



Research Article

Assessment of Cybersecurity Challenges and Their Implications for National Security in Nigeria

Nura Umar Manya Manya¹, Isah Maina²

1. School of Postgraduate Studies, Institute of Governance and Development Studies Nasarawa State University, Keffi, Nigeria; umarmanyamanyanura@gmail.com ORCID: ID 0009-0006-4980-085
2. School of Postgraduate Studies, Institute of Governance and Development Studies Nasarawa State University, Keffi, Nigeria; isamaina@yahoo.com

Copyright © 2026 by Authors, Published by **Interkoneksi: Journal of Computer Science and Digital Business**. This is an open access article under the CC BY License <https://creativecommons.org/licenses/by/4.0/>

Received : May 16, 2026

Revised : June 13, 2026

Accepted : July 19, 2026

Available online : August 14, 2026

How to Cite: Nura Umar Manya Manya, & Isah Maina. (2026). Assessment of Cybersecurity Challenges and Their Implications for National Security in Nigeria. *Interkoneksi: Journal of Computer Science and Digital Business*, 4(1), 191–207. <https://doi.org/10.61166/interkoneksi.v4i1.92>

Abstract. The rapid expansion of Nigeria's digital ecosystem has transformed cybersecurity from a technological concern into a critical component of national security. As government institutions, financial systems, telecommunications, education, healthcare, and other critical infrastructure increasingly rely on digital technologies, the country has become more vulnerable to cyber threats. This study assessed the cybersecurity challenges facing Nigeria and examined their implications for national security. A qualitative descriptive research design based on documentary analysis was adopted. Data were obtained from secondary sources, including peer-reviewed journal articles, books, government publications, policy documents, and reports from national and international organizations. The collected data were analyzed using qualitative content analysis. The findings revealed that Nigeria continues to face diverse cybersecurity threats, including phishing, ransomware, business email compromise, identity theft, cyber fraud, cyber-enabled terrorism, misinformation, and attacks on critical national infrastructure. These threats undermine economic stability, weaken institutional resilience, threaten public safety, and compromise national sovereignty. The study further

found that weak cybersecurity governance, inadequate funding, limited institutional capacity, shortage of skilled cybersecurity professionals, poor public cyber awareness, and insufficient inter-agency collaboration remain major barriers to effective cybersecurity management. The study also established that emerging technologies, particularly Artificial Intelligence (AI), offer significant opportunities for strengthening cybersecurity through automated threat detection, predictive analytics, anomaly detection, biometric authentication, malware identification, and real-time incident response. However, the misuse of AI by cybercriminals for sophisticated phishing attacks, deepfakes, automated malware, and intelligent cyberattacks presents new security challenges that require effective regulation and ethical governance. The analysis was anchored on Systems Theory, National Security Theory, and Deterrence Theory, which collectively explain the interconnected nature of cyberspace, the responsibility of government to protect national digital assets, and the importance of strong legal and institutional measures in preventing cybercrime. The study concludes that cybersecurity has become indispensable to Nigeria's national security and sustainable development. It recommends increased investment in AI-enabled cybersecurity technologies, effective implementation of the National Cybersecurity Policy and Strategy and the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, continuous capacity building for cybersecurity professionals, enhanced public awareness, stronger inter-agency coordination, and greater international cooperation. Implementing these measures will improve Nigeria's cyber resilience, protect critical national infrastructure, strengthen national security, and support sustainable socio-economic development in the digital age.

Keywords: Cybersecurity, National Security, Cybercrime, Artificial Intelligence, Critical Infrastructure, Nigeria, Cyber Resilience, Digital Governance.

INTRODUCTION

The rapid advancement of information and communication technology (ICT) has transformed the way governments, businesses, educational institutions, financial organizations, and individuals communicate and conduct daily activities. The widespread adoption of digital technologies has significantly improved economic growth, governance, financial inclusion, and access to information. In Nigeria, increasing internet penetration, mobile banking, electronic commerce, digital governance, cloud computing, and the emergence of Artificial Intelligence (AI) have accelerated digital transformation and created new opportunities for national development.

Despite these benefits, the expansion of the digital ecosystem has exposed Nigeria to a growing number of cybersecurity threats. Cybersecurity has therefore become one of the most important components of national security in the twenty-first century. Cyberattacks such as phishing, ransomware, identity theft, hacking, and business email compromise (BEC), cyber fraud, cyber espionage, cyberterrorism, and attacks on critical national infrastructure have become increasingly sophisticated. These threats affect government institutions, financial systems, telecommunications networks, healthcare services, educational institutions, energy facilities, and private businesses, resulting in financial losses, disruption of essential services, erosion of public confidence, and threats to national stability.

Nigeria has witnessed a significant increase in cybercrime due to rapid digitalization, expanding internet access, limited cybersecurity awareness, inadequate institutional capacity, shortage of skilled cybersecurity professionals,

weak enforcement of cybersecurity regulations, and increasing dependence on digital technologies. Criminal groups continue to exploit technological vulnerabilities to perpetrate financial fraud, compromise sensitive information, spread misinformation, and disrupt essential national services. The increasing use of cyberspace by terrorist organizations for recruitment, communication, propaganda, intelligence gathering, and financing further demonstrates the strategic relationship between cybersecurity and national security.

The emergence of Artificial Intelligence has introduced both opportunities and challenges for cybersecurity. AI-powered technologies improve cyber defence through automated threat detection, predictive analytics, anomaly detection, malware identification, biometric authentication, and real-time incident response. At the same time, cybercriminals increasingly employ AI to develop sophisticated phishing campaigns, automated malware, deepfake technology, and intelligent cyberattacks capable of bypassing conventional security mechanisms. Consequently, effective cybersecurity governance requires continuous technological innovation, legal reforms, institutional strengthening, public awareness, and international cooperation.

Recognizing these challenges, the Nigerian government has introduced several legal and institutional frameworks to strengthen cybersecurity. These include the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, the National Cybersecurity Policy and Strategy, the Office of the National Security Adviser (ONSA), the National Information Technology Development Agency (NITDA), the Nigerian Communications Commission (NCC), the Nigeria Computer Emergency Response Team (ngCERT), and other relevant security institutions. However, despite these initiatives, cyber threats continue to evolve rapidly, creating significant implications for national security, economic development, and sustainable governance.

It is against this background that this study assesses the cybersecurity challenges confronting Nigeria and examines their implications for national security. The study also explores the role of Artificial Intelligence and other emerging technologies in strengthening cybersecurity while identifying policy measures capable of improving Nigeria's cyber resilience and protecting critical national infrastructure.

Statement of the Problem

The increasing reliance on digital technologies has made Nigeria more vulnerable to cyber threats that undermine national security and socio-economic development. Government institutions, financial organizations, telecommunications companies, educational institutions, healthcare systems, and other critical infrastructure are increasingly targeted by cybercriminals through phishing, ransomware, identity theft, cyber fraud, business email compromise, cyber espionage, and cyber-enabled terrorism.

Although the Nigerian government has enacted cybersecurity laws and established relevant institutions to address these threats, challenges such as inadequate funding, shortage of cybersecurity professionals, weak institutional coordination, poor public awareness, obsolete technological infrastructure, and

ineffective implementation of cybersecurity policies continue to limit the country's cyber resilience. Furthermore, the rapid evolution of Artificial Intelligence presents both opportunities for strengthening cybersecurity and new risks arising from AI-enabled cybercrime.

If these cybersecurity challenges remain inadequately addressed, they could compromise national sovereignty, weaken economic growth, disrupt essential public services, threaten public safety, and reduce citizens' confidence in digital governance. Therefore, there is a need to comprehensively assess cybersecurity challenges and their implications for national security in Nigeria while identifying practical strategies for strengthening national cyber resilience.

Objectives of the Study

The main objective of this study is to assess cybersecurity challenges and their implications for national security in Nigeria.

The specific objectives are to:

1. Examine the major cybersecurity challenges confronting Nigeria;
2. Assess the implications of cybersecurity threats for Nigeria's national security;
3. Evaluate the effectiveness of existing cybersecurity laws, policies, and institutional frameworks;
4. Examine the role of Artificial Intelligence in strengthening cybersecurity and its associated risks; and
5. Recommend strategies for improving cybersecurity and enhancing national security in Nigeria.

LITERATURE REVIEW

This chapter reviews existing literature on cybersecurity challenges and their implications for national security in Nigeria. The review is organized into the conceptual review, theoretical review, empirical review, and identified gaps in the literature. It provides the theoretical and empirical foundation for understanding the relationship between cybersecurity and national security while highlighting previous scholarly contributions and areas requiring further investigation.

1. Conceptual Review

Concept of Cybersecurity

Cybersecurity refers to the protection of computer systems, networks, digital infrastructure, software applications, and information assets against unauthorized access, cyberattacks, theft, disruption, and destruction. According to the International Telecommunication Union (ITU, 2023), cybersecurity consists of technologies, policies, guidelines, risk management approaches, security safeguards, training, best practices, and institutional arrangements designed to protect cyberspace and users. The primary objectives of cybersecurity are to ensure the confidentiality, integrity, and availability of information.

In Nigeria, cybersecurity has become increasingly important because of rapid digital transformation in banking, telecommunications, healthcare, education,

electronic commerce, and public administration. As internet penetration and digital services continue to expand, cyber risks have also increased significantly.

Concept of National Security

National security refers to the protection of a country's sovereignty, territorial integrity, political institutions, economy, citizens, and strategic national interests against internal and external threats. Contemporary national security extends beyond military defence to include economic, environmental, health, technological, and cyber security. Cybersecurity has therefore become an essential component of national security because attacks on digital infrastructure can cripple government operations, financial systems, critical infrastructure, and public services.

Concept of Cybercrime

Cybercrime involves criminal activities committed through computers, mobile devices, digital networks, or the internet. Examples include hacking, phishing, ransomware, identity theft, online fraud, cyberstalking, malware attacks, and unauthorized access to confidential information.

Nigeria continues to experience increasing cybercrime because of rapid internet adoption, youth unemployment, inadequate cybersecurity awareness, and weaknesses in digital governance. The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 provides the legal framework for addressing these offences.

Concept of Artificial Intelligence and Cybersecurity

Artificial Intelligence (AI) refers to computer systems capable of performing tasks requiring human intelligence, including learning, reasoning, prediction, and decision-making. AI has transformed cybersecurity by enabling automated threat detection, predictive analytics, behavioural analysis, malware detection, biometric authentication, and rapid incident response.

However, AI also presents security risks because cybercriminals increasingly use AI to generate phishing emails, develop sophisticated malware, conduct automated attacks, and create deepfake content.

National Concept of Critical Infrastructure

Critical national infrastructure comprises essential facilities and systems whose disruption would seriously affect national security, economic stability, governance, and public welfare. These include financial institutions, telecommunications, healthcare, transportation, electricity, water supply, defence installations, and government information systems.

Protecting these infrastructures has become a major national security priority because cyberattacks can interrupt essential services and cause widespread economic and social disruption.

3. Cybersecurity Threats in Nigeria

Nigeria experiences numerous cyber threats, including:

- Phishing attacks targeting banking customers and government officials.

- Business Email Compromise (BEC).
- Ransomware attacks against healthcare institutions, schools, and businesses.
- Identity theft and financial fraud.
- Cyber espionage against government agencies
- Cyber-enabled terrorism and extremist propaganda.
- Social media misinformation and disinformation.
- Malware attacks.
- Distributed Denial-of-Service (DDoS) attacks.
- Attacks on critical national infrastructure.

These threats continue to evolve because cybercriminals adopt more sophisticated technologies, including Artificial Intelligence.

4. Implications of the Study

The findings of this study have significant implications for Nigeria's national security, public policy, institutional governance, economic development, and cybersecurity management. As Nigeria continues to expand its digital economy and adopt emerging information and communication technologies (ICT), cybersecurity has become a strategic national priority rather than merely a technical concern. The increasing sophistication of cyber threats demonstrates that weaknesses in cyberspace can directly undermine national stability and sustainable development.

From a national security perspective, the study reveals that cyber threats such as cybercrime, cyberterrorism, ransomware attacks, espionage, and digital misinformation have the potential to compromise Nigeria's sovereignty and weaken public confidence in government institutions. Attacks on critical national infrastructure, including financial institutions, telecommunications networks, power systems, healthcare facilities, and government databases, could disrupt essential services, threaten public safety, and adversely affect national resilience.

The study also has important policy implications. Although Nigeria has established legal and institutional frameworks such as the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 and the National Cybersecurity Policy and Strategy, effective implementation remains a major challenge. The findings suggest the need for stronger enforcement mechanisms, periodic policy reviews, improved institutional coordination, and increased investment in cybersecurity infrastructure to address emerging threats effectively.

Economically, persistent cyberattacks impose substantial financial losses on businesses, government agencies, and individuals. Cyber fraud, identity theft, online banking attacks, and business email compromise reduce investor confidence, increase operational costs, and hinder the growth of Nigeria's digital economy. Strengthening cybersecurity is therefore essential for promoting economic stability, attracting investment, and supporting sustainable national development.

The study further highlights the implications for education and human capacity development. There is an urgent need to integrate cybersecurity education into school curricula, professional training programmes, and public awareness campaigns. Building a digitally literate population will enhance cyber resilience,

reduce human-related vulnerabilities, and promote responsible use of digital technologies across society.

Furthermore, the research underscores the importance of inter-agency collaboration and international cooperation. Since cyber threats are transnational in nature, Nigeria must strengthen partnerships with regional organizations, international cybersecurity agencies, and global law enforcement institutions to improve intelligence sharing, cybercrime investigation, and incident response capabilities.

Finally, this study contributes to academic knowledge by expanding the existing literature on the relationship between cybersecurity and national security in Nigeria. It provides a foundation for future empirical studies, comparative analyses, and policy-oriented research aimed at developing innovative strategies for protecting Nigeria's digital environment. Overall, the study emphasizes that strengthening cybersecurity is indispensable for safeguarding national security, promoting economic prosperity, protecting democratic institutions, and ensuring sustainable development in an increasingly interconnected digital world.

5. Implications of Cybersecurity Challenges for Nigerian National Security

Cybersecurity challenges have profound implications for Nigeria's national security because they threaten the country's economic stability, political institutions, critical infrastructure, and social cohesion. As Nigeria continues to embrace digital transformation across government, finance, education, healthcare, and commerce, cyber threats increasingly pose strategic risks capable of undermining national development and state security.

Economic Implications

Cybercrime has become one of the major threats to Nigeria's economy. Financial institutions, businesses, and individual citizens lose billions of naira annually through phishing attacks, ransomware, identity theft, business email compromise, online banking fraud, and electronic payment scams. These financial losses discourage both local and foreign investment, reduce investor confidence, and negatively affect economic growth. Furthermore, the cost of recovering from cyberattacks places additional financial burdens on organizations and government agencies.

Political and Governance Implications

Cybersecurity threats have serious consequences for democratic governance and political stability. The increasing use of misinformation, fake news, hate speech, and disinformation campaigns through social media platforms has influenced public opinion, intensified political polarization, and weakened citizens' confidence in government institutions. During elections, cyber-enabled propaganda and manipulation of digital information may compromise electoral integrity and threaten democratic legitimacy.

National Defence and Sovereignty

Modern military operations depend heavily on digital communication systems, intelligence networks, satellite technologies, and information-sharing platforms. Cyberattacks targeting defence institutions can expose classified information, disrupt military communications, and weaken national defence capabilities. Foreign-sponsored cyber espionage also threatens Nigeria's sovereignty by compromising sensitive government information and strategic national assets.

Critical Infrastructure Vulnerability

Nigeria's critical infrastructure—including electricity, telecommunications, transportation, healthcare, banking systems, water supply, and oil and gas facilities—is increasingly dependent on digital technologies. Cyberattacks against these sectors can disrupt essential public services, cause widespread economic losses, and create national emergencies. Weak cybersecurity measures within these infrastructures expose the country to significant operational and security risks.

Social Implications

The widespread use of digital platforms has created opportunities for cyberbullying, identity theft, online radicalization, internet fraud, and digital harassment. These activities undermine public trust in digital technologies and contribute to fear, insecurity, and social instability. Terrorist organizations and criminal groups also exploit cyberspace for recruitment, propaganda, fundraising, and operational coordination, thereby expanding security threats beyond traditional physical boundaries.

Legal and Institutional Implications

Although Nigeria has enacted the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, and developed the National Cybersecurity Policy and Strategy, implementation challenges remain significant. Weak institutional coordination, inadequate funding, shortages of cybersecurity professionals, outdated technological infrastructure, and limited public awareness continue to constrain effective cybersecurity governance. These institutional weaknesses reduce Nigeria's capacity to prevent, detect, and respond to cyber threats effectively.

Educational and Human Capacity Implications

The shortage of trained cybersecurity professionals limits Nigeria's ability to protect its digital infrastructure. Universities and research institutions have only recently begun expanding cybersecurity education, while digital literacy among the general population remains relatively low. Without sustained investment in education, research, professional training, and public awareness campaigns, Nigeria will continue to face difficulties in developing a resilient cybersecurity workforce.

International Implications

Cyber threats transcend national borders, making international cooperation essential. Nigeria's reputation in global cyberspace has, at times, been affected by

cyber fraud activities, influencing international confidence in digital transactions. Strengthening cybersecurity governance and participating actively in regional and international cybersecurity initiatives will enhance Nigeria's credibility, improve intelligence sharing, and facilitate collaborative responses to transnational cybercrime.

Overall Implication

The study demonstrates that cybersecurity is no longer merely a technological issue but a strategic national security concern. The growing dependence on digital technologies means that successful cyberattacks can simultaneously affect economic development, political stability, national defence, public administration, and social welfare. Consequently, Nigeria must adopt a comprehensive cybersecurity strategy that integrates technological innovation, effective legislation, institutional reforms, public awareness, international cooperation, and continuous investment in cybersecurity infrastructure. Such an integrated approach will enhance national resilience, protect critical information infrastructure, and strengthen Nigeria's overall national security in the digital era. :::

6. Empirical Review

Adebayo and Obayan (2020) examined cybercrime and economic security in Nigeria and found that phishing, identity theft, and Business Email Compromise significantly undermine financial institutions and investor confidence. Okeshola and Adeta (2021) investigated cybersecurity preparedness among Nigerian public institutions. Their findings revealed inadequate cybersecurity infrastructure, insufficient funding, weak institutional capacity, and a shortage of skilled professionals. Muhammed (2022) studied digital misinformation during Nigerian elections and concluded that fake news and coordinated disinformation campaigns increased political polarization and weakened public trust in democratic institutions. Ndukwe (2023) evaluated Nigeria's cybersecurity governance and observed that despite existing laws and policies, poor implementation, inadequate funding, and weak inter-agency collaboration continue to limit cybersecurity effectiveness. Adeolu (2024) assessed cybersecurity vulnerabilities affecting Nigeria's critical infrastructure and found that financial institutions, telecommunications providers, healthcare facilities, transportation systems, and energy infrastructure remain highly vulnerable because of outdated technologies and limited investment in cybersecurity. International studies equally support these findings. ENISA (2023) reported that ransomware, phishing, supply-chain attacks, and social engineering remain among the most significant global cyber threats. IBM Security (2024) found that organizations increasingly experience higher financial losses due to data breaches, emphasizing the importance of proactive cybersecurity investment. The World Economic Forum (2024) further observed that Artificial Intelligence is transforming both cyber defence and cybercrime by improving automated detection while simultaneously enabling more sophisticated attacks.

7. Literature Gap

Although numerous studies have examined cybercrime, cybersecurity governance, and digital security in Nigeria, many focus primarily on financial fraud or institutional cybersecurity. Limited studies comprehensively assess the relationship between cybersecurity challenges and national security while examining the emerging role of Artificial Intelligence in strengthening cybersecurity and creating new security risks.

Furthermore, few studies integrate Systems Theory, National Security Theory, and Deterrence Theory to explain Nigeria's cybersecurity environment. This study addresses these gaps by providing a comprehensive assessment of cybersecurity challenges, their implications for national security, and the contribution of Artificial Intelligence to Nigeria's cyber resilience.

8. Summary of Literature Review

The reviewed literature demonstrates that cybersecurity has become an indispensable component of national security in Nigeria. Existing studies agree that cybercrime, ransomware, phishing, cyber espionage, misinformation, and attacks on critical infrastructure threaten economic stability, governance, and public safety. The literature also shows that Artificial Intelligence offers significant opportunities for improving cybersecurity through automated threat detection and predictive analytics, while simultaneously creating new risks through AI-enabled cyberattacks. The review further establishes that effective cybersecurity requires strong institutional capacity, adequate funding, modern technologies, skilled professionals, effective legislation, public awareness, and international cooperation. These findings provide the foundation for the present study, which assesses cybersecurity challenges and their implications for national security in Nigeria.

Theoretical Review

Systems Theory

Systems Theory, developed by Ludwig von Bertalanffy, explains that society consists of interconnected systems whose components depend on one another. Applied to cybersecurity, disruption within banking, telecommunications, energy, or government information systems can produce cascading effects throughout the national economy and governance structure.

National Security Theory

National Security Theory argues that governments have the responsibility to protect national sovereignty, citizens, strategic assets, and public institutions against emerging threats. Modern national security recognizes cyberspace as a strategic domain requiring strong legal frameworks, technological capabilities, intelligence gathering, and institutional coordination.

Deterrence Theory

Deterrence Theory suggests that crime can be minimized when offenders believe they are likely to be detected, prosecuted, and punished. Within

cybersecurity, deterrence includes strong cybercrime legislation, effective law enforcement, cyber intelligence, digital forensics, and international cooperation.

These theories collectively explain the importance of coordinated cybersecurity governance in protecting Nigeria's national security.

METHODOLOGY

Research Design

This study adopted a qualitative descriptive research design based on documentary analysis. The qualitative approach was considered appropriate because the study sought to examine cybersecurity challenges and their implications for national security in Nigeria through an in-depth analysis of existing literature, government publications, policy documents, and institutional reports. Documentary analysis enabled the researcher to obtain comprehensive information on cybersecurity trends, legal frameworks, institutional responses, and emerging technologies such as Artificial Intelligence (AI). The design was suitable because it allowed for the systematic interpretation of secondary data without manipulating any variables.

Sources of Data

The study relied entirely on secondary sources of data. Information was obtained from credible and authoritative materials, including:

- Peer-reviewed journal articles on cybersecurity and national security;
- Books and academic textbooks;
- Government publications and policy documents;
- The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015;
- The National Cybersecurity Policy and Strategy;
- Publications of the Office of the National Security Adviser (ONSA);
- Reports from the National Information Technology Development Agency (NITDA);
- Reports of the Nigerian Communications Commission (NCC);
- Reports of the Nigeria Computer Emergency Response Team (ngCERT);

Publications from international organizations such as the International Telecommunication Union (ITU), International Monetary Fund (IMF), World Bank, United Nations (UN), INTERPOL, and Cisco.

These sources provided current and reliable information on cybersecurity threats, institutional frameworks, and their implications for Nigeria's national security.

Method of Data Collection

Data were collected through systematic documentary review. Relevant literature and official documents published between 2015 and 2025 were carefully identified through academic databases such as Google Scholar, Scopus, ResearchGate, JSTOR, and institutional websites. Priority was given to recent publications,

government documents, and internationally recognized reports to ensure the reliability and relevance of the information used in the study.

Method of Data Analysis

The collected data were analyzed using qualitative content analysis. The researcher carefully examined the documents, identified recurring themes, categorized the information, and interpreted the findings in relation to the objectives of the study. The analysis focused on:

- Major cybersecurity threats confronting Nigeria;
- Implications of cyber threats for national security;
- Existing cybersecurity laws, policies, and institutional frameworks;
- The role of Artificial Intelligence in cybersecurity;

Strategies for improving cybersecurity and national security.

The findings were presented descriptively and supported with evidence from existing literature and official reports.

eria.

Validity and Reliability of Data

To enhance the credibility of the study, only information obtained from credible academic publications, government agencies, and recognized international organizations was utilized. Data were cross-checked across multiple sources to ensure consistency, accuracy, and reliability. The use of authoritative documentary sources strengthened the validity of the study's findings and conclusions.

Ethical Considerations

Since the study relied exclusively on secondary data, no human participants were involved. Ethical standards were maintained by accurately acknowledging all sources of information through appropriate APA 7th edition referencing, avoiding plagiarism, and ensuring faithful representation of the original authors' ideas and findings.

This methodology is appropriate for a scholarly research paper and aligns with the objectives, research questions, and qualitative nature of your study on "Assessment of Cybersecurity Challenges and Their Implications for National Security in Nigeria."

DISCUSSION/ANALYSIS

The findings from the reviewed literature indicate that cybersecurity has evolved from a purely technological concern into a strategic national security issue in Nigeria. The rapid digitalization of government services, financial institutions, telecommunications, education, and critical infrastructure has significantly expanded the country's cyber-attack surface. While digital transformation has enhanced economic development and governance, it has simultaneously increased vulnerabilities that threaten national security.

The reviewed studies consistently reveal that cybercrime—including phishing, ransomware, business email compromise, identity theft, financial fraud, and cyber-enabled terrorism—continues to undermine Nigeria's economic stability and institutional resilience. These threats affect not only individuals and private organizations but also government agencies and critical national infrastructure. Weak cybersecurity governance, inadequate investment in digital security technologies, shortage of skilled cybersecurity professionals, poor inter-agency collaboration, and limited public cyber awareness further compound these challenges.

The analysis also demonstrates a close relationship between cybersecurity and emerging technologies such as Artificial Intelligence (AI). AI has become a powerful tool for strengthening cybersecurity through automated threat detection, predictive analytics, anomaly detection, malware identification, biometric authentication, and real-time incident response. AI-driven security systems can rapidly identify suspicious network activities, detect cyber intrusions before they escalate, and support intelligence-led national security operations. For Nigeria, integrating AI into national cybersecurity architecture offers significant opportunities to improve cyber resilience, protect critical infrastructure, and enhance national defense capabilities.

However, the deployment of AI also introduces new cybersecurity risks. Cybercriminals increasingly exploit AI technologies to develop sophisticated phishing attacks, deepfake videos, automated malware, social engineering campaigns, and intelligent hacking tools. Consequently, Nigeria must adopt balanced cybersecurity policies that maximize AI's defensive capabilities while regulating its misuse through effective legislation, ethical governance, and institutional oversight.

Furthermore, the discussion aligns with Systems Theory, which explains that Nigeria's digital ecosystem functions as an interconnected system where a successful cyberattack on one sector, such as banking or telecommunications, can trigger cascading disruptions across multiple sectors. Likewise, National Security Theory reinforces the government's responsibility to safeguard cyberspace as an essential component of national sovereignty, while Deterrence Theory emphasizes the importance of strong legal sanctions, effective law enforcement, and advanced cyber defense mechanisms to discourage cybercriminal activities.

The analysis further suggests that strengthening Nigeria's cybersecurity posture requires a multidimensional strategy that combines technological innovation, institutional reforms, human capacity development, and international cooperation. Continuous training of cybersecurity professionals, increased investment in AI-enabled cyber defense systems, implementation of the National Cybersecurity Policy and Strategy, enforcement of the Cybercrimes Act, and collaboration with regional and international cybersecurity organizations are essential for building a resilient digital ecosystem.

Overall, the evidence demonstrates that cybersecurity has become indispensable to Nigeria's national security agenda. As digital technologies continue to reshape governance, commerce, education, and security, protecting cyberspace must remain a national priority. A resilient cybersecurity framework supported by Artificial Intelligence, effective public policy, robust institutional capacity, and active

stakeholder collaboration will significantly enhance Nigeria's ability to prevent, detect, respond to, and recover from evolving cyber threats while promoting sustainable national development and Security.

CONCLUSION

This study assessed the cybersecurity challenges confronting Nigeria and examined their implications for national security using a qualitative descriptive research design based on documentary analysis. The findings demonstrate that cybersecurity has evolved from a purely technological concern into a strategic national security issue that affects governance, economic development, public safety, and the protection of critical national infrastructure.

The study revealed that Nigeria faces a wide range of cyber threats, including phishing, ransomware, identity theft, business email compromise, cyber espionage, cyber-enabled terrorism, misinformation, distributed denial-of-service (DDoS) attacks, and attacks on critical national infrastructure. These threats have resulted in significant financial losses, disruption of essential public services, and erosion of public confidence in digital systems, and increased risks to national sovereignty and economic stability.

The study further established that despite the existence of legal and institutional frameworks such as the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, the National Cybersecurity Policy and Strategy, the Office of the National Security Adviser (ONSA), the National Information Technology Development Agency (NITDA), the Nigerian Communications Commission (NCC), and the Nigeria Computer Emergency Response Team (nicer), effective cybersecurity governance is constrained by inadequate funding, weak implementation of policies, shortage of skilled cybersecurity professionals, obsolete technological infrastructure, poor public cyber awareness, and insufficient collaboration among relevant stakeholders.

Furthermore, the study found that Artificial Intelligence (AI) has become both an opportunity and a challenge for cybersecurity. While AI enhances cyber defence through automated threat detection, predictive analytics, behavioural analysis, malware detection, biometric authentication, and rapid incident response, it is also increasingly exploited by cybercriminals to launch sophisticated phishing campaigns, generate deep fake content, automate malware, and conduct intelligent cyberattacks. Consequently, AI governance must accompany technological innovation to ensure that its benefits outweigh its risks.

The theoretical foundations of the study—Systems Theory, National Security Theory, and Deterrence Theory—demonstrate that cybersecurity is an interconnected national responsibility requiring coordinated action by government institutions, private organizations, security agencies, educational institutions, and international partners. Since disruption in one sector can produce cascading effects across the entire national system, cybersecurity must be integrated into Nigeria's broader national security and development agenda.

In conclusion, achieving effective cybersecurity in Nigeria requires sustained investment in modern technologies, stronger institutional capacity, effective enforcement of cybersecurity laws, continuous public awareness, development of

skilled human resources, and enhanced regional and international cooperation. Strengthening these areas will improve Nigeria's cyber resilience, protect critical national infrastructure, support digital transformation, and promote sustainable national security and economic development.

Recommendations

Based on the findings of this study, the following recommendations are made:

1. **Strengthen Cybersecurity Governance:** The Federal Government should ensure the effective implementation and periodic review of the National Cybersecurity Policy and Strategy and strengthen enforcement of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.
2. **Increase Investment in Cybersecurity Infrastructure:** Government agencies and private organizations should allocate adequate financial resources for modern cybersecurity technologies, secure digital infrastructure, cyber threat intelligence, and incident response capabilities.
3. **Promote Artificial Intelligence for Cyber Defence:** Nigeria should adopt AI-powered cybersecurity solutions for automated threat detection, predictive analytics, intrusion detection, malware analysis, and real-time cyber incident response while establishing regulatory frameworks to prevent the misuse of AI by cybercriminals.
4. **Develop Human Capacity:** Universities, research institutions, and professional organizations should expand cybersecurity education, certification programmes, and specialized training to address the shortage of qualified cybersecurity professionals.
5. **Enhance Public Cybersecurity Awareness:** Continuous nationwide awareness campaigns should educate citizens, public servants, students, and businesses on safe online practices, phishing prevention, password management, data protection, and responsible use of digital technologies.
6. **Strengthen Inter-Agency Collaboration:** Government institutions responsible for cybersecurity—including ONSA, NITDA, NCC, niger, law enforcement agencies, and intelligence organizations—should improve information sharing, joint operations, and coordinated responses to cyber incidents.
7. **Protect Critical National Infrastructure:** Operators of critical sectors such as finance, telecommunications, and healthcare, transportation, energy, and government services should implement internationally recognized cybersecurity standards, conduct regular vulnerability assessments, and establish robust business continuity and disaster recovery plans.
8. **Strengthen International Cooperation:** Nigeria should deepen collaboration with regional and international organizations, including the African Union, INTERPOL, ECOWAS, the International Telecommunication Union (ITU), and the United Nations, to improve intelligence sharing, cybercrime investigations, capacity building, and adoption of global cybersecurity best practices.
9. **Support Cybersecurity Research and Innovation:** Government should increase funding for cybersecurity research, digital innovation, and local technology

development while encouraging collaboration among universities, research institutes, and the private sector.

10. Establish Continuous Monitoring and Evaluation: Regular cybersecurity audits, risk assessments, policy evaluations, and national cyber resilience exercises should be conducted to ensure that cybersecurity strategies remain effective against evolving cyber threats.

REFERENCE

- Andress, J. (2019). The basics of information security: Understanding the fundamentals of InfoSec in theory and practice (3rd Ed.). Syngress.
- ENISA. (2023). ENISA threat landscape 2023. European Union Agency for Cybersecurity.
- International Telecommunication Union. (2023). Global cybersecurity index 2023. ITU Publications.
- Kshetri, N. (2021). Cybercrime and cybersecurity in Africa. Palgrave Macmillan.
- National Information Technology Development Agency. (2023). Nigeria data protection framework and cybersecurity guidelines. NITDA.
- National Information Technology Development Agency. (2023). Nigeria data protection act implementation framework. NITDA.
- National Security Adviser. (2021). National cybersecurity policy and strategy. Office of the National Security Adviser.
- Nigerian Communications Commission. (2023). Annual report and financial statements 2023. NCC.
- Nigerian Computer Emergency Response Team. (2023). Annual cyber threat report 2023. Nicer.
- NIST. (2024). Cybersecurity framework (CSF) 2.0. National Institute of Standards and Technology.
- OWASP Foundation. (2021). OWASP Top 10: The ten most critical web application security risks. <https://owasp.org/www-project-top-ten/>
- Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. W. W. Norton & Company.
- Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know? Oxford University Press.
- Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th Ed.). Pearson.
- United Nations Office on Drugs and Crime. (2023). Comprehensive study on cybercrime. United Nations.
- Von Solms, B., & Van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security*, 38, 97–102.
- World Economic Forum. (2024). Global cybersecurity outlook 2024. World Economic Forum.
- IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation.
- Microsoft. (2024). Microsoft digital defense report 2024. Microsoft Corporation.
- Cisco. (2024). Cisco cybersecurity readiness index 2024. Cisco Systems.

- ISACA. (2023). State of cybersecurity 2023. ISACA.
- World Bank. (2021). World development report 2021: Data for better lives. World Bank.
- Whitman, M. E., & Mattord, H. J. (2022). Principles of information security (7th Ed.). Cengage Learning.
- . (2014). African Union Convention on Cyber Security and Personal Data Protection. African Union.
- . (2024). Cisco Cybersecurity Report 2024. Cisco Systems.
- . (2023). Cybersecurity Best Practices. U.S. Department of Homeland Security.
- . (2015). Cyber crimes (Prohibition, Prévention, etc.) Acta, 2015. Federal Government Printer.
- . (2021). National Cybersecurity Policy and Strategy. Office of the National Security Adviser.
- . (2023). Global Cybersecurity Index 2023. ITU.
- . (2023). Nigeria Data Protection Framework and Cybersecurity Guidelines. NITDA.
- . (2023). Annual Cyber Threat Report. Nicer.
- . (2023). Annual Report and Financial Statements. NCC.
- . (2021). National Cybersecurity Policy and Strategy. ONSA.
- . (2021). OWASP Top 10: The Ten Most Critical Web Application Security Risks. OWASP Foundation.
- . (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton.
- . (2020). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley.
- . (2024). Global Cybersecurity Outlook 2024. World Economic Forum.
- . (2023). Comprehensive Study on Cybercrime. United Nations.
- . (2024). Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce.
- . (2024). Cost of a Data Breach Report 2024. IBM Security.
- . (2024). Microsoft Digital Defense Report 2024. Microsoft Corporation.