Published by

British Journal of Contemporary Research

BEXFORD PUBLISHING

# Digital Transformation And Emerging Cyber Threats: Assessing Vulnerabilities In Nigeria's Security Sector

**Original Research Article | Volume 1 | Issue 3 | 2026 | Article Number: 043**

**Accepted: 04 August 2026 | Published: 10 August 2026 | ISSN: 2979-8582 (Online)**

Crossref : **https://doi.org/10.67693/BJCR-UQPMTDPC**

**Obinna Ukaeje[1], Igboeli Uchenna[2], Ekoh Kolawole Oluwatosin[3]**

[1]Defence and Security Studies, Center for Strategic Research and Studies, National Defence College , Nigeria,
[2]Department of Computer Science, University of Abuja, Nigeria
[3]Irregular Warfare Centre, National Defence College, Abuja, Nigeria

OU 0000-0002-7231-168X

Correspondence: Obinna Ukaeje, obinnaukaeje@yahoo.com

## Abstract

The utilization of digital technologies in Nigeria's security sector has enhanced Intelligence Surveillance and Reconnaissance (ISR), border security and control, communication, and law enforcement. Nonetheless, it has also heightened vulnerability to advanced cyber threats aimed at government systems and critical infrastructure. Malicious actors like criminals, hacktivists, terrorist organizations, and government-backed groups are taking advantage of these weaknesses in networks, databases, and communication systems to carry out their nefarious activities. This research examines new cyber threats and vulnerabilities in the sector through a qualitative method relying on literature, reports, and policy documents. Results indicate that significant dangers encompass ransomware, phishing, cyber espionage, political disinformation and misinformation, etc. Key vulnerabilities consist of outdated systems, lack of cybersecurity awareness, inadequate regulatory compliance, insufficient funding, and a deficit of skilled workers. Despite these obstacles, the research underscores opportunities including Artificial Intelligence (AI), Machine Learning, Zero Trust Models, Cyber threat intelligence systems, and enhanced governance. It determines that a unified national cybersecurity approach and heightened investment in technology and human resources are crucial for bolstering Nigeria's cybersecurity resilience. The research is anchored on the Diffusion of Innovation Theory (DIT) for its analysis.

**Keywords:** Cybersecurity, Cyber Threats, Cyber Resilience, Critical Infrastructure, Artificial Intelligence, Security Sector, Intelligence Surveillance and Reconnaissance

 

## INTRODUCTION

The advent of the 21st century, which coincided with the rise of Information Communication Technology (ICT), has brought about accelerated changes that are disrupting existing systems in almost every sector of human activity. One of such changes is the optimisation of digital infrastructure such as the internet, mobile devices and software applications, to improve socio-economic sectors and enhance global security. Consequently, governments around the globe have progressively embraced these technologies to enhance governance, service provision, intelligence activities, and management of national security. Nigeria is not left out of this innovative transformation, as it has adopted digital transformation through numerous initiatives aimed at modernising public institutions and bolstering security operations. These include Nigerian National Broadband Plan (NNBP) 2013-2018, aimed at international connectivity, national backbone network, metropolitan and local access network; the National Digital Economy Policy and Strategy (NDEPS) 2020-2030 under the Federal Ministry of Communication and Digital Economy, to provide the federal roadmap and mandate needed for digital transformation in Nigeria; the National Digital Economy and E-Governance Act, 2024, to enable the growth of digital economy and digital governance in Nigeria by improving the certainty of digital transactions, digital service delivery, and related matters; the Cybercrimes Prohibition and Prevention Act (CPPA), which was signed into law in 2015 and amended in 2024; and the Nigeria Data Protection Act 2023, whose objective is to provide protection and legal backing for personal and corporate data protection against cybercriminals. These policies and laws provided the needed roadmap, frameworks, mandates and legal backing that facilitated the integration of Nigeria's economy and governance into the global digital ecosystem

Subsequently, several sectors of the economy have expanded their operations to include digital services, such as the e-governance tools in states like Lagos and Enugu, and the deployment of command-and-control fusion centres for counter-insurgency and counter-terrorism operations like the National Counter Terrorism Centre (NCTC) and the Nigerian Defence Space Administration, as well as the communication tracking system in the Nigerian Police Headquarters. Presently, Nigeria's security and defence agencies such as the Defence Intelligence Agency (DIA), the Nigerian Police Force (NPF), Department of State Service (DSS), Nigeria Intelligence Agency (NIA) and the Office of the National Security Adviser have established and integrated digital platforms for surveillance, data management, communication, and cyber defence to enhance defence and security. As a result, operational efficiency has been significantly optimized, proactive threat detection enabled, and rapid data-driven decision-making facilitated in Nigeria's security sector (Aliuba et al., 2025; Momoh & Kefas, 2025).

While digital transformation has significantly enhanced operational efficiency, it has increased exposure to cyber threats, as critical national infrastructure and digital databases have been subjected to attacks by criminals. The CYFIRMA 2025 report on cyber threats in Nigeria noted that Dark Web and Russian forum actors were observed actively selling banking databases, stolen credentials, and facilitating unauthorised access to Nigerian financial institutions, including the Chartered Institute of Bankers of Nigeria (CIBN) and Princeps Credit Systems Limited, which suffered a ransomware attack by Killsec (CYFIRMA, 2025). Telecom data sales were reported to be rampant, with claims of over 60 million Nigerian records being traded, while government agencies, including the Lower Niger River Basin Development Authority and the Nigerian Navy, were also reported to have been targeted, with sensitive internal data leaked (CYFIRMA, 2025). Healthcare records were not spared as data comprising 130,000 patient entries were exposed, highlighting risk to personal data privacy and raising concerns over Nigeria's broader critical infrastructure security. Most recently, Boko Haram and Islamic State West Africa Province (ISWAP) terrorists in Nigeria have adopted commercial drones to gather intelligence, monitor events and conduct attacks, representing a dangerous aspect of digital transformation (Dunamis, 2025).

 

Incidentally, these incidents occurred not because there are no efforts at protecting and securing Nigeria's digital space, as the federal government has put in place measures to ensure effective protection of the digital space such as the Nigeria Computer Emergency Response Team (ngCERT) to manage the risks of cyber threats in Nigeria's national cyberspace and coordinate incident response across government, private sector, and critical infrastructure (ngCERT, 2016); National Data Protection Act 2023, the Cybercrime Prohibition and Prevention Act 2024 as amended, and the Executive Order No.21 passed by President Bola Ahmed Tinubu on the 24th of June 2024 on the Designation and Protection of Critical National Information Infrastructure (DPCNII), which makes it an offense to damage critical national information assets (DPCNII Order No. 21, 2024). In light of the above gaps, the study examines digital transformation and emerging cyber threats in Nigeria's security sector, so as to identify emerging cyber threats, assess the vulnerabilities in Nigeria and proffer actionable policy recommendations to improve the protection of Nigeria's cyber security space. To achieve this, the study is divided into different sections: the methodology of the study, literature review and theoretical framework, emerging cyber threats and vulnerabilities in Nigeria's digital space, and policy recommendations to enhance government efforts.

## METHODOLOGY

The paper adopts a qualitative and non-empirical approach rooted in interpretive analysis. Data sources include government digital policy documents, cybersecurity protection acts, and international laws on cybersecurity and digital transformation. Others include research publications such as textbooks, journal publications, and digital transformation reports from national and international monitors from 2020 to 2026. These were analysed using thematic content analysis, which identified recurring themes related to the integration of digital technology in Nigeria's security sector, enabling a critical examination of the diverse perspectives that support the development of a nuanced conceptual framework.

## LITERATURE REVIEW AND THEORETICAL FRAMEWORK

The critical concepts considered important to this discourse are digital transformation, emerging cyber threats, and the security sector. Efforts were made in this section to explain these concepts, tracing their backgrounds, ensuring clarity and familiarity, and positioning the paper within the broader scholarly conversation to ensure its significance.

### *Digital transformation*

Digital transformation is a new concept triggered by the intensified prevalence and use of digital technologies that are fundamentally changing organizations and economies. Although it is frequently used in business research and marketing, scholars disagree on a common definition (Siachou et al., 2021). However, many of the scholars approach the definition of digital transformation from a technological or value-based angle (Xiaoli & Weiqing, 2022). Scholars like Berman (2012), Horlacher et al (2016), and Guler and Buyukozkan (2019) see it as the leveraging of digital technologies by an organisation to remain abreast of current realities in the business landscape, which would undoubtedly lead to improved customer experience. In their view, enhanced customer service is the by-product of adopting digital transformation and utilizing them in an organization's business processes.

To Gray and Rumpe (2017), it is the gamut of steps through which data is processed and assessed with the intent of providing stakeholders with relevant information that could help improve their processes and products. This definition is similar to the understanding of digital transformation by Berman (2012), Horlacher et al (2016), and Merve Guler et al (2019), which implies that the application of digital transformation leads to key feedback that can facilitate product enhancement. Similarly, Morankanyane et al (2017) allude that digital transformation is a system that takes advantage of the capabilities inherent in

 

the digital sphere to improve operational processes in business models to better customer experience, a definition which is akin to the perspective espoused by Merve Guler et al.

Incorporating digital transformation into the existing structure is advantageous as its benefits could be seen across diverse sectors (Bertola & Teunissen, 2018). This view is supported by Kraus et al (2021), who opine that digital transformation is capable of considerably enhancing efficiency, productivity and competitiveness through modifying work processes and operations. This has been proven by several studies on digital transformation in various sectors, including the security sector, where drones, centralized command centres and Artificial Intelligence-powered capabilities such as video detection, real-time alerts, incident analysis, technology integration have been used to enhance operations (Airbus, 2026). It is on this basis that Xiaoli and Weiqing (2022) conclude that the concept of digital transformation is better approached from a technological or value-based angle.

***Emerging Cyber Threats***

Analysis of several works on the subject of cyber security has shown that the term "emerging cyber threats" has not been duly conceptualized. However, most studies agree that emerging cyber threats cover a broad spectrum of malicious activities that can be conducted over the cyber space. Wheeler (2011) notes that in the context of information security risks, the threats generally describe the source of the attack and also the activity or means of attack. Essentially, the threat source has the potential to harm the resource, and the threat activity is the way in which it will be harmed. He further grouped cyber security threats into several categories, including natural disaster, infrastructural failure, internal abuse, accident, external targeted attack and external mass attack.

The above view was upheld by Luiijf (2014) who opines that any information communication technology innovation cycle will result in new threats to end-users and society. He notes that new ICT inventors focus on the new functionality, increased efficiency and effectiveness of people and organizations, and ease of use, but lack any historical understanding of previous design failures and of earlier lessons identified in good coding practices. He believes that emerging cyber threats can be predicted in new fields of ICT, especially where ICT is deeply embedded in functional systems, noting that they are often old threats disguised in a new look. He concluded that these threats allow cybercriminals, hacktivists, cyber spies, and states to enter ICT-based systems in an unauthorized way.

It is in light of the above that Borges (2024) refers to emerging cyber threats as new tactics, techniques, and procedures (TTPs) that criminals employ to exploit, disrupt, or breach security systems. According to him these threats constantly evolve, making them harder to predict and mitigate. He further identified emerging cyber threats to include sophisticated malware, ransomware, social engineering tactics and advanced persistent threats (APTs). He noted that as technology advances, so are the threats, leveraging the latest developments in artificial intelligence (AI), machine learning, and Internet of Things (IoT) devices to carry out their malicious activities.

Going by the understanding of the concept of emerging cyber threat, we can infer that it refers to a new or evolving source of attack or risk that has the potential to harm a system or organization. It includes novel attack techniques, sophisticated attackers, or vulnerabilities that are not yet widely known or addressed, which hackers and cybercriminals leverage to compromise digital innovations. There is therefore a need to ensure that every loophole that can serve as a gateway for cyber criminals to penetrate is effectively blocked and protected.

***Security Sector***

The concept of the security sector encompasses all the structures, institutions, and personnel responsible

 

for maintaining internal and external security, upholding the rule of law, and providing justice. Its primary objective is to ensure the protection of the state and its citizens (DCAF, 2015). According to Organization for Economic Cooperation and Development (OECD)/Development Assistance Committee (DAC) (2005) a comprehensive security sector comprises four main categories, which includes [a]core security actors (such as the armed forces); law enforcement agencies – Police, Gendarmeries, Border Security Guards); Intelligence service (Civilian and military intelligence agencies); and Other Agencies such as Custom Services, Immigration Services, Prison Services etc., [b] Management and Oversight bodies such as the executive and legislature, financial authorities (finance ministries and budget/audit offices that oversee funding), and Civil Society Organizations (CSOs); [c] Justice and Rule of Law, comprising judiciary and Ministry of Justice, Penal systems, and Human Rights Commissions, and [4] Non-Statutory Security Forces like private security companies and non-state armed groups like guerrilla armies, liberation forces and local political militias. However, the study is limited to the core security actors, which comprises the Armed Forces of Nigeria (AFN), the Police and other security agencies including the intelligence community as its security sector focus, so as not to digress into areas that are not relevant to our study. As such emphasis would be on the digital transformation in these security organizations and the vulnerabilities that have allowed emerging cyber threats and attacks on their systems.

## THEORETICAL FRAMEWORK

The analysis of this study is anchored on the Diffusion of Innovation Theory (DIT) developed by Professor Everette Rogers of the University of New Mexico in the United States of America (USA) and Professor James Dearing of Michigan State University, USA in 1962. The theory emphasises that technological innovations such as digital transformation impacts significantly in the growth and development of an economy through certain channels over time among members of a social system (Rogers, 1995). According to Rogers cited in Hoffman, Probst, and Christinck (2007), as innovations spread through a society, it becomes gradually embraced by an increasing number of people over the period. He further identifies the attributes of DIT that make it easily permeable in a society include relative advantage of the innovation, compatibility, less complexity, and ability to be tested as well as observed (Rogers, 1995). Accordingly, if an innovation has these attributes, it will permeate a society and impact it in a transformative pattern. However, the speed of adoption often outpaces security measures, creating significant threats and structural vulnerabilities across users.

Empirical studies of the DIT have shown that while there is a relationship between the spread of innovative technology and its impact on the socioeconomic life of a society, there are also significant threats and imbalances associated with such innovation (Lile, Ansari, & Urmetzer, 2025). This explains why Lyytinen and Damsgaard (2001), Greenhalgh et al., (2008) opined that the theory might not be suitable in explaining the adoption of complex and networked information technology (IT) solutions. However, the criticisms were largely attributable to the level of complexity of the innovation, which does not make the theory invaluable for this research, as it proffers solutions on how a social system can overcome the threats and vulnerabilities that are likely to accompany technological innovations like that of digital transformations, which include identifying such threats and creating solutions to manage them. This thus aligns with Professor Rogers and Professor Dearing's Diffusion of Innovation Theory, explaining the process by which an innovation is communicated through certain channels over time among members of a society.

### Overview of Digital Transformation in Nigeria's Security Sector

The idea of the digitalization of Nigeria's security sector is underpinned in the global digital transformation initiative propelled by the spread of the internet. As a result of this global transformation,

 

several sectors of the economy were absorbed into the digital transformation agenda, ushering the country into the global digital revolution. With the Nigerian economy being absorbed into the digital ecosystem, resulting in electronic transactions and service deliveries, such as e-commerce and e-governance systems, the security sector was not left behind. The Federal Government of Nigeria (FGN) had pushed for a digitalized sector that would utilize digital tools to address security challenges and threats. On May 13, 2007, the NIGCOMSAT-1 was launched. The aim was to build an Intelligence Surveillance and Reconnaissance (ISR) satellite system to provide efficient satellite communication and imagery intelligence for security agencies. However, one year into the launch of NIGCOMSAT-1, it was shut down due to technical problems (Agency France-Presse, 2008).

With the rise of Boko Haram insurgency in 2009 and the attendant acts of terrorism that followed across the northern region, it became obvious that the traditional analogue system can no longer be sufficient for the challenges, due to lack of real-time intel capability to ensure effective satellite communication and imagery intelligence: the analogue security structure cannot effectively track and monitor the movement and operations of the terrorists, leading to the escalation of violent attacks across the northern region and Abuja. On December 19, 2011, NIGCOMSAT-1R was launched to replace the failed and de-orbited NIGCOMSAT-1, signalling the restoration of Nigeria's lost satellite communication and imagery capability (Okonji, 2026). It also marked a strategic step towards security sector digitalisation, complementing the existing traditional analogue operational system. However, insecurity continues to increase, spreading down to the Lake Chad Basin and other parts of the country.

In 2014, precisely in April, Boko Haram expanded its strategy to include the abduction of school children, resulting in the abduction of over 200 Chibok school girls in Borno State in April without a trace (Saleh & Ukaeje, 2024). The abduction of Chibok school girls caused a serious international embarrassment to the federal government and its security forces, as the country could not explain the whereabouts of the abducted school children, due to a lack of integrated ISR. This therefore called for urgent and expedient action for the federal government to restore its satellite ISR capability for enhanced intelligence and surveillance operations. Moreover, as digitalization evolved, security concerns also evolved, resulting in several security concerns in Nigeria's cybersecurity space and a national need to have laws that would ensure the protection and acceptance of digital forensics, electronic evidence, and the protection of digital databases in Nigeria.

In May 2015, the Cybercrime Prohibition and Prevention Act (CPPA) was signed into law and amended in 2024, making it possible for Nigerian security agencies to trace NIN and SIM cards, monitor and prosecute drone footage, and empower anti-graft agencies like the Economic and Financial Crimes Commission (EFCC) to seize crypto networks (CPPA, 2024). The Act did three important things for security operatives: [a] it criminalized digital acts like hacking, online terror and attacks, and identity theft; [b] legalized digital investigation, including interception, data requests, and e-evidence; and [c] mandated infrastructure development to monitor and protect government websites, data retention, and breach reporting (Cybercrime Act, 2024). Accordingly, in September 2016, the Office of the National Security Adviser (ONSA) launched the Nigeria Computer Emergency Response Team (ngCERT), to manage the risks of cyber threats in Nigeria's national cyberspace and coordinate incident response across government, private sector, and critical infrastructure (ONSA, 2016). Despite these efforts, over 60 per cent of Nigerian businesses were reported to have experienced cyberattacks with estimated losses of N127 billion in 2018, thus impacting on the financial security of the country (Osagwu, 2019).

In furtherance of the efforts at ensuring security and protection of data in Nigeria, the federal government, on January 25, 2019, through the National Information Technology Development Agency (NITDA), established the Nigeria Data Protection Regulation (NDPR), as the foundational framework for data

 

privacy. The core objectives of the NDPR are safeguarding the privacy rights of Citizens, fostering safe transactions, preventing data manipulation, and strengthening global competitiveness by aligning national corporate practices with global data protection regulations to ease global trade (NDPR, 2019). While it remains active alongside its 2020 Implementation Framework, its provisions are now fully subordinated to and integrated into the Nigeria Data Protection Act (NDPA) 2023 and overseen by the Nigeria Data Protection Commission. This, amongst others, makes cybersecurity a crucial factor for consideration in digital transformation and emerging cyber threats in Nigeria.

Recognizing the crucial role of digital transformation in Nigeria's security sector, the military and other security agencies have begun the development of digital command sectors to support the traditional analogue operational structure, such as the Nigerian Army Cyber Warfare Command established in 2018, dedicated as the first military cyber unit that signalled shift in military doctrine; the Nigerian Navy Falcon Eye System established in 2018, as the first integrated maritime domain awareness network, the Nigerian Air Force Unmanned Aerial Vehicle (UAV) Command Networks, and the Joint Service (Army-Navy-Air Force) Command and Control Centre for live ISR feeds and interdiction operations (C4ISR) built in 2019 at the Defence Space Administration (DSA) located at the Obasanjo Space Centre, Abuja.

Others include the Nigerian Police Force National Command and Control Centre (NPF-C4i) and Electronic Central Motor Registry (e-CRMS), to enhance national security, motor vehicle data, and coordinate emergency responses, the Nigeria Immigration Services electronic gates (NIS e-gates) system, a biometric border control operation at international airports in Nigeria and the NCTC domiciled in the ONSA to monitor, track and coordinate counterterrorism and counterinsurgency operations, using a highly digitalized security system. Despite the tremendous achievements of these initiatives to enhance operational effectiveness in Nigeria's security sector, advancements in the digital ecosystem coupled with vulnerabilities in Nigeria's digital space have made it difficult to effectively secure and protect the nation's cybersecurity space, resulting in heightened security concerns. These vulnerabilities and the emerging cyber threats will be addressed in the subsequent section.

**Emerging Cyber Threats and Vulnerabilities in Nigeria's Security Sector: An Assessment**

Nigeria has experienced swift advancement in digital governance through efforts like electronic tax management, biometric identification systems, digital payment solutions, and e-government service, including digital platforms for operations in the security sector. Though these efforts have enhanced public service delivery and security operations, they have simultaneously heightened cybersecurity threats thereby undermining efforts at improving public service delivery as well as the management of national security. Studies indicate that numerous Nigerian government bodies and critical infrastructure encounter issues stemming from ransomware attacks, data breaches from Distributed Denial of Service (DDoS) attacks, Dark Web Leaks, and politically driven disinformation and misinformation (CYFIRMA, 2025; Deloitte Nigeria Cybersecurity Outlook, 2025). The Deloitte Nigerian Cybersecurity Outlook (2025) observed that the year 2024 recorded a surge in cyber threats, with organizations facing unprecedented challenges ranging from ransomware attacks to insider threats. It identified the emerging cyber threats to include, AI automated Phishing nets, which create polymorphic malware that evade detection and craft hyper-realistic deepfakes that attack databases, noting that malicious actors and cybercriminals are increasingly using it to undermine institutional databases, particularly government institutions and critical infrastructure. The report, however, noted that the increasing sophistication of cybercriminals has left no sector immune, highlighting the urgent need for proactive security measures.

Corroboratively, the 2025 CYFIRM report on Cyber Threat Assessment on Nigeria highlighted the major cyber threat incidents that occurred in 2025, to include banking data breaches, telecom data breaches,

 

government data breaches, healthcare data breach, and critical infrastructure leak. The report observed that between January and September 2025, Nigeria experienced a surge in data breaches and cybercrime activities across banking, telecom, government, healthcare, and critical infrastructure sectors, confirming the increasingly emerging cyber threats. It further stated that dark web and Russian forum actors were observed actively selling banking databases, stolen credentials, and unauthorized access to Nigerian financial institutions, including the Chartered Institute of Bankers of Nigeria and Princeps Credit Systems Limited, which suffered a ransomware attack by killsec. Telecom data sales were also reported to be rampant, with claims of over 60 million Nigeria records being traded (CYFIRM, 2025). Also, Government agencies, including the Lower Niger Basin Development Authority and the Nigerian Navy, were targeted with sensitive internal data leaked. Healthcare records comprising 130,000 patient entries were reportedly exposed, highlighting risks to personal data privacy. Additionally, offers of compromised Mikro Tik routers have raised concerns over Nigeria's broader critical infrastructure security (CYFIRMA, 2025).

Based on the foregoing reports, the emerging cyber threats in Nigeria's security sector include phishing nets, ransomware, DDoS attacks, data breaches within critical infrastructure and government Ministries, Departments and Agencies (MDAs), Generative AI Misinformation and Dark Web Leak. Incidentally, these threats do not just occur; they are enabled by vulnerabilities in the Nigerian digital space, such as human, technical, institutional and policy vulnerabilities. These are discussed subsequently.

***Human Vulnerability***

Since individuals are frequently the weakest link in any security system, human vulnerability continues to be one of the biggest security challenges. Human mistakes, carelessness, ignorance, and malevolent insider activities continue to expose organizations to significant threats, regardless of how sophisticated security technology develops. Studies have indicated that phishing and social engineering assaults take advantage of human vulnerabilities by tricking employees into disclosing confidential information or installing harmful software, rendering insufficient cybersecurity awareness a significant weakness (Niall & Willie 2023; Gbemisola, 2025). Some of the identifiable human vulnerabilities include insufficient knowledge about cybersecurity. A situation where many employees do not have adequate knowledge of social engineering assaults, phishing emails, password security, and secure internet usage creates an opportunity for cybercriminals to exploit and enter the systems without authorization. Another human vulnerability is the issue of insider danger. Niall and Willie (2023) noted that insider threats, whether deliberate or inadvertent, continue to pose serious challenges to Nigeria's digital space, due to the difficulty to identify the insider that authorized entry to the organizational system. They further noted that insufficient access controls, lack of monitoring, and ineffective employee vetting procedures further heighten insider risks within the public sector in Nigeria. There is also the challenge of inadequate culture of security, which is a common vulnerability in Nigeria. Organizations in Nigeria are frequently more vulnerable to security problems because they do not encourage accountability, security knowledge, and adherence to established processes and have resulted in data breaches that have impacted governmental organizations. The Deloitte Nigeria Cybersecurity Outlook (2025) report observed that several high-profile incidents exposed vulnerabilities in third-party networks, resulting in data breaches, financial losses, and operational disruption. This implies a serious inadequate culture of security among employees who handle institutional cyber units.

***Technical Vulnerability***

Technical vulnerabilities are flaws in networks, apps, hardware, software, and information systems that hackers take advantage of to undermine cybersecurity. This can be easily explained under the following: outdated programmes, inadequate patch management, inadequate network security, and insecure

 

configuration of the system. [a] Outdated Programs: a situation where businesses and government are frequently using unsupported software that is not receiving security updates, leaving known vulnerabilities unpatched. [b] Inadequate Patch Management: poor management of patch that leave systems vulnerable to attack, such as unable to install security updates on time. [c] Inadequate Network Security: improper firewall configurations, unprotected wireless networks, inadequate segmentation, and exposed services that leave systems vulnerable to attack. [d] Insecure Configuration of the system: critical systems are vulnerable to unwanted access due to default passwords, superfluous services, incorrectly set up servers, and inadequate access control. Additionally, the risk of credential compromise has greatly increased in organizations that use just passwords and do not use Multi-Factor Authentication (MFA), as they cannot assure the protection of the systems. In Nigeria, ransomware has emerged as a highly disruptive risk to government entities, encrypting essential data and often making demands for frivolous conditions of restoration that allow easy data breaches by cybercriminals, heightening threats to government databases and citizens' information systems (Nuraeni et al., 2025). The 2025 CYFIRM report on Cyber Threats Assessment in Nigeria noted that the surge of data breaches and cybercrimes experienced by critical sectors in Nigeria, such as the banking, telecom, government, healthcare, and security, was attributed to ransomware attack by Killsec, indicating the dangers of ransomware.

Similarly, in April this year a fresh data breach was reported in Nigeria's financial sector, targeting Fast Credit Finance Company Limited (fastcredit-ng.com) a microfinance and lending institution licensed and regulated by the Central Bank of Nigeria (CBN) (Ibeh, 2026). The report noted that the cybercriminal is offering approximately 870 GB of data containing 939,887 highly sensitive customer information records (such as Personal Identification Information-PII, government-issued ID scans, loan and credit transaction records, bank statements, customer correspondence, contractual agreements, next-of-kin details, personal photographs and selfies and other confidential records) for sale on a popular cybercrime forum that was limited to just five buyers with allegedly stolen data (Ibeh, 2026). Notable portions were also reported to involve Nigerian Police officers and Law enforcement personnel, raising serious concerns about potential doxing, targeted scams, blackmail, or risks to officers' safety and ongoing investigations (Ibeh, 2026). These vulnerabilities pose severe threats to Nigeria's digital space and thus, an urgent need for enhanced cyber threat intelligence detection capability and effective monitoring.

***Institutional Vulnerabilities***

Institutional vulnerabilities exist when organizational internal structures, governance frameworks, and cultural practices create systemic security gaps that allow threat actors to compromise networks and data. These vulnerabilities are rooted in systemic management failures such as inadequate coordination across agencies, poor capability to respond to incidents, insufficient risk control, and bureaucracy challenge. Across sectors in Nigeria, be it healthcare, education, infrastructure, or security, public officials and contractors often divert funds meant to secure digital systems, resulting in outdated, poorly configured IoT deployments vulnerable to exploitation by cyber criminals/attackers (Auwal, 2025). In public health, insecure patient data systems and unpatched devices expose hospitals to breaches and ransomware attacks; in schools, compromised procurement processes enable vendors to supply substandard IoT tools lacking basic safeguards (Auwal, 2025). In the Economic and Financial Crimes Commission (EFCC), system management failure led to leaked data containing the identities, phones numbers, operational codes names, and password hashes of commission operatives, severely compromising investigation and personnel safety (Ibeh, 2026). Meanwhile, technicians and engineers in some organizations may intentionally bypass protocols or install backdoors for personal gain, compounding systemic vulnerabilities. Without enforceable accountability mechanisms, such breaches often go undetected, creating an environment where internal actors pose greater threats to security than external hackers (Shenkoya, 2022; Auwal, 2025). These

 

vulnerabilities weaken digital trust and threaten Nigeria's broader digital ecosystem.

***Policy Vulnerability***

Policy vulnerability is a significant enabler of emerging cyber threats in Nigeria's digital ecosystem because it leads to fragmented governance, regulatory uncertainty, and inability to combat rising cyber threats. Without a cohesive and strictly enforced regulatory framework, the digital economy struggles with systematic inefficiency. The Nigerian digital ecosystem is engulfed with government malpractices in the deployment of digital technologies with no clear enforceable rules, even when there are regulatory frameworks like the National Digital Economy and E-Governance Act, 2024, the National Artificial Intelligence Strategy, and the Nigeria Data Protection Act (Open Government Partnership, 2026). The impact has been the increasing emerging ethical concerns and human rights concerns, including issues such as data privacy, AI bias, human rights abuse, digital divide, and the arbitrary development and deployment of digital technologies for service delivery. The Open Government Partnership (2026) observed that Nigeria has recorded a significant increase in internet penetration over the years, with a penetration rate presently at 55 per cent as of 2024, making the number of internet users about 123 million. This means that there is a higher probability of having more people who lack digital literacy, raising concerns about potential misuse and exploitation. Meanwhile, the various frameworks and initiatives designed to address these issues operate in a fragmented and siloed manner, with little to no transparency regarding their enforcement effectiveness (OGP, 2026). The recent breach reports and cyber incidents involving Remita, Sterling Bank, the Corporate Affairs Commission, and the National Bureau of Statistics, as well as the earlier concerns in the fintech space and government agencies without commensurate response by the regulatory agencies, are a serious national concern about the enforcement effectiveness of the agencies (Edun, 2026). Thus, allowing criminals the latitude to carry out attacks without fear of the system, leaving both institutions and individuals vulnerable. Strengthening legal frameworks and policy measures for digital governance and enforcement mechanisms with clear, enforceable rules will help increase the cost of malpractice in digital deployment and create avenues for redress.

## CONCLUSION

Obviously, rapid digital change and changing hostile capabilities have created an increasingly complicated threat picture for several sectors in Nigeria, including the security sector. Ransomware and phishing nets, insider threats, and a lack of security awareness are human vulnerabilities that continue to expose organizations to cyber threats. Unpatched systems, unsafe setups, and antiquated infrastructure are examples of technical flaws that give attackers exploitable entry points. Inadequate investment in cybersecurity, shortage of qualified staff, poor coordination across agencies, and poor capability to respond to incidents are identifiable examples of institutional vulnerabilities that weaken operational resilience and postpone timely reactions. The sectors' capacity to prevent, identify, and address contemporary challenges is further weakened by policy vulnerabilities, such as antiquated laws and uneven regulatory enforcement. To address these challenges, the study suggests; a thorough and integrated approach that incorporates people, technology, governance, and policy to address the issues; a strong legislative and regulatory framework; institutional capacity building; ongoing workforce education; and contemporary technical safeguards that would guarantee security of Nigeria's digital ecosystem. Adopting this strategy would greatly increase the resilience of the security sector, safeguard vital assets, bolster public confidence, and enhance national security in the face of changing physical and cyber threats.

## RECOMMENDATIONS

In light of the foregoing, the study recommends the following:

 

1. The FGN led by NITDA should implement continuous interactive training on cybersecurity awareness across government agencies, to ensure that all staff acquired role-based training on social engineering, phishing, password management, and secure data handling. This training should be complemented by frequent phishing simulation exercises on a quarterly basis.
2. The FGN in collaboration with the NDPC should enforce the adoption of Patch and Vulnerability Management in all government MDAs. This would keep an asset inventory, regularly scan for technical vulnerabilities, improve rank remediation according to risk, and quickly apply security fixes. In addition, agencies should implement a zero-trust-principles, to lessen the impact of compromised accounts, monitor network activities, impose least-privilege access, eliminate implicit trust, and continuously verify users and devices.
3. The FGN should boost investment in cyber security by providing long term financing for workforce development, cybersecurity tools, infrastructure improvements, and operational resilience. MDAs should complement this by establishing safe channels for information exchange, cooperative threat intelligence, and coordinated incident response with critical infrastructure operators.
4. The Federal Ministry of Communication and Digital Economy (FMCDE) should ensure that cybersecurity legislation is reviewed and updated on a regular basis to meet new technology, cybercrime patterns, digital evidence, and international investigations. This should be complemented by strengthening data protection and privacy enforcement by implementing thorough data protection laws, mandating prompt notification of breaches, and applying appropriate sanctions for non-compliance.
5. FGN led by FMCDE should strengthen international collaboration by increasing cooperation with regional and global partners for collaborative investigations, capacity building, intelligence sharing, and harmonising cybercrime laws.

## References

AFP (2008). "Technical Problems Shut Down Nigeria Satellite". *AFP,* November 12. https://web.archive.org/web/20110104051741/http://afp.google.com/article/

Aliuba, U.H., Onwuchekwa, F.C, and Edokobi, T.D. (2025). "Digital Transformation and Operational Efficiency in Traditional Banking Institutions in Anambra State, Nigeria". *Tansian University Journal of Arts, Management and Social Sciences*, 9(2): 142-161. https://acjol.org/index.php/tujamss/about/editorialTeam/

Auwal, A.M. (2025). "Invisible Intrusions, Internal Threats and Ethical Vulnerabilities in Nigeria's Internet of Things". *Discov Internet Things,* 5: 128. https://doi.org/10.1007/s43926-05-00251-0.

Bayo-Balogun, F. (2019). "The Evolution of Cyber Security in the Nigerian Banking Sector". *AELEX,* April 19. www.aelex.com/

Berman, S.J. (2012). "Digital Transformation: Opportunities to Create New Business Models". *Journal of Strategy and Leadership,* 40(2): 16-24. https://doi.org/10.1108/10878571211209314.

Bertola, P. and Teunissen, J. (2018). "Fashion 4.0. Innovating Fashion Industry through Digital Transformation". *Research Journal of Textile and Apparel,* 22(4): 352-369. https://doi.org/10.1108/RJTA-03-2018-0023/

Borges, E. (2024). "What are Emerging Threats?". *Recorded Future,* February 06.

 

https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/emerging-threats/

CYFIRMA (2025). Cyber Threat Assessment on Nigeria. https://www.cyfirma.com/research/cyber-threat-assessment-on-nigeria/

Darko, G., Darko, M., and Boris, G. (2017). "Cybersecurity and Cyber Defence: National Level Strategic Approach". *Automatika,* 58(3): 273-286. Doi10.1080/0005114.2017.1407022

Dauda, S. and Ukaeje, O. (2024). "Appraisal of Multinational Joint Task Force and Counterinsurgency in the Lake Chad Basin". *University of Nigeria Journal of Political Economy,* 14(1). https://www.unjpe.com/index.php/UNJPE/article/view/251.

Deloitte (2025). Nigeria Cyber Security Outlook. Deloitte and Touché. https://www.deloitte.com/ng/en/services/consulting-risk/perspectives/Nigerias-cybersecurity-landscape-in-2025.html/

Dunamis, O. (2025). "Weekend Horror: Terrorists Use Drones, Arms to Monitor, Kidnap, Kill in Four Nigerian States". *Premium Times,* December 2. https://www.premiumtimesng.com/news/headlines/840071-weekend-of-horror-terrorists-use-drones-arms-to-monitor-kidnap-kill-in-four-nigerian-states.html/

Edun, A. (2026). "What Nigeria's Recent Cybersecurity Breaches Reveal About Our Digital Future". *The Cable,* April 20. https://www.thecable.ng/what-nigerias-recent-cybersecurity-breaches-reveal-about-our-digital-future/

Federal Republic of Nigeria Executive Order No. 21 (2024). Designation and Protection of Critical National Information Infrastructure (DPCNII) Order: Presidential Directive, 24 June.

Gbemisola K. (2025). "Cybersecurity Awareness and Risk Management in the Public Sector". *International Journal of Intelligent Systems and Applications in Engineering*, *13*(1s): 146-155. https://ijisae.org/index.php/IJISAE/article/view/7609/

Geneva Centre for Security Sector Governance (2015). The Security Sector: Roles and Responsibilities in Security Provision, Management and Oversight. SSR Backgrounder Series. Geneva: DCAF. www.dcaf.ch/

Gray, J. and Rumpe, B. (2017). "Models for the Digital Transformation". *Software and Systems Modelling,* 16(2). Doi:10.1007/s10270-017.0596-7.

Greenhalgh, T., Bratan, T., Byrne, E., Mohammed, Y., and Russell, J. (2008). "Introduction of Shared Electronic Records: Multi-Site Case Study Using Diffusion of Innovation Theory". *BMJ,* 337. https://doi.org/10.1136/mj.a1786/

Guler, M. and Buyukozkan, G. (2019). "Analysis of Digital Transformation Strategies with an Integrated Fuzzy AHP-Axiomatic Design Methodology". *IFAC-Papers Online,* 52(13): 1186-1191. https://doi.org/10.1016/j.ofacol.2019.11.359/

Hoffmann, V., Probst, K., and Christinck, A. (2007). "Farmers and Researchers: How can Collaborative Advantages be Created in Participatory Research and Technology Development". *Journal of Agriculture and Human Values,* 24(3): 355-368. https://doi.org/10.1007/s10460-007-9072-2.

Horlacher, A., Klarner, P., and Hess, T. (2016). Crossing Boundaries: Organization on Design Parameters Surrounding CDOs and their Digital Transformation Activities, Americas Conference of Information Systems. San Diego, CA.

 

Ibeh, R. (2026). "New Alleged Breach Hits Nigerian Lender as Cyber Attacks mount on Financial Sector". *Business Day,* April 26.

Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., and Roig-Tierno, N. (2021). "Digital Transformation: An Overview of the Current State of the Art of Research". *SAGE Open,* 11(3). https://doi.org/10.1177/21582440211047576.

Lile, S., Ansari, S (Shaz), and Urmetzer, F. (2025). "Rethinking Disruptive Innovation: Unravelling Theoretical Controversies and Charting New Research Frontiers". *Innovation,* 27(3): 394-416. https://doi.org/10.1080/14479338.2024.2313197/

Luiijf, E. (2014)." New and Emerging Threats of Cyber Crime and Terrorism" in B. Akhgar, A. Staniforth, and F. Bosco, *Cyber Crime and Cyber Terrorism Investigator's Handbook.* London: Elsevier Inc.

Lyytinen, K. and Damsgaard, J. (2001). "What's Wrong with the Diffusion of Innovation Theory: The Case of a Complex and Networked Technology?" *Proceedings of the International Federation for Information Processing (IFIP),* Banff, Alberta, Vol. 3: 40-44.

Momoh, S.A. and Kefas, I.N. (2025). "Digital Economy and National Security". *University of Jos Journal of Political Science,* 2(1): 1-15. https://journals.unijos.edu.ng/index.php/ujjps/article/view/779/

Morakanyane, R., Grace, A.A., and O'Reilly, P. (2017). "Conceptualizing Digital Transformation in Business Organization: A Systematic Review of Literature". *Bled E-Conference*, *21*. https://doi.org/10.18690/978-961-286-043-1.30/

Niall, M., & Willie, A. (2023). "Phishing Attacks and Organizational Resilience in Government Institutions". *International Journal of Cyber Security,* 12(1): 22-38

NITDA. (2019). Nigeria Data Protection Regulation. Federal Republic of Nigeria, Abuja.

NITDA. (2024). National Digital Economy and E-Governance Act. Federal Ministry of Communications, Innovation and Digital Economy, Abuja.

Nuraeni, A., Nugraha, Y. & Aminanto, M. (2025). "Revisiting cyber threats in government sectors: A systematic review of attacks, challenges, and policy-level defenses". *International Journal of Advances in Data and Information Systems, 6*(2), 447–459.

OECD (2005). *Security System Reform and Governance,* DAC Guidelines and References= Series, OECD Publishing, Paris, https://doi.org/10.1787/9789264007888-en/

Okonji, E. (2026). "Why Nigeria Needs Another Satellite in Orbit". *ThisDay Business,* April, 16. https://www.thisdaylive.com/2026/04/16/why-nigeria-needs-another-satellite-in-orbit/

ONSA (2016). The Nigeria Computer Emergency Response Team (ngCERT). https://www.cybersecurityintelligence.com.

Open Government Partnership (2026). Nigeria: Advanced Inclusive and Responsible Digital Governance. OGP/NITDA https://www.opengovpartnership.org/the-open-gov-challenge/nigeria-advance-inclusive-and-responsible-digital-governance/

Rogers, E. M. (1995). *Diffusion of Innovations,* 4th Edition. New York: The Free Press.

Shenkoya, T. (2022). "Can Digital Transformation Improve Transparency and Accountability of Public Governance in Nigeria?" *Transform Gov People Process and Policy,* 17(1): 54-71. https://doi.org/10.1108/tg-08-2022-0115/

 

Siachou, E., Vrontis, D., and Trichina, E. (2021). "Can Traditional Organizations be Digitally Transformed by Themselves? The Moderating Role of Absorptive Capacity and Strategic Interdependence". *Journal of Business Research,* 124: 408-421. https://doi.org/10.1016/j.jbusres.2020.11.011/

Wheeler, E. (2011) *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up.* London: Elsevier Inc.

Xiaoli, J. and Weiqing L. (2022). "Digital Transformation: A Review and A Research Framework". *Frontiers in Business, Economics and Management,* 5(3): 1-6.