financial institution and the economy, leading to significant losses.
  - ii. **National Security:** Safeguards critical infrastructure from cyber threats, preventing disruptions that could compromise national defense.
  - iii. **Public Safety and Trust:** Ensures essential services like health care, water and emergency services remains operational. Breaches can erode confidence in digital systems and government services

- c. **Economic Implication:** Cyber security threats are having a significant impact on Nigeria's economy and national security; with cybercrime costing the country an estimated 500 million dollars (250 billion naira) in the last two years. [34], [31], [35]; The rise in cyber threats has led to increased financial losses, compromised national security and erosion of public trust in digital systems. Key Economic Implication
- i. **Financial Losses:** Cyber attacks have resulted in significance financial losses, with Nigeria ranking third in Africa for ransomware threat detection in 2024
  - ii. **Economic Instability:** Cyber Threats undermine economic stability deterring investment and hindering digital growth.
  - iii. **National Security Risks:** Cyber attacks compromise critical infrastructure, threatening national security and public safety

## I. CONCLUSION

Nigeria's cybersecurity landscape is a growing concern, with the country facing numerous cyber threats that impacts its national security and economic stability. The country's increasing reliance on digital technologies has exposed it to a range of cyber threats, including AI-driven phishing, ransomware attacks, and data breaches. These threats compromise critical infrastructure, undermine economic growth, and erode public trust in digital systems. To address these challenges, Nigeria must prioritize robust cybersecurity measures, effective law enforcement, and public-private partnerships. The country's cyber policy framework, including the National Cybersecurity Policy and Strategy, the Cybercrime Prevention Act, and international cooperation, is a step in the right direction. However, more needs to be done to address gaps in legislative frameworks, insufficient public awareness, and inadequate infrastructure. Capacity building, research and development, and public awareness are essential for enhancing Nigeria's cybersecurity posture. The country must also leverage emerging technologies like AI and blockchain to stay ahead of evolving cyber threats. Ultimately, protecting Nigeria's critical infrastructure and promoting a secure digital environment requires a collaborative effort from government agencies, private sector organizations, and civil society. By working together, Nigeria can mitigate cyber risks, ensure economic stability, and safeguard national security in the digital age.

## ACKNOWLEDGMENT

We express our heartfelt appreciation to TetFund for their financial support, which enabled the successful completion of this study. We also acknowledge the Vice Chancellor of Imo State University Owerri, for fostering a collaborative research environment at the university.

## REFERENCES

- [1] Digital Watch Observatory (2019). Nigeria's National Digital Economy Policy and Strategy 2020-2030: <https://dig.watch/resource/nigerias-national-digital-economy-policy-and-strategy-2020-2030>
- [2] (Kshetri N (2019). Cybersecurity in Nigeria: Challenges and Opportunities. Journal of Cybersecurity 5(1), 1- 12.
- [3] ENISA (European Union Agency for Cybersecurity) Threat Landscape (2020): Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected | ENISA <https://share.google/M4uVNs0XLjVJBRcoY>
- [4] (NCPS 2021). National Cybersecurity Policy and Strategy. <https://cybersecfill.com/nigeria-cybersecurity-strategy/>
- [5] Ojedokun A.O (2020). Cybersecurity in Nigeria: A Review of the literature. Journal of Cybersecurity 6(1), pp. 1-15.

- [6] Vicens A.J (2025) Microsoft Seizes 340 Website linked to growing phishing Subscription service. Microsoft News Center: <https://www.reuters.com/sustainability/boards-policy-regulation/microsoft-seizes-340-websites-linked-growing-phishing-subscription-service-2025-09-16/>
- [7] Generis Global Legal services 2024. (Understanding Cybersecurity Regulations in Nigeria: Key Measures and Compliance 2024): <https://generisonline.com/understanding-cybersecurity-regulations-in-nigeria-key-measures-and-compliance/>
- [8] Atoyebi O.M (SAN) 2024. The potency of extant law regulating Security in Nigeria: <https://omaplex.com.ng/the-potency-of-extant-laws-regulating-security-in-nigeria/>
- [9] Adewunmi j. Falode Cyber security policy in Nigeria: A tool for National Security and Economic Prosperity). [https://ebrary.net/173537/political\\_science/cybersecurity\\_policy\\_nigeria\\_tool\\_national\\_security\\_economic\\_prosperity](https://ebrary.net/173537/political_science/cybersecurity_policy_nigeria_tool_national_security_economic_prosperity)
- [10] (Cybersecurity and Cybercrime in Africa: Continental and Regional Policies 2021. <https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/cybersecurity-cybercrime-africa-continental-regional-policies/>
- [11] Olisa Agbakoba (2021). Cybercrimes and Cyber laws in Nigeria: All you Need to Know. <https://www.mondaq.com/nigeria/security/1088292/cybercrimes-and-cyber-laws-in-nigeria-all-you-need-to-know>
- [12] 1st Attorneys Law Articles (2023) cybercrime and Data Protection in Nigeria: Legal Implications and Safeguarding Measures: <https://1stattorneys.com/articles/2023/08/01/cybercrime-and-data-protection-in-nigeria-legal-implications-and-safeguarding-measures/>
- [13] Cybercrime Act – Legal Framework for Cybercrimes in Nigeria: <https://wigweandpartners.com/the-legal-framework-for-cyber-crimes-in-nigeria/#:~:text=The%20Cybercrime%20Act%20is%20a%20cornerstone%20of%20Nigeria%E2%80%99s,forms%20of%20cybercrimes%20as%20stated%20in%20the%20Act>
- [14] Chen Yizhen (2025). Cybersecurity in Nigeria: Emerging issues, domestic governance and international cooperation. World Journal of Advanced Research and Reviews, 2025, 26(02), 935-942. DOI: <https://doi.org/10.30574/wjarr.2025.26.2.1687>
- [15] Nigerian Communications Commission. National Cybersecurity Policy and Strategy 2021. February (2021). <https://ncc.gov.ng/media/800/view>.
- [16] Gana IM, Ibrahim AF, Oluwaseyi WA, Wali AI. (2024). Cyber Warfare and National Security in Nigeria: Threats and Responses. Kwararafa Security Review. 2024; 1(2):8.
- [17] LawCare: (2025). Nigeria Data Protection Act 2023. <https://lawcarenigeria.com/nigeria-data-protection-act-2023/>
- [18] King M. (2023). Nigeria's New Data Protection Act, Explained. Future of Privacy Forum. June 28, 2023. <https://fpf.org/blog/nigerias-new-data-protection-act-explained/>.
- [19] Nigerian Lawyer Center.com (2023). Important Cybersecurity Laws and Regulations in Nigeria. <https://nigerianlawyerscenter.com/blog/important-cybersecurity-laws-and-regulations-in-nigeria/>
- [20] S.P.A Ajibade and Co. 2025. Cybersecurity Laws and Regulations Nigeria. <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/nigeria>

- [21] Dov Goldman (2025). What are the Best Practices for Security Compliance: What is Security Compliance. <https://panorays.com/blog/what-is-security-compliance/>
- [22] Cybersecurity Policies and Regulatory Compliance 2024. <https://online.yu.edu/katz/blog/cybersecurity-policies-and-regulatory-compliance>
- [23] Leah Sadoian (2025) Ultimate List of Cybersecurity Regulations by Industry. <https://www.upguard.com/blog/cybersecurity-regulations-by-industry>
- [24] Novatia Consulting (2024). Cybersecurity Regulatory Compliance in Nigeria/ Novatia Consulting. <https://novatiaconsulting.com/cybersecurity-regulatory-compliance-in-nigeria/>
- [25] Udo Udoma and Belo-Osagie (2025). Data Protection Laws and Regulation Nigeria 2025. <https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria>
- [26] Moyosore Kukoyi (2025). The Role of Cybersecurity in National Security, Economic Stability. <https://www.vanguardngr.com/2025/02/the-role-of-cybersecurity-in-national-security-economic-stability-moyosore-kukoyi/>
- [27] Ahmed Abubakar Aliyu (2024). A Multi-Pronged Framework for a Cyber-Secure Nigeria. Scientific and Practical Cyber security Journal (SPCSJ) 8(1): 69 -75; ISSN 2587 4667. Scientific Cyber Security Association (SCSA).
- [28] Quadrant Four (2025). Building Trust and Transparency in public – private Partnership: A Framework for Success. <https://quadrantfour.com/perspective/building-trust-and-transparency-in-public-private-partnerships-a-framework-for-success>
- [29] Cyber Security and Infrastructure Security Agency (2024). Partnership and Collaboration. <https://www.cisa.gov/topics/partnerships-and-collaboration>
- [30] Radanliev, P. (2025). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. Journal of Cyber Security Technology, 9(1), 28-78. <https://doi.org/10.1080/23742917.2024.2312671>
- [31] Kayode Adebisi (2025). Cybersecurity and Nigeria's Unpleasant Record. <https://businessday.ng/features/article/cybersecurity-and-nigerias-unpleasant-record/>
- [32] Ben Awoks (2025). Nigeria's 2025 Cyber Threat Landscape from BEC to AI-Driven Attacks. <https://benawoks.substack.com/p/nigerias-2025-cyber-threat-landscape>
- [33] Mojisola Ojuri (2024). How Cyber security Governance Protects National Infrastructure in Nigeria and Beyond. <https://www.vanguardngr.com/2024/07/how-cybersecurity-governance-protects-national-infrastructure-in-nigeria-and-beyond/>
- [34] Emma Okonji (2025) Experts: Nigeria Need Unified Sovereign Cybersecurity Strategy to Address Rising Cyberspace Threats. <https://www.thisdaylive.com/2025/07/03/experts-nigeria-needs-unified-sovereign-cybersecurity-strategy-to-address-rising-cyberspace-threats/>
- [35] Olisa Agbakoba (2025). Legal Implications of Ransomware in Nigeria: Legal Risk, Regulatory Duties and Cybersecurity Compliance. <https://www.mondaq.com/nigeria/security/1691386/legal-implications-of-ransomware-in-nigeria-legal-risks-regulatory-duties-and-cybersecurity-compliance>