World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Cybersecurity in Nigeria: Emerging issues, domestic governance and international cooperation

Chen Yizhen *

Institute of African Studies (College of African Area and Country Studies), Zhejiang Normal University, Jinhua, China.

World Journal of Advanced Research and Reviews, 2025, 26(02), 935-942

Publication history: Received on 28 March 2025; revised on 05 May 2025; accepted on 08 May 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.2.1687

Abstract

Driven by factors such as digitization, advanced technology, large telecom operators, internet penetration, and government initiatives, Nigeria is regarded as Africa's largest information and communications technology (ICT) market. Cyberspace presents significant opportunities that enhance communication, and boost business and socio-economic prosperity in Nigeria. At the same time, as a major economy in Africa, Nigeria faces complex and diverse challenges in terms of cybersecurity. While cyber criminals thrive to exploit any vulnerability for their gains, the Nigeria Government has taken some measures to safeguard its cyberspace. This study used secondary source methodology by referring previous and related research works including books, articles, news among others, evaluated the efforts of the Nigeria Government in the coordination of cybersecurity in the country and cooperation with the major cyberpowers in the world. It holds significant practical significance for understanding the development of Africa in the digital revolution era. It also serves as a valuable supplement to existing research on cybersecurity in Nigeria, thereby enhancing its academic relevance.

Keywords: Cybersecurity; Governance; Cooperation; Nigeria; Africa; China

1. Introduction

With the wide application of Internet, Nigeria is enjoying the technological dividend while also facing cybersecurity threats such as cyber-attacks, data leaks and malware. The economic, financial and reputational implication and potential impact of these cybercrime related activities are significant, with potential negative ramifications on the national economy, business operations, and personal security.

Nigeria's cyberspace is experiencing an increase in digital transformation [1]. In Nigeria, the cybercrime has increased due to the growth, adoption and increased integration of digital technologies in the core fibre of daily usage by the populace. The cyber related crimes range from financial fraud, social engineering, identity theft, software piracy, hacking, cyber espionage, and many more [2].

To address the increasing cybercrimes and its impact on the national economy, the Nigerian government has formulated and implemented a series of policies and initiatives. However, these measures still exhibit limitations. Moving forward, Nigeria will need to continuously update and enhance these strategies while proactively collaborating with leading cyberpowers to better address emerging cybersecurity issues.

* Corresponding author: Chen Yizhen.

2. Emerging Cybersecurity Issues in Nigeria

Cybercrime is a common occurrence in Nigeria. According to the report from the Nigerian Communication Commission (NCC) Nigeria loses about $500m yearly to cybercrime. This accounts for 0.08 percent of the country's Gross Domestic Product. Most cases of cybercrimes in Nigeria are a result of unauthorised access to the private data of individuals [3]. It is not uncommon for people to receive emails, sms, chats and even voice calls detailing their private information. Cyber Security Experts Association of Nigeria (CSEAN) indicates that Cybersecurity remains a critical concern for Nigeria as the nation continues its digital transformation. As Nigeria's digital economy continues to grow, so does the complexity of its cybersecurity landscape, according to the Nigeria Cybersecurity Outlook 2025 published by consultancy Deloitte [4]. In recent years, with the rapid development of the digital revolution, some new issues have emerged in the field of cybersecurity in Nigeria, such as AI-Powered Attacks, Cryptocurrency Scams, Third-Party Risk, Identity Theft and Fraud, Cyber Talent Drain, etc.

2.1. AI-Powered Attacks/AI-Assisted Cybercrimes

The adoption of Artificial Intelligence (AI) is empowering cybercriminals. AI-powered attacks are making cyber threats more sophisticated, automated, and precise. Malicious actors are using AI to automate phishing campaigns, create polymorphic malware that evade detection, and craft hyper-realistic deepfakes. AI amplifies the scale and precision of cyberattacks, moving them closer to pandemic-like proportions. Cybercriminals are increasingly exploiting the ability of Generative AI (Gen AI) to mimic human communication and create hyper-realistic content. In a country already grappling with phishing and social engineering attacks, AI generated fake emails, texts, and voice impersonations are poised to make scams virtually indistinguishable from legitimate communication. Data privacy concerns are also mounting as these AI models require extensive datasets for training, often involving sensitive personal or corporate information. "Yahoo Boys" leverage advanced AI tools such as deepfakes, enabling more realistic phishing, social engineering, romance, and sextortion attacks [5]. As AI techniques evolve, threat actors can manipulate voice and video content with startling precision, undermining trust in digital communications.

2.2. Cryptocurrency Scams

The surge in cryptocurrency scams is set to escalate, driven in part by rising crypto prices following Donald Trump's reelection and his promise to bolster the sector by easing regulations and establishing a National Strategic Bitcoin Reserve. This optimistic climate will likely spark increased investments but also heightened opportunities for fraud, especially in Nigeria, which boasts the world's largest crypto-aware population [6]. Nigeria recorded the highest rates of cryptocurrency ownership worldwide, malicious actors will exploit this fervor, targeting inexperienced and eager investors through tactics such as social media crypto giveaway scams, Ponzi schemes, rug pulls, fake cryptocurrency exchanges, and phony investment platforms.

2.3. Third-Party Risk

As Nigeria's digital economy continues to expand, third-party risks are becoming increasingly concerning. Cybercriminals frequently target the weakest links in the supply chain, exploiting gaps in third parties' security practices. This challenge is exacerbated by the widespread adoption of cloud-based solutions, including financial applications, HR platforms, and document-signing tools, which are now commonplace across Nigeria. Additionally, the proliferation of Application Programming Interfaces (APIs), which are critical for integrating applications and enabling seamless operations across entities, introduces new vulnerabilities. Poorly secured APIs can serve as entry points for attackers, allowing unauthorized access to systems and data. The interconnected nature of APIs means a single compromised integration can have a ripple effect across multiple systems, escalating the impact of an attack.

2.4. Identity Theft and Fraud

As digital transformation accelerates, identity theft and fraud are becoming increasingly pervasive in Nigeria, raising serious concerns for businesses and individuals alike. With the growing reliance on online services for banking, e-commerce, and communication, cybercriminals are leveraging advanced tools and tactics to steal personal information, financial data, and corporate identities. According to the Nigeria Inter-Bank Settlement System (NIBSS) report released in 2024, there were notable incidents involving fraudsters using techniques such as social engineering to gain unauthorized access to sensitive information and successfully performing account takeovers. The rapid adoption of digital payment systems, mobile banking, and e-commerce platforms in Nigeria has also fueled the growth of these crimes. With many businesses still working on enhancing their security infrastructure, criminals are finding new ways to exploit system weaknesses and gain access to consumers' financial information.

2.5. "Japa" of Professionals/ Cyber Talent Drain

In Nigeria, "Japa" (derived from Yoruba to mean "runaway" or "escape") has become emblematic of skilled professionals emigrating for better prospects. The cybersecurity talent shortage is a pressing global issue, but in Nigeria, it has reached a critical level. Over the past few years, the country has experienced a significant brain drain in its cybersecurity workforce, with many experts seeking opportunities abroad due to better pay, career growth, and stability. In 2024, this trend surged among information technology and cybersecurity experts, driven by economic instability, soaring inflation, and the depreciating currency. The departure of these specialized workers has severely impacted sectors heavily reliant on robust digital infrastructure, most notably banking. As the pool of professionals shrinks, organizations grapple with heightened vulnerabilities, leaving critical systems exposed to sophisticated attacks. This phenomenon will continue, potentially straining Nigeria's digital ecosystem even further.

3. Cybersecurity Governance in Nigeria

As a way of ensuring a safe and secure cyberspace for Nigerians, Nigeria has issued a series of laws and regulations in the field of ICT, digital, and Cyberspace.

3.1. Cybercrimes (Prohibition, Prevention, etc) Act, 2015 and its amendment

In a bid to put in place a stronger legal framework to curb cybercrime, the Government put forward a revision of the existing cybercrime legislation in September 2008. The bill titled "A Bill for an Act to Provide for the Prohibition of Electronic Fraud in all Electronic Transactions in Nigeria and for Other Related Matters" passed a second reading in November 2012 at the Senate. In May 2015, the cybercrime bill was signed into law, properly defining the act as unlawful with penalties attached to any disobedience of the law—the Act, known as the *Cybercrimes (Prohibition, Prevention, etc) Act, 2015*. The objectives of the Act are to:

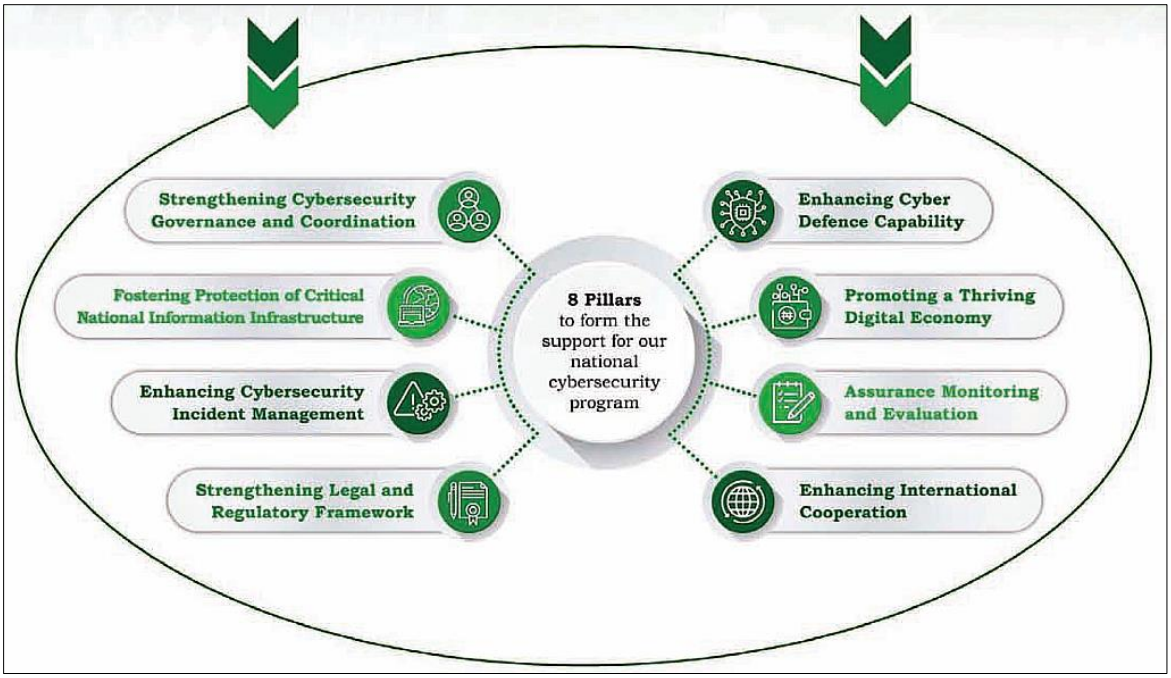
- provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;
- ensure the protection of critical national information infrastructure; and
- promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

The Act 2015 creates a legal, regulatory and institutional framework for the governance of cybercrimes and other related matters. Particularly, the Act engenders a platform for cyber security and, in turn, ensures the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property, privacy rights, as well as preservation and protection of critical national information. Act 2015, is, thus, the first legislation in Nigeria that deals specifically with cybercrimes and cyber security, and creates a comprehensive legal, regulatory, and institutional framework to prohibit, prevent, detect, prosecute, and punish cybercrime. The Act prescribes stringent penalties for offenders and perpetrators of cybercrime, which stipulates that, any crime or injury on critical national information infrastructure, sales of preregistered SIM cards, unlawful access to computer systems, Cyber-Terrorism, among others, would be punishable under the new law.

However, the Act 2015 was perceived by experts with mixed feelings. Apart from the ambiguity and lack decisive roles of the Act, there are the inability to provide modern tools of surveillance, the ineffective operation and application of the law failed to prevent cybercrimes. In addition, experts lamented that although the Act 2015 succeeded in making some couple of arrests, the selective treatment of offenders and a perceived crackdown on political opponents is bastardising the law [7]. In 2024, therefore, *Cybercrimes (prohibition, prevention, etc) (amendment) act, 2024* amended the Act 2015 to insert some consequential words that were inadvertently omitted in the Act, such as the amendment of section 17, 21, 22, 24, 27, 30, 37, 38, 41, 44, 48, which makes the provisions of the Act 2015 clearer to a certain extent. Following the enactment of this Amendment Act 2024 and pursuant to the provision of Section 44 (2)(a) of the Act, "a levy of 0.5%(0.005) equivalent to a half percent of all electronic transactions value by the business specified in the Second Schedule of the Act", is to be remitted to the National Cybersecurity Fund (NCF), which shall be administered by the Office of the National Security Adviser (ONSA). After that, Central Bank of Nigeria (CBN) published a circular named *Implementation Guidance On The Collection And Remittance Of The National Cybersecurity Levy* to direct banks and other financial institutions to start charging a cybersecurity levy on all banking transactions. But amid widespread public criticism of the scheme as the cost of living rises and the naira currency falls, Nigeria had to suspend the planned levy on domestic money transfers to fund cybersecurity [8].

3.2. National Cybersecurity Policy and Strategy 2021

The Nigerian government has implemented a number of measures to strengthen national security as a result of realizing how important it is to combat cyber threats. The *National Cybersecurity Policy and Strategy 2021* is a significant step in this direction. In February 2021, Nigeria unveiled this policy as the overarching policy and strategy framework for driving Nigeria's cybersecurity efforts towards the attainment of our national objectives, which is a purposeful and living document which outlines the roadmap for realisation of Nigeria's cybersecurity vision of "a safe and secure digital community that provides opportunities for its citizenry and promotes peaceful and proactive engagements in cyberspace for enhanced national prosperity", and mission of "to foster a trusted cyber environment that optimises Nigeria's cybersecurity readiness and coordination capacities towards addressing the nation's cyber risk exposure." The Policy is a confluence of ends, ways and means which articulates the efforts of allstakeholders and emplaces Nigeria National Cybersecurity Programme on 8 critical pillars:



Source: National Cybersecurity Policy and Strategy 2021[9]

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

To deliver the objectives of National Cybersecurity Programme, the Policy have an Implementation Plan that is its roadmap for driving success, measuring progress and transforming its prescribed strategic actions into reality. Nigeria's cyberspace will be secured by the complete framework outlined in this policy. The policy aims to address the growing dangers posed by cyber-attacks by emphasizing enhanced governance, information sharing, capacity building, and public-private partnerships. Additionally, the policy also focuses on improving incident response capabilities and fostering international cooperation to effectively tackle cyber threats. However, the study discovered that these efforts are not yet sufficient, since issues such as restricted enforcement, insufficient cybersecurity awareness, and a trained labor scarcity continue. Furthermore, deficiencies in cooperation among critical agencies and unreliable reporting of cyberattacks undermine the overall security posture [10].

3.3. Nigeria Data Protection Act, 2023

To prevent criminals from accessing private data, bank information, and other personal information, the Nigerian government put in place measures to promote data protection in the country. Section 37 of the Constitution of the Federal Republic of Nigeria (FRN) guarantees privacy protections to citizens in their homes, correspondence, telephone conversations and telegraphic communications. In order to implement this and prepare Nigeria for the digital economy, Nigeria has issued the *Nigeria Cloud Computing Policy (2019), Nigeria Data Protection Regulation (2019),* and other policies and regulations, which provides for Nigerians to have greater control over how their data is collected, shared, and used. Based on that, The Nigerian Government finally enacted the *Nigeria Data Protection Act, 2023,* whose objectives are to:

- safeguard the fundamental rights and freedoms, and the interests of data subjects, as guaranteed under the Constitution of the Federal Republic of Nigeria, 1999;
- provide for the regulation of processing of personal data;
- promote data processing practices that safeguard the security of personal data and privacy of data subjects;
- ensure that personal data is processed in a fair, lawful and accountable manner;
- protect data subjects' rights, and provide means of recourse and remedies, in the event of the breach of the data subject's rights;
- ensure that data controllers and data processors fulfil their obligations to data subjects;
- establish an impartial, independent, and effective regulatory Commission to superintend over data protection and privacy issues, and supervise data controllers and data processors;and
- strengthen the legal foundations of the national digital economy and guarantee the participation of Nigeria in the regional and global economies through the beneficial and trusted use of personal data.

Besides providing a legal framework for the protection of personal information, this Act also establishes the Nigeria Data Protection Commission (NDPC) to oversee the implementation of the provisions of this Act, regulate the processing of personal information, promoting data processing practices that safeguard the security of personal data and the privacy of data citizens, institutions, and organizations. As Nigeria continues to make its mark within the global digital economy and rapidly expand its technology ecosystem, this Act represents a continued focus on protecting the personal data of Nigerian citizens, in alignment with common internationally accepted principles of data protection. However, the Act contains unique provisions that should not be overlooked, including a new classification of data controllers and processors “of major importance” and specific obligations attached to them, as well as broader protections for exempt processing activities. Overall, the Act represents a significant step in Nigerian data protection and notably resolves the long-running dispute regarding the identity and institutional authority of Nigeria’s primary data protection regulator [11].

3.4. Other institutions and policies related to cybersecurity

The agencies enacted by law play a vital role in combating and prosecuting cybercriminals. This will serve a strong deterrent which will ultimately aid in the reduction of cybercrimes in the society at large. Some law enforcement agencies include: The specialized units within the Nigerian Police Force and other security agencies are tasked with investigating and prosecuting cybercrime cases; Economic and Financial Crimes Commission(EFCC); National Information Technology Development Agency(NITDA); Office of the National Security Adviser(ONSA)-National Cybersecurity Coordination Centre(NCCC); Nigerian Communications Commission(NCC); Independent Corrupt Practices and Other Related Offences Commission(ICPC).

Nigerian government has also established Cybersecurity Centers, namely, the NITDA’s Computer Emergency Readiness and Response Team (CERRT), the Nigerian Communications Commission (NCC)’s Computer Security Incident Response Team (CSIRT), and Galaxy Backbone (GBB)’s Security Operations Centre (SOC). These Centers were established after 2020 in line with the Nigerian government policy directives and have been monitoring Nigerian cyberspace for potential threats and taking appropriate actions to mitigate them, both individually and collectively as well as in collaboration with other stakeholders. Nigeria has taken several measures to secure data and cyberspace in 2022: Nigeria Data Protection Bureau (NDPB) was established to advance data protection and privacy; NITDA issued a code of conduct aimed at guiding the activities of social media companies in the country, requiring Facebook, Twitter, and others to open local offices and pay taxes to ensure that Nigeria fully utilizes the potential of the digital economy while safeguarding the security and interests of the country and its citizens; and the National Shared Services Center(NSSC) was established to support the ICT industry, develop the digital economy and work to combat cybercrime.

Some policies related to cybersecurity, like the *National Policy on 5G for Nigeria's Digital Economy* was also released, with the former Nigerian President Muhammadu Buhari saying the federal government would take complete advantage of the opportunities that 5G provides for the economy, security, and well-being of the nation. The former Nigerian president directed all the security institutions to immediately leverage on the 5G technology, when deployed, to enhance security in the country. In May 2025, Nigeria launched *National Artificial Intelligence Strategy* to accelerate AI development, productivity, and economic growth across sectors. “Cybersecurity is required within the AI strategy, incorporating cybersecurity measures specific to AI systems, mitigating potential vulnerabilities, and ensuring the security of AI-powered applications,” the Strategy reads,“The growing dependence on digital assets and the escalating nature of cyber threats emphasise the urgent need for strong cybersecurity measures to protect against potential threats in Nigeria's rapidly changing digital landscape” [12]. And one of its objective is to develop and implement AI and AI-driven training and education systems that identify, nurture, and develop diverse AI talent across the different AI domains and related areas like cybersecurity.

4. Nigeria's International Cooperation in Cybersecurity

In addition to abovementioned laws and policies, Nigeria is also leveraging international cooperation to solve cybersecurity issues and promote digital development.

4.1. Cooperation with global organizations

Globally, Nigeria collaborates with the International Telecommunication Union (ITU) to protect its cyberspace, benefiting from frameworks like the Global Cybersecurity Agenda. It works with Interpol to tackle cybercrime and engages with the Organization of the Islamic Cooperation-Computer Emergency Response Teams (OIC-CERT) for cybersecurity enhancements. Nigeria's digital identity initiative is also funded by the World Bank.

4.2. Cooperation with Europe

In July 2022, Nigeria acceded to the Council of Europe Convention on cybercrime (ETS No. 185), which is known as the Budapest Convention. The Convention entered into force for Nigeria on 1 November 2022. In addition, as a part of the Global Gateway Africa-Europe Investment Package, Nigeria is working with the EU to strengthen its secure connectivity, digitalize public services, support entrepreneurship and digital skills, and build a people-centered democratic governance framework for technological development. Recently, Nigeria signed a multilateral Memorandum of Understanding (MoU) with the UK to combat the menace of cybercrimes in the two countries in April 2025. The Joint Case Team on Cybercrime (JCTC) was launched in response to the need for a coordinated and robust approach to fighting cybercrimes [13].

4.3. Cooperation with the U.S.

The United Stated of America (U.S.) has taken a step to bolster cybersecurity efforts in Nigeria by establishing a special office at its embassy in Abuja in July 2024. This initiative aims to enhance collaboration with Nigeria’s EFCC in combating cybercrimes. In response to the growing cybercrimes in Nigeria, the U.S. had earlier announced plans to deploy a cybercrime advisor to Nigeria. The advisor will facilitate cooperation between the two nations by providing essential training, equipment, and technical assistance to enhance Nigeria’s ability to address cyber threats such as fraud scams and sextortion [14]. In addition, American companies such as Microsoft and SpaceX are also working with Nigeria on connectivity, skills training, and digital transformation.

4.4. Cooperation with China

China and Africa join hands to build a community with a shared future in cyberspace and enable the Cyberspace to better benefit African people, which is an organic part of jointly building a closer China-Africa community with a shared future and an important manifestation of its construction achievements. China-Africa cooperation in cyberspace is an important component of the construction of the "Digital Silk Road". As China-Africa cooperation continues to develop in an all-round, multi-level and high-quality manner, digitalization, with cyberspace development as an important content, is increasingly becoming a new highland of China-Africa cooperation. China is supporting African countries, including Nigeria, to bridge the digital divide.

In January 2021, Nigerian former president Muhammadu Buhari met with Chinese Foreign Minister Wang Yi in Abuja. During their meeting, Wang said that China is willing to share digital economy experience and technology with Nigeria and carry out green economy cooperation. Moreover, China has proposed the China-Africa Digital Innovation Partnership Program, and China-Africa practical cooperation in the digital field. These two initiatives have been mounting to better meet the needs of the Chinese and African people. Nigeria is leveraging Chinese investment to develop its infrastructure and training to enhance its digital domain. Chinese companies, especially Huawei, have launched data protection products and trained a large number of ICT talents for Nigeria to promote Nigeria's autonomous and secure digital development. In March 2025, China and Nigeria have agreed to cooperate together to crack down on cybercrimes in the West African country, particularly those that involve Chinese nationals, which reflects China's responsibility and commitment as a major cyberpower. China is ready to send out a working group to Nigeria to work with Nigeria law enforcement officers, EFCC, for evidence collection, fraud tracing, and bringing criminals to justice [15].

In a significant move towards deepening bilateral relations, Nigeria and China have reaffirmed their commitment to strengthening cooperation across various sectors including Cyberspace and digital development at the second edition of Lagos Forum in April 2025, which is Co-hosted by the Institute of African Studies at Zhejiang Normal University(IASZNU), Nigerian Institute of International Affairs(NIIA), Chinese Consulate General in Lagos, and the Africa-China Economy Magazine, and has become a vital platform for China-Nigeria dialogue and has played a pivotal

role in fostering partnership between both countries. "Nigeria and China need to create better digital capabilities to implement the swap for the good of Nigeria's economy, especially its economy, which is chocking under the monopoly of the US dollar," as Ikenna Emewu, Editor-in-Chief of Africa China Economy Magazine said at the Forum, "We, therefore, need a very effective digital economy cooperation and cybersecurity system between Nigeria and China to sail through this bad weather" [16].

5. Conclusion

From the discussion above, it can be concluded that cybercrime is still severe in Nigeria. The study found that with the rapid development of the digital revolution, some new issues have emerged in the field of cybersecurity in Nigeria, such as AI-Powered Attacks, Cryptocurrency Scams, Third-Party Risk, Identity Theft and Fraud, Cyber Talent Drain. It also revealed that the Nigeria Government through a series of laws and regulations in the field of ICT, digital, and Cyberspace, like Cybercrimes (Prohibition, Prevention, etc) Act, 2015 and its amendment, National Cybersecurity Policy and Strategy 2021, National Cybersecurity Policy and Strategy 2021, as a way of ensuring a safe and secure cyberspace for Nigerians. In addition, Nigeria is also leveraging international cooperation to solve cybersecurity issues and promote digital development. In particular, the joint efforts of China and Africa to build a community with a shared future in cyberspace bring bright prospects for Nigeria-China Cooperation in cyberspace.

Compliance with ethical standards

Acknowledgments

This article is sponsored by the Institute of African Studies (College of African Area and Country Studies), Zhejiang Normal University 2023 Research Project in Africa (Project Number: FF202304).

Disclosure of conflict of interest

No conflict of interest to be disclosed

References

[1] Idowu OA, Madaki M. Cybercrimes and Challenges of Cyber-Security in Nigeria. International Journal of Sociology and Development. 2021;3(1):4.

[2] Ayub AO, Akor L. Trends, patterns and consequences of cybercrime in Nigeria. Gusau International Journal of Management and Social Sciences. 2022;5(1):241-62.

[3] DoP AA, Chigbu G, Osazuwa CM. effect of data protection frameworks against cybercrimes on cyber security in Nigeria. The American Journal of Political Science Law and Criminology. 2024 Sep 23;6(09):67.

[4] Nigeria Cybersecurity Outlook 2025. Deloitte. https://www.deloitte.com/ng/en/services/risk-advisory/perspectives/Nigerias-cybersecurity-landscape-in-2025.html.

[5] Macaskil G. Evil world of Yahoo Boys sextortion gang who drive Brits to suicide… and then flaunt £1k trainers from ill-gotten gains. THE IRISH SUN. Sep 1, 2024. https://www.thesun.ie/news/13729614/twisted-world-of-yahoo-boys-sextortion/.

[6] Okonkwo K, Akpan S. What's the Most Crypto-Savvy Country in the World? Consensys. August 31, 2023. https://consensys.io/blog/whats-the-most-crypto-savvy-country-in-the-world-hint-its-not-the-usa.

[7] Sule B, Sambo U, Yusuf M. Countering cybercrimes as the strategy of enhancing sustainable digital economy in Nigeria. Journal of Financial Crime. 2022 Oct 28;30(6):1557-74.

[8] Onuah F. Nigeria suspends cybersecurity levy amid cost of living crisis. Reuters. May 14, 2024. https://www.reuters.com/world/africa/nigeria-suspends-cybersecurity-levy-amid-cost-living-crisis-2024-05-14/.

[9] Nigerian Communications Commission. National Cybersecurity Policy and Strategy 2021. February 2021. https://ncc.gov.ng/media/800/view.

[10] Gana IM, Ibrahim AF, Oluwaseyi WA, Wali AI. Cyber Warfare and National Security in Nigeria: Threats and Responses. Kwararafa Security Review. 2024; 1(2):8.

[11] King M. Nigeria's New Data Protection Act, Explained. Future of Privacy Forum. June 28, 2023. https://fpf.org/blog/nigerias-new-data-protection-act-explained/.

[12] NCAIR& NITDA. National Artificial Intelligence Strategy. August 2024. https://ncair.nitda.gov.ng/wp-content/uploads/2024/08/National-AI-Strategy_01082024-copy.pdf.

[13] Nigeria, UK sign MoU to combat cybercrimes, improve criminal justice system. Vanguard. April 29, 2025. https://www.vanguardngr.com/2025/04/nigeria-uk-sign-mou-to-combat-cybercrimes-improve-criminal-justice-system/#google_vignette.

[14] Ozibo R. U.S. opens special cybersecurity office in Abuja to boost collaboration with EFCC. Nairametrics. July 26, 2024. https://nairametrics.com/2024/07/26/u-s-opens-special-cybersecurity-office-in-abuja-to-boost-collaboration-with-efcc/.

[15] Olander E. China, Nigeria to Cooperate in Combatting Cybercrime. China Global South Project. March 10, 2025. https://chinaglobalsouth.com/2025/03/10/china-nigeria-to-cooperate-in-combatting-cybercrime/.

[16] Emewu I. Nigeria, China need stronger digital economy cooperation for currency swap success. Africa China Economy. April 29, 2025. https://africachinapresscentre.org/2025/04/29/nigeria-china-need-stronger-digital-economy-cooperation-for-currency-swap-success-emewu/.