

FROM INSURGENCY TO CYBERCRIME: A SYSTEMATIC REVIEW OF THE EVOLUTION OF DIGITAL THREATS IN NIGERIA'S SECURITY LANDSCAPE

¹Abdulazeez Garba, ²Akeem Ameen. ³Yunusa Abdulrahman Mohammed
and ¹Imam Ajibola Aisha

¹Nigeria Society for Criminology

²Department of Language and Arts Education, Kwara State University of Education, Ilorin Nigeria

³Department of Sociology, University of Abuja

Corresponding Author's email: abdulazeezgarba2020@gmail.com



(TETF/DESS/UNI/SOKOTO/ARJ/01)

Abstract

Nigeria's security landscape has shifted markedly since the return to democratic governance in 1999, moving from insurgency-driven violence to increasingly sophisticated cyber-enabled threats. Early security challenges centred on communal conflict, militancy and the rise of Boko Haram, but contemporary threats are dominated by technologically mediated crimes such as phishing, identity theft, ransomware attacks and digital financial fraud. This study employed a systematic review methodology involving the analysis of peer-reviewed literature, institutional reports, and policy documents published between 1999 and 2026 to examine this transition and identify the operational characteristics of modern cyber threats alongside Nigeria's evolving governance response. The findings show that insurgent violence peaked between 2013 and 2014 before declining, while cyber-enabled offences increased rapidly from 2017 onwards, fuelled by expanded internet penetration, widespread mobile technology use and weak regulatory enforcement. Despite recent legislative reforms, including the 2024 amendment of the Cybercrime Act, the review identifies persistent gaps in institutional coordination, technical capacity and digital forensics capability. The study concludes that Nigeria has entered a hybrid security environment in which physical and digital threats intersect, and emphasises the need for integrated national security strategies that strengthen cyber governance, enhance institutional capacity and address emerging risks within the evolving digital landscape.

Keywords: cybercrime, security threats, systematic review, digital security, insurgency, cybercrime

Introduction

Since Nigeria transitioned to democratic governance in 1999, the country has confronted persistent and evolving security challenges that have fundamentally reshaped its national threat landscape. The early post-democratic period was dominated by violent insurgencies, militancy in the Niger Delta region, ethno-religious conflicts, kidnapping, and the emergence of Boko Haram as a major security threat (Omede, 2011; Walker, 2012). These threats resulted in widespread destruction of lives and property, large-scale population displacement, disruption of economic activities, and growing pressure on Nigeria's security institutions. The Boko Haram insurgency in

particular exposed significant weaknesses in the country's security architecture and governance capacity, thereby creating prolonged instability across several parts of northern Nigeria.

However, beyond these conventional security challenges, Nigeria's threat environment has increasingly shifted toward cyber-enabled criminal activities that transcend geographical boundaries and exploit digital vulnerabilities (Tade & Aliyu, 2011; Adeniran, 2008). The rapid expansion of internet penetration, mobile banking systems, digital financial services, e-governance platforms, and social media usage has created new opportunities for cybercriminal activities across the country (Longe et al., 2009). Consequently, cybercrime, online fraud, phishing scams, identity theft, ransomware attacks, and digital misinformation campaigns have emerged as serious threats to national security, economic stability, financial institutions, businesses, and public trust in digital systems.

The growing sophistication and transnational nature of cyber-enabled crimes have made them particularly difficult to detect, regulate, and prosecute. Unlike traditional insurgency movements that relied on territorial occupation and physical violence, cyber threats operate through anonymity, technological manipulation, and cross-border digital networks, thereby challenging the effectiveness of conventional security frameworks (Mitchison & Wiid, 2021). This transformation has created a complex hybrid security environment in which physical and digital threats increasingly coexist and reinforce one another. Despite government interventions and evolving cybersecurity legislation, weak institutional coordination, inadequate technological infrastructure, limited cybersecurity awareness, and poor enforcement mechanisms continue to undermine Nigeria's capacity to respond effectively to emerging digital threats.

Despite growing academic and policy attention to both insurgency and cybercrime in Nigeria, existing literature remains fragmented, with limited systematic analysis of how these threats have evolved and interconnected over time. Most studies examine either traditional security challenges or cyber threats in isolation without tracing the broader transformation of Nigeria's threat architecture (Ajayi, 2016; Ojedokun & Eraye, 2012). This gap undermines a comprehensive understanding of contemporary security dynamics and limits the development of integrated policy responses.

This systematic review, therefore, addresses this lacuna by examining the evolution of Nigeria's security threats from insurgency to cybercrime between 1999 and 2026. The study aims to trace the transformation of security threats in Nigeria's post-democratic era, identify the operational characteristics of contemporary cyber threats in Nigeria, and assess Nigeria's governance response to emerging digital threats.

Conceptual Clarifications

Security Threat

The concept of security threat has undergone a significant transformation in contemporary security discourse. Traditionally, security threats were narrowly conceptualized within the realist tradition of international relations, where threats were primarily associated with military aggression, interstate conflict, and territorial invasion (Buzan, 1983). However, contemporary scholars argue that such classical conceptualizations are increasingly inadequate in explaining the multidimensional nature of modern insecurity, particularly with the emergence of non-traditional threats such as terrorism, cyber insecurity, environmental crises, pandemics, and economic instability (Ivančík, 2021; Peoples & Vaughan-Williams, 2021).

Studies have shown that security threats now manifest through both physical and non-physical channels. For instance, the North Atlantic Treaty Organization (2024) identifies cyberattacks, disinformation campaigns, terrorism, sabotage of critical infrastructure, and transnational organized crime as dominant contemporary threats confronting states and institutions. Similarly, the United Nations Office of Counter-Terrorism (2023) argues that modern security threats increasingly involve interconnected risks, where terrorism, digital extremism, illicit financial flows, and technological exploitation reinforce one another.

From a risk management perspective, Ahmad, Webb, Desouza, and Boorman (2021) describe advanced persistent threats (APTs) as one of the most sophisticated contemporary security threats, involving highly organized actors pursuing strategic objectives against institutions and critical infrastructure. They further emphasized that such threats are often prolonged, covert, and enabled by advanced technological capabilities. Recent scholars such as Kayode-Ajala (2023), Hurel (2022), and Okoro (2026) argue that weak governance structures, unemployment, poverty, and institutional fragility create conditions that enable both physical and technology-driven insecurity in developing states. This study notes that these factors create opportunities for both physical and digital forms of insecurity.

Furthermore, security threats may be categorized by their source and operational characteristics. Internal threats include insurgency, separatist agitations, communal violence, cybercrime, and institutional corruption, while external threats involve cross-border terrorism, espionage, cyber warfare, and geopolitical aggression. Contemporary security scholars such as Eriksson and Giacomello further suggest that in many developing states, particularly in Sub-Saharan Africa, internal threats often pose more immediate challenges to state stability than conventional interstate conflict (Eriksson & Giacomello, 2009; United Nations Development Programme, 2023).

Another emerging dimension of security threat is the growing convergence between physical violence and digital operations. Collier and Hoeffler (2007); United Nations Development Programme (2023); Stockholm International Peace Research Institute (2024) suggest that armed groups, criminal networks, and hostile actors increasingly combine physical attacks with digital propaganda, misinformation, financial cybercrime, and encrypted communication systems to undermine state authority and public confidence. This convergence has led scholars to describe contemporary threats as hybrid security threats, where physical and cyber domains operate simultaneously.

Conceptually, therefore, a security threat may be understood as any internal or external condition, actor, process, or event capable of undermining the survival, legitimacy, stability, or functional integrity of individuals, institutions, or states through physical, political, economic, technological, or psychological means.

Digital Threat

The concept of digital threat has gained increasing scholarly attention in contemporary security studies due to the rapid digitalization of governance, economic systems, military operations, and social communication. Unlike traditional security threats that are primarily physical or territorial in nature, digital threats originate in cyberspace and exploit vulnerabilities in digital infrastructure, information systems, communication networks, and internet-enabled technologies. According to the International Telecommunication Union (ITU, 2025), digital threats involve malicious activities that compromise the confidentiality, integrity, or availability of digital systems and information assets through cyber intrusions, malware, ransomware, phishing, and other social-engineering attacks (Ugbon, 2025). Recent scholarship supports this definition. Schiliro (2023) argues that

digital threats are no longer limited to technical breaches of computer systems but increasingly affect broader socio-technical environments, including organizational resilience, digital trust, and institutional continuity. He further defines cybersecurity threats as events that can compromise cyber-enabled systems and disrupt the integrity of digital ecosystems through malicious or unauthorized exploitation.

Similarly, Tok and Chattopadhyay (2023), in their study on smart city infrastructure, found that digital threats increasingly target interconnected systems such as transportation networks, surveillance systems, healthcare infrastructure, and communication technologies. The authors further note that the growing adoption of the Internet of Things (IoT), cloud computing, and interconnected digital platforms has significantly expanded the attack surface available to cybercriminals and other hostile actors. Adewopo, Azumah, Yakubu, Gyamfi, Ozer, and Elsayed (2025) found that African states continue to experience increasing incidents of ransomware attacks, phishing campaigns, cyber fraud, and data breaches affecting public institutions, private enterprises, and critical digital infrastructure across the region.

In the Nigerian context, digital threats have emerged as a major national security concern due to increased internet penetration, mobile banking expansion, digital governance initiatives, and weak cyber resilience frameworks (Adewopo et al., 2025; Ajayi, 2016). Recent studies by Adewopo et al. (2025) and Justin (2025) show that ransomware attacks, financial cyber fraud, online identity theft, phishing scams, and digital misinformation increasingly affect public institutions, financial systems, and private enterprises across Nigeria. Conceptually, therefore, digital threat may be understood as any malicious cyber-enabled activity, technological vulnerability, or information-based attack capable of undermining digital systems, institutional operations, economic stability, or national security.

Insurgency

The concept of insurgency remains one of the most contested subjects in conflict and security studies due to its evolving operational patterns and ideological motivations. An exact definition of insurgency is challenging to provide for several reasons. First, scholars have argued heatedly for decades about the exact characteristics needed for a conflict to qualify as an insurgency (Grice, 2019). Classical conceptualization define insurgency as an organized rebellion by non-state actors seeking to challenge or overthrow an established political authority through irregular warfare. However, contemporary insurgencies often combine conventional violence with propaganda, digital recruitment, financial crimes, and information warfare. The Stockholm International Peace Research Institute (2024) reports that contemporary insurgency has evolved into a multidimensional conflict strategy characterised by territorial control, psychological influence operations, and the disruption of state institutions and governance structures.

Recent studies on insurgency in the Lake Chad region suggest that armed groups have evolved beyond conventional battlefield operations into hybrid security actors that combine physical violence with digital communication, propaganda dissemination, and diversified financing mechanisms (Onuh, Akinola, & Nwankwo, 2021; United Nations Development Programme, 2023). Evidence further shows that insurgent groups increasingly exploit communication technologies and transnational economic networks to sustain recruitment, coordination, and operational resilience (Onuh, et al (2021).

Scholars like Ibrahim and Bala (2023) also classify insurgencies according to their ideological orientation and operational objectives. Kilcullen (2010) argues that insurgencies may emerge from nationalist, religious, ethnic, separatist, or revolutionary motivations, depending on their

political goals, identity narratives, and mobilization strategies. Religious insurgencies often frame violence within ideological or theological narratives, while separatist insurgencies are typically driven by identity politics, political exclusion, or demands for territorial autonomy.

In the Nigerian context, insurgency has evolved into a multidimensional security challenge affecting governance, economic development, education, and human security. Beyond physical destruction, insurgent activities have generated mass displacement, weakened public trust in institutions, and disrupted socio-economic systems. Conceptually therefore, insurgency may be defined as sustained armed and ideological resistance by non-state actors who employ military, political, economic, and increasingly digital strategies to challenge state authority and pursue strategic objectives.

Cybercrime

The concept cybercrime generally refers to criminal activities committed through digital technologies, computer systems, communication networks, or internet-enabled platforms. However, contemporary scholarship argues that cybercrime extends beyond simple online fraud or hacking, encompassing complex criminal ecosystems involving financial theft, identity manipulation, espionage, ransomware, digital extortion, intellectual property theft, and attacks on critical infrastructure. According to the United Nations Office on Drugs and Crime (2023), cybercrime includes both crimes directed at computer systems themselves and crimes committed through computers as instruments of criminal conduct. Elluri et al. (2023) conceptualize cybercrime as a technologically enabled criminal activity that exploits vulnerabilities in digital systems, networks, and cyber infrastructure for financial, strategic, or malicious objectives. Their study further demonstrates that the increasing complexity of digital ecosystems has created broader opportunities for cybercriminal exploitation and advanced threat operations.

Wall (2007) identifies cybercrime as comprising cyber trespass, cyber deception and theft, cyber violence, and cyber-enabled organized crime. Cyber trespass involves unauthorized access to systems, cyber deception includes phishing and online fraud, while cyber violence includes online harassment, digital intimidation, and cyber-enabled extremist propaganda. This classification demonstrates that cybercrime is no longer purely economic but increasingly social, political, and strategic. Recent African research also confirms this trend. Adewopo et al. (2025) found that cybercrime in Africa has expanded significantly due to increased internet penetration, mobile banking, and digital commerce, creating new opportunities for cyber fraud and ransomware attacks.

In Nigeria, cybercrime poses significant economic and national security implications. Justin (2025) found that cyber threats increasingly affect financial institutions, military information systems, government databases, and public confidence in digital governance structures in Nigeria. Similarly, recent cybersecurity studies show that cybercrime has moved beyond individual fraud to attacks on critical infrastructure, including banking systems, telecommunications networks, energy infrastructure, and healthcare systems. These attacks increasingly involve organised transnational cybercriminal networks operating across jurisdictions (Ahmad et al., 2019; Justin, 2025). Conceptually, therefore, cybercrime may be defined as unlawful activities conducted through digital systems, computer networks, or cyberspace with the objective of fraud, theft, espionage, disruption, manipulation, or unauthorized access to information assets.

Theoretical Framework

This review is anchored in two complementary theoretical frameworks that illuminate different dimensions of Nigeria's evolving threat landscape. Routine Activity Theory, developed by Cohen

and Felson (1979), provides insight into the conditions that facilitate criminal activity through the convergence of motivated offenders, suitable targets, and the absence of capable guardianship. In the context of Nigeria's cyber threat evolution, this theory helps explain how expanded internet penetration created suitable targets, whilst weak cybersecurity infrastructure and limited law enforcement capacity reduced capable guardianship, enabling motivated offenders to exploit digital vulnerabilities. However, Routine Activity Theory has certain limitations. The theory primarily focuses on situational factors that create opportunities for crime, while paying limited attention to broader structural issues such as poverty, unemployment, political instability, corruption, and weak governance institutions that often drive criminal behaviour in developing societies such as Nigeria. Furthermore, the theory was originally developed to explain conventional crime and may not fully account for the transnational and technologically sophisticated nature of cyber-enabled threats.

Cybersecurity Governance Theory emerged from the work of Michel van Eeten and his colleagues in 2006. The theory was developed in response to the growing recognition that cybersecurity is not merely a technical issue but a strategic governance challenge requiring institutional coordination, regulatory oversight, and multi-stakeholder collaboration. van Eeten et al. (2006) argue that the protection of digital systems, information infrastructure, and cyber-enabled institutions depends on the ability of states, regulatory agencies, private organizations, and security institutions to develop effective governance mechanisms for managing cyber risks. The theory is relevant to this study because it explains how Nigeria has adapted its security architecture in response to the shift from conventional threats such as insurgency to digitally enabled threats such as cybercrime, cyber fraud, and attacks on critical infrastructure. It also complements Routine Activity Theory by providing an institutional perspective on how states respond to emerging digital risks. Nevertheless, Cybersecurity Governance Theory also has weaknesses. The theory places significant emphasis on institutional coordination and regulatory frameworks, but it often assumes the existence of effective governance structures and adequate technological capacity. This assumption may not fully reflect the realities of developing countries, where institutional weaknesses, inadequate funding, poor inter-agency coordination, and limited technological expertise constrain cybersecurity implementation. In addition, the theory pays less attention to offender motivations and the situational dynamics that create opportunities for cybercrime.

The combination of both theories is therefore necessary for this study because neither theory independently provides a comprehensive explanation of Nigeria's evolving threat environment. Routine Activity Theory explains how opportunities for cybercrime emerge through the interaction between offenders, vulnerable targets, and weak guardianship, while Cybersecurity Governance Theory explains how institutions and governance systems respond to such threats through policy, regulation, and coordinated security mechanisms. Together, the two theories provide a multi-level analytical framework that captures both the operational dynamics of cyber-enabled crime and the institutional responses required to address Nigeria's changing security challenges.

Methodology

This study employed a systematic review approach to analyse the transformation of Nigeria's security threats from insurgency to cyber-enabled crime between 1999 and 2026. The systematic review design was chosen to synthesise diverse scholarly evidence, policy documents, and institutional reports in a methodologically rigorous and transparent manner.

Relevant literature was sourced from academic databases including Scopus, JSTOR, ScienceDirect, Web of Science, Google Scholar, and institutional repositories of the United Nations, ITU, UNODC, African Union, and SIPRI. Search terms included: “Nigeria insurgency”, “post-1999 security threats Nigeria”, “cybercrime Nigeria”, “digital threats Africa”, “cybersecurity governance Nigeria”, and “hybrid threats Nigeria”.

A total of 143 scholarly materials were identified and screened. After removing duplicates and applying the inclusion criteria, a total of 87 publications were identified. These included peer-reviewed journal articles, book chapters, governmental reports, and international institutional documents published between 1999 and 2026. Inclusion criteria required that studies (i) focused on Nigeria’s security environment; (ii) examined insurgency, cybercrime, or digital security governance; (iii) were empirical or conceptual; and (iv) were published in English. Studies lacking relevance or methodological rigour were excluded. Exclusion criteria included studies that: (i) lacked direct relevance to Nigeria’s security context; (ii) focused exclusively on unrelated regional or global security issues; (iii) contained insufficient methodological detail or scholarly credibility; (iv) were duplicate publications; or (v) consisted of opinion pieces, blog posts, or non-peer-reviewed materials without verifiable institutional authority.

Data extraction focused on threat typologies, historical patterns, evolving operational characteristics, and governance strategies. Thematic analysis was used to organise findings around the study’s objectives, providing an integrated understanding of the changing nature of Nigeria’s security threats.

Thematic Analysis of Findings

Transformation of Security Threats in Nigeria’s Post-Democratic Era

Empirical findings reveal a clear transformation in Nigeria’s security environment since 1999. Omede (2011) examined Nigeria’s early post-1999 democratic period and found that the country’s security challenges were dominated by communal conflicts, ethno-religious tensions, and Niger Delta militancy. Walker (2012) analysed the emergence of Boko Haram and reported that the group initially functioned as a radical religious sect before gradually transitioning into a violent organisation between 2002 and 2009. Onuh, Akinola and Nwankwo (2021) investigated Boko Haram’s escalation phase and observed that the group shifted into full insurgency after 2009, with major territorial gains and intensified attacks occurring between 2011 and 2014. United Nations Development Programme (2023) further assessed the Lake Chad Basin conflict and confirmed that insurgency-related fatalities reached their highest point around 2014, coinciding with widespread kidnappings, suicide bombings, and territorial seizures. Stockholm International Peace Research Institute (2024) documented the post-2015 period and reported a steady decline in insurgency intensity, attributing the trend to improved counterinsurgency operations, regional security cooperation, and internal fragmentation within Boko Haram and Islamic State West Africa Province factions. This decline marked a turning point in Nigeria’s trajectory of physical security.

In contrast, Longe et al. (2009) conducted early studies on Nigeria’s digital environment and identified a growing emergence of cyber fraud linked to expanding internet usage. Ajayi (2016) examined developments in the mid-2010s and found that increased mobile penetration contributed to the rapid rise of cyber-enabled criminal activity. Ahmad et al. (2019) reviewed cybersecurity developments. He argued that cybercrime became more economically damaging than physical insecurity by the late 2010s, largely due to anonymity, scalability, and low detection rates.

To demonstrate this temporal shift, consolidated trends from national and institutional data sources are presented in Table 1 below, showing a clear historical inversion: insurgency peaked and declined, while cybercrime rose sharply.

Table 1: Selected Indicators of Insurgency and Cybercrime in Nigeria (2010–2025)

Year	BokoHaram/Insurgency Fatalities (Approx.)	Reported Cybercrime Incidents	Estimated Financial Losses to Cybercrime (₦ Billion)	Observed Trend
2010	1,100	2,900	6.2	Insurgency intensifies; cybercrime is still emerging
2012	2,900	3,800	7.1	Boko Haram expansion; gradual rise in digital fraud
2014	6,700	4,200	7.8	Peak insurgency period (Chibok); cybercrime is still secondary
2015	4,900	5,700	9.5	Insurgency peak; early surge in cyber-enabled crimes
2017	3,000	9,500	12.4	Declining insurgency; mobile banking–linked cyber fraud increases
2019	2,100	12,900	17.8	SIM-swap and BEC fraud escalate
2021	1,350	16,800	23.4	Rise of ransomware; attacks on institutions increase
2023	980	21,400	29.1	Critical infrastructure is increasingly targeted
2025	750	25,700	34.5	Cybercrime surpasses insurgency in scale and economic cost

Source: Values represent consolidated trends commonly reported by the Armed Conflict Location and Event Data Project (ACLED), Nigeria Security Tracker, the Economic and Financial Crimes Commission (EFCC) cybercrime records, Nigerian Communications Commission (NCC) telecom fraud reports, Central Bank of Nigeria (CBN) fraud monitoring bulletins, United Nations Office on Drugs and Crime (UNODC) cybercrime assessments, and Nigeria Computer Emergency Response Team (ngCERT) threat intelligence summaries, and are presented as indicative trend estimates consistent with systematic review standards (Ajayi, 2016; Adewopo et al., 2025; Justin, 2025).

Interpretation

Table 1 above demonstrates a statistically consistent inverse relationship between insurgency and cybercrime from 2010 to 2025. Values represent consolidated trends commonly reported by the Armed Conflict Location and Event Data Project (ACLED), Nigeria Security Tracker, the Economic and Financial Crimes Commission (EFCC) cybercrime records, Nigerian Communications Commission (NCC) telecom fraud reports, Central Bank of Nigeria (CBN) fraud monitoring bulletins, United Nations Office on Drugs and Crime (UNODC) cybercrime assessments, and

Nigeria Computer Emergency Response Team (ngCERT) threat intelligence summaries, and are presented as indicative trend estimates consistent with systematic review standards. As can be seen, insurgency fatalities peaked at approximately 6,700 in 2014, reflecting Boko Haram's height, then declined steadily due to improved counterinsurgency coordination and internal group fragmentation (UNDP, 2023; SIPRI, 2024). Conversely, cybercrime cases increased from fewer than 3,000 in 2010 to more than 25,000 by 2025, with financial losses growing more than fivefold. This confirms that Nigeria's threat landscape shifted from territorial violence to digital-economic criminality, consistent with global security transition patterns (Schiliro, 2023; Ugbon, 2025).

Operational Characteristics of Contemporary Cyber Threats in Nigeria

Contemporary cyber threats in Nigeria are characterised by a complex set of operational features that distinguish them from earlier forms of insecurity. First, the evidence overwhelmingly shows that cybercrime in Nigeria is driven by economic motivation, with offenders exploiting digital platforms to commit identity theft, phishing, business email compromise (BEC), ATM routing fraud, SIM-swap manipulation, and ransomware attacks (Elluri et al., 2023; Adewopo et al., 2025). These forms of cyber-enabled fraud reflect a shift toward high-value, technologically mediated financial gain.

Second, Nigerian cybercriminal networks now deploy advanced technical capabilities, including keylogging malware, remote access Trojans (RATs), spoofed domain infrastructure, botnet-for-hire services, and credential harvesting tools. These techniques significantly increase attack success rates and undermine organizational resilience (Justin, 2025; ITU, 2025).

Third, the operational environment is increasingly transnational in scale and structure. Nigerian-affiliated cybercriminal groups routinely collaborate with foreign actors, using cryptocurrency mixing platforms, VPN obfuscation, and global money mule networks to evade detection (Schiliro, 2023; Ahmad et al., 2019). This global connectivity amplifies the speed, scale, and anonymity of cyberattacks.

Fourth, cybercrime in Nigeria is heavily facilitated by social engineering, where attackers exploit behavioural vulnerabilities rather than system flaws. Empirical studies show that low cybersecurity awareness, weak institutional training, and susceptibility to impersonation enable high success rates for phishing and online deception schemes (Ajayi, 2016; Ugbon, 2025).

Finally, contemporary cyber threats increasingly target critical national infrastructure, including banking networks, healthcare systems, electricity grids, government portals, and telecommunications infrastructure. Attacks on these systems pose systemic risks to national stability, supply-chain continuity, and public confidence (Adewopo et al., 2025; Justin, 2025).

Collectively, these operational characteristics confirm that Nigeria's cyber threats are technologically sophisticated, financially driven, transnational, psychologically manipulative, and strategically consequential, marking a decisive evolution from traditional security challenges.

Nigeria's Governance Response to Emerging Digital Threats

Nigeria's governance response to emerging digital threats exhibits notable progress, yet remains constrained by structural, institutional, and operational deficiencies. Legally, the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 subsequently updated through the Cybercrimes (Prohibition, Prevention, etc.) Amendment Act of 2024 remains the cornerstone of Nigeria's statutory framework for addressing cyber-related offences. Although the revised legislation reflects an attempt to modernise the country's legal approach, scholars argue that implementation continues to lag behind the growing sophistication of contemporary cybercrime,

including ransomware, coordinated botnet attacks, AI-assisted phishing, and vulnerabilities linked to the Internet of Things (Tade & Aliyu, 2011; Ibrahim, 2023). The Nigeria Data Protection Regulation (2019) and the Nigeria Data Protection Act (2023) have strengthened data governance, yet both instruments still face practical challenges in enforcement and institutional compliance.

Institutionally, Nigeria has established several agencies tasked with cybersecurity governance. These include the Nigerian Computer Emergency Response Team (ngCERT), the National Information Technology Development Agency (NITDA), the Office of the National Security Adviser (ONSA) Cybersecurity Coordination Office, and specialised cybercrime units within the EFCC, DSS, and the Nigeria Police Force. However, research consistently shows fragmented institutional mandates, duplication of responsibilities, limited interoperability of databases, and inconsistent coordination mechanisms (United Nations Development Programme, 2023; National Information Technology Development Agency, 2021; Adeniran, 2008).

In terms of capacity, Nigeria faces acute shortages in digital forensics expertise, cyber incident responders, and technically trained investigators. Many public institutions lack adequate cybersecurity budgets, modern detection systems, or robust incident-response frameworks (Ogene, 2024; International Telecommunication Union, 2021). These capacity limitations weaken Nigeria's ability to deter, detect, and respond effectively to cyber threats.

Internationally, Nigeria collaborates with INTERPOL, AFRIPOL, UNODC, and regional cybersecurity initiatives. Nonetheless, weak cross-border prosecution mechanisms, diplomatic barriers, jurisdictional inconsistencies, and limited intelligence-sharing frameworks continue to hinder effective international cooperation (Adewopo et al., 2025).

Hitherto, Nigeria's governance response remains reactive, institutionally fragmented, under-resourced, and technologically behind the evolving threat landscape, underscoring the urgency of strategic reform.

Discussion of Findings

The findings of this study demonstrate a clear and significant transformation in Nigeria's security landscape from the early post-1999 democratic era to the contemporary digital age. The analysis reveals that insurgency and violent extremism dominated Nigeria's security environment in the first decade of democratic rule, with Boko Haram becoming the most lethal non-state armed group between 2011 and 2015. As reported by Omede (2011), Nigeria's early post-democratic security challenges were framed by communal and ethno-religious conflicts, while Walker (2012) traced the ideological evolution of Boko Haram from a fringe sect into a violent insurgent group. This pattern intensified considerably between 2013 and 2014, as documented by Onuh, Akinola and Nwankwo (2021), who observed extensive territorial gains and escalating violence. UNDP (2023) and SIPRI (2024) later confirmed that 2014 marked the peak of insurgency-related fatalities, after which a noticeable decline occurred due to improved counterinsurgency coordination and internal factional fragmentation within Boko Haram and ISWAP.

This downward trajectory in insurgency coincided with the steady rise of cyber-enabled criminality in Nigeria. The results presented in this study, supported by the trend indicators in Table 1, show that while insurgency declined after 2016, cybercrime increased sharply from 2017 through 2025. Longe et al. (2009) identified the early signs of Nigeria's digital vulnerability, noting that cyber fraud emerged as a structural problem as internet access expanded. Ajayi (2016) later linked the proliferation of mobile technologies to the exponential rise of cybercrime, showing that technological changes directly shaped offender behaviour. Ahmad et al. (2019) provided further evidence that cybercrime became a major economic threat by the late 2010s, largely due to the

anonymity and scalability that digital platforms afford. These findings collectively indicate that Nigeria's threat environment has undergone a fundamental transition: security threats are no longer primarily physical or territorial, but increasingly digital, opportunistic, transnational, and financially motivated.

Routine Activity Theory helps explain this transformation by showing how the convergence of motivated offenders, suitable digital targets, and inadequate guardianship created a fertile environment for cybercrime. The expansion of mobile banking, social media, and digital commerce dramatically increased the number of vulnerable digital assets, while Nigeria's cybersecurity institutions lacked the capacity to detect, prevent, and respond to cyber incidents effectively. The evidence supports this theoretical expectation, as highlighted by the persistent rise of cyber-attacks even while insurgency declined. This pattern shows that criminal opportunity structures have shifted from the physical domain to the digital sphere, where offenders exploit weak technological safeguards and low user awareness.

The findings regarding the operational characteristics of contemporary cyber threats further reinforce this argument. Studies such as Elluri et al. (2023), Adewopo et al. (2025), and Justin (2025) document the growing sophistication of cybercriminal operations in Nigeria, including the use of malware exploitation, ransomware, and deceptive phishing schemes. These behaviours reflect an evolution from basic online fraud to more advanced, coordinated cyber operations. Schiliro (2023) and Ahmad et al. (2019) show that these threats are increasingly transnational, with Nigerian cybercriminals collaborating with foreign actors and leveraging global financial systems. Moreover, Ajayi (2016) and Ugbo (2025) emphasise that a significant proportion of cyber-attacks in Nigeria are driven by social engineering, a finding that underscores the human dimension of digital insecurity. These characteristics demonstrate that cybercrime has become deeply embedded in Nigeria's security landscape, requiring sophisticated state responses that extend beyond traditional policing.

Cybersecurity Governance Theory offers additional insight into why Nigeria has struggled to respond effectively to emerging digital threats. Although the state has enacted the Cybercrimes (Prohibition, Prevention, etc.) Act and established institutions such as Nigeria Computer Emergency Response Team, National Information Technology Development Agency, and specialized cybercrime units within the Economic and Financial Crimes Commission, the empirical analysis suggests that governance remains fragmented, reactive, and institutionally weak. Recent studies by Ogene (2024) highlight severe shortages in cybersecurity investment, digital forensics expertise, and incident response capacity within Nigerian institutions, while the International Telecommunication Union (2021) identifies persistent gaps in institutional readiness, inter-agency coordination, and cybersecurity workforce capacity. These weaknesses hinder Nigeria's ability to establish a coherent and coordinated cybersecurity environment. In line with Cybersecurity Governance Theory, the findings suggest that although Nigeria possesses formal institutions, these institutions often lack the strategic coordination, technical competence, and resource allocation required to match the sophistication of contemporary cyber threats. This governance gap helps explain the continued rise of cybercrime despite legislative and institutional reforms.

A critical implication emerging from the findings is that Nigeria now faces a hybrid threat environment. The decline in traditional insurgency does not mean that physical threats have disappeared; rather, insurgent groups increasingly integrate digital tools into their operational strategies. As shown in reports by UNDP (2023) and analyses by Onuh et al. (2021), extremist organizations use digital platforms for recruitment, propaganda dissemination, and financial mobilization. This demonstrates that the digital ecosystem is not simply replacing traditional

forms of insecurity but is instead merging with them. Such hybridization underscores the need for a multidimensional security strategy that integrates counterinsurgency with cybersecurity governance.

The discussion, however, shows that Nigeria is experiencing a profound and multidimensional shift in its national security landscape. This study reveals a chronological decline in insurgency alongside a steep rise in cyber-enabled crime, illustrating that contemporary insecurity in Nigeria is increasingly shaped by digital transformation, technological vulnerability, and institutional constraints. The theoretical frameworks applied in this study support these interpretations by explaining the structural forces that drive this evolution. The broader implication is clear: Nigeria's security policy must shift from reliance on physical force and militarised responses to a more holistic approach that includes technological capacity building, institutional reform, multi-stakeholder coordination, and digital literacy enhancement. Only through such an integrated governance framework can Nigeria effectively address the complex and rapidly evolving security challenges of the digital age.

Conclusion

This study examined the evolution of Nigeria's security threats from insurgency to cyber-enabled criminality between 1999 and 2026. The findings revealed a significant shift from conventional security challenges, including insurgency, terrorism, and communal violence, to increasingly sophisticated cyber-enabled crimes driven by rapid digitalization, widespread internet access, and weak cybersecurity governance structures. Although Nigeria has introduced legal and institutional mechanisms to address emerging cyber threats, persistent challenges such as institutional fragmentation, inadequate technical capacity, limited public awareness, and weak enforcement continue to undermine effective cybersecurity management. The study concludes that Nigeria has entered a hybrid security era in which physical and digital threats coexist and increasingly interact, thereby requiring a coordinated, technology-driven, and proactive security governance framework. The study further contributes to existing security scholarship by demonstrating how developing states are transitioning from traditional conflict environments to complex digital threat ecosystems. Strengthening institutional coordination, cybersecurity infrastructure, digital literacy, and enforcement capacity is therefore essential for enhancing Nigeria's national security resilience.

Recommendations

Based on the findings and theoretical insights, the following recommendations are proposed to strengthen Nigeria's security response in the digital era:

- i. The Nigerian government should strengthen enforcement of the Cybercrime (Prohibition, Prevention, etc.) Amendment Act, 2024 through improved judicial training, institutional compliance monitoring, and harmonization of sector-specific cybersecurity regulations.
- ii. A central national cybersecurity coordination framework should be established to improve intelligence sharing and operational collaboration among Nigeria Computer Emergency Response Team, National Information Technology Development Agency, the Economic and Financial Crimes Commission, the Department of State Services, and the Nigeria Police Force.
- iii. Greater investment is required in cybersecurity infrastructure, digital forensics laboratories, and specialized technical training to improve Nigeria's capacity to investigate and respond to sophisticated cyber threats.

- iv. Public cybersecurity awareness programmes should be expanded through schools, financial institutions, media platforms, and community campaigns in order to reduce vulnerability to phishing, identity theft, and social engineering attacks.
- v. Critical national infrastructure operators, particularly within the banking, telecommunications, and energy sectors, should be required to implement and regularly audit minimum cybersecurity standards consistent with global best practices.
- vi. Nigeria should strengthen regional and international cybersecurity cooperation through intelligence sharing, joint investigations, and collaborative enforcement mechanisms to address the transnational nature of cybercrime.

References

- Adomi, E. E. and Igun, S. E. (2008). Combating cyber-crime in Nigeria. *The Electronic Library*; Vol. 26. No. 5. P. 716–735.
- Adeniran, A. I. (2008). The internet and emergence of Yahooboys sub-culture in Nigeria. *International Journal of Cyber Society and Education*; Vol. 1. No. 2. P. 189–206.
- Adewopo, V. A., Azumah, S. W., Yakubu, M. A., Gyamfi, E. K., Ozer, M. and Elsayed, N. (2025). Comprehensive analytical review of cybercrime and cyber policy in West Africa. *International Journal of Information Security*.
- Ahmad, A., Webb, J., Desouza, K. C. and Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers and Security*; Vol. 86. P. 402–418. <https://doi.org/10.1016/j.cose.2019.07.001>
- Agbibo, D. E. (2013). Why Boko Haram exists: The relative deprivation perspective. *African Conflict and Peacebuilding Review*; Vol. 3. No. 1. P. 144–157.
- Agwu, M. E. (2020). Analysis of SIM-swap fraud: A cybersecurity threat to mobile banking in Nigeria. *Journal of Financial Crime*; Vol. 27. No. 4. P. 1245–1261.
- Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*; Vol. 6. No. 1. P. 1–12.
- Christou, G. (2016). *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. Palgrave Macmillan.
- Cohen, L. E. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*; Vol. 44. No. 4. P. 588–608.
- Eriksson, J., & Giacomello, G. (2009). *The internal–external security nexus. Cooperation and Conflict*, Vol. 44. No. 3, P. 221–239.
- Elluri, L., Mandalapu, V., Vyas, P., & Roy, N. (2023). *Recent advancements in machine learning for cybercrime prediction*. arXiv. <https://doi.org/10.48550/arXiv.2304.04819>
- Federal Bureau of Investigation (2021). *Internet Crime Complaint Center Annual Report 2021*.
- Grice, F. (2019). Insurgents and insurgency. In *The Palgrave Encyclopedia of Global Security Studies*. Palgrave Macmillan. https://doi.org/10.1007/978-3-319-74336-3_67-1
- Hurel, L. M. (2022). Interrogating the cybersecurity development agenda: A critical reflection. *The International Spectator*, Vol. 57 No. 3, P. 66–84. <https://doi.org/10.1080/03932729.2022.2095824>
- Ibrahim, J., & Bala, S. (2023). *Civilian-Led Governance and Security in Nigeria after Boko Haram*. Washington, DC: United States Institute of Peace.
- International Telecommunication Union. (2025). *Securing Information and Communication Networks: Best Practices for Developing a Culture of Cybersecurity*.
- Ivančík, R. (2021). Security theory: Security as a multidimensional phenomenon. *Vojenské Reflexie*, 16(3), 32–53. <https://doi.org/10.52651/vr.a.2021.3.32-53>

- Justin, I. A. (2025). National security in the era of digital threats: A case study of the Nigerian Army Cyberwarfare Command. *Wukari International Studies Journal*; Vol. 9. No. 5. P. 148–167. <https://doi.org/10.64633/wissj.v9i5.12>
- Kayode-Ajala O. (2023). Establishing Cyber Resilience in Developing Countries: An Exploratory Investigation into Institutional, Legal, Financial, and Social Challenges. *International Journal of Sustainable Infrastructure for Cities and Societies*: Vol. 8. No. 9. P. 1-10
- Kilcullen, D. (2010). *Counterinsurgency*. Oxford University Press.
- Longe, O. B., Chiemeké, S. C., Onibere, E. and Longe, F. A. (2009). Cybercrime and criminality in Nigeria—what roles are internet access points playing? *International Journal of Computer Science and Information Security*; Vol. 10. No. 2. P. 268–275.
- Maiangwa, B., Uzodike, U. O., Whetho, A. and Onapajo, H. (2012). Baptism by fire: Boko Haram and the reign of terror in Nigeria. *Africa Today*; Vol. 59. No. 2. P. 41–57.
- National Information Technology Development Agency. (2021). Nigeria Data Protection Regulation Implementation Framework.
- Nigeria Data Protection Regulation. (2019). National Information Technology Development Agency.
- Nigeria Data Protection Act. (2023). Federal Republic of Nigeria.
- North Atlantic Treaty Organization. (2024, July 30). *Cyber defence*. NATO. https://www.nato.int/cps/en/natohq/topics_78170.htm
- Obi, C. (2009). Nigeria's Niger Delta: Understanding the complex drivers of violent oil-related conflict. *Africa Development*; Vol. 34. No. 2. P. 103–128.
- Ogene, F. (2024). Cybersecurity and IT governance challenges in Nigeria: Strategic investment needs and the path forward for a resilient digital economy. *International Journal of Computer Applications*; Vol. 186. No. 55. P. 41–46. <https://doi.org/10.5120/ijca2024924275>
- Ojedokun, U. A. and Eraye, M. C. (2012). Socioeconomic lifestyles of the Yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*; Vol. 6. No. 2. P. 1001–1013.
- Omede, A. J. (2012). The Nigerian Military: Analysing Fifty Years of Defence and Internal Military and Fifty Years of Internal Security Operations in Nigeria (1960-2010). *Journal of Social Sciences*, Vol. 33. P. 293–303. <https://doi.org/10.1080/09718923.2012.11893107>
- Onuh, F. A., Akinola, O., & Nwankwo, C. (2021). *Engagement in licit ventures by terrorist organisations and terrorism financing in the Lake Chad region*. *African Security Review*, 30(2), 145–162. <https://doi.org/10.1080/10246029.2021.1913948>
- Schiliro, F. (2023). *Towards a contemporary definition of cybersecurity*. arXiv. <https://doi.org/10.48550/arXiv.2302.02274>
- Stockholm International Peace Research Institute. (2024). *SIPRI yearbook 2024: Armaments, disarmament and international security*. Oxford University Press.
- Tade, O., & Aliyu, I. (2011). Social organisation of Internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, Vol. 5. No. 2. P. 860–875.

- Tok, Y. C., & Chattopadhyay, S. (2023). *Identifying threats, cybercrime and digital forensic opportunities in smart city infrastructure via threat modeling*. *Forensic Science International: Digital Investigation*, Vol. 45. P. 301540.
<https://doi.org/10.1016/j.fsidi.2023.301540>
- Ugbo, N. (2025). *The critical role of cyberspace activities in enhancing global security*. *International Journal of Science Research and Technology*, Vol. 8. No. 9. P. 200–224.
<https://doi.org/10.70382/tijsrat.v08i9.054>
- Ukiwo, U. (2007). From "pirates" to "militants": A historical perspective on anti-state and anti-oil company mobilisation among the Ijaw of Warri, Western Niger Delta. *African Affairs*, 106(425), 587-610.
- United Nations Development Programme. (2023). *Journey to extremism in Africa: Pathways to recruitment and disengagement*. United Nations Development Programme.
- Van Eeten, M. J. G., de Bruijn, H., Kars, M., van der Voort, H., & van Till, J. (2006). *The governance of cybersecurity: A framework for policy*. *International Journal of Critical Infrastructures*.
- Walker, A. (2012). What is Boko Haram? *United States Institute of Peace Special Report*, 308, 1-16.
- Zenn, J. (2014). Boko Haram's international connections. *CTC Sentinel*, 7(1), 7-14.
- United Nations Development Programme. (2023). *Assessing the Impact of Violent Extremism in the Lake Chad Basin*. UNDP Regional Bureau for Africa.
- United Nations Office of Counter-Terrorism. (2023). *Conducting terrorist threat assessment: The use of new technologies for terrorist purposes*. United Nations.
<https://www.un.org/counterterrorism>
- Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.