RECONCEPTUALISING NATIONAL SECURITY IN THE DIGITAL AGE: CYBER POWER AND THE NIGERIAN STATE

YUSUF, IDOWU BOBADE
INSTITUTE OF GOVERNANCE AND DEVELOPMENT STUDIES,
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA, yusufbobade2022@gmail.com

OCHEFU, YAKUBU, PhD
INSTITUTE OF GOVERNANCE AND DEVELOPMENT STUDIES,
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA, yochefu@gmail.com

BABAN'UMMA, MOHAMMED BELLO, PhD
INSTITUTE OF GOVERNANCE AND DEVELOPMENT STUDIES,
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA, muhammedbello22@gmail.com

DOI: https://doi.org/10.64633/wissj.v10i8.13

Keywords

National Security; Cyber Power; Cybersecurity; Securitisation Theory and National Security Strategy

Abstract

Research Problem: *Despite the rapid digitalisation of state functions and the rise of cyber-enabled threats in Nigeria, its national security framework remains largely rooted in the traditional military-territorial paradigm. This study addresses the gap between Nigeria's emerging cyber threat environment and its conventional security architecture.*
Methods/Theory: *The study adopts a qualitative research design anchored in Securitisation Theory and analyses secondary data from Nigeria's security and cybersecurity policy documents, legal instruments, institutional reports, cybersecurity publications, and relevant scholarly literature covering 2015–2025. Data were analysed using qualitative content analysis.*
Results: *The findings reveal that cyber threats in Nigeria are partially securitised. Although policy documents recognise digital threats, institutional responses remain fragmented, technical and law-enforcement-oriented. Cyber-enabled threats, including terrorism, insurgency, banditry, and electoral disinformation, cut across territorial boundaries and undermine state authority, economic stability, and democratic institutions.*
Conclusion: *The study concludes that Nigeria's capacity to address hybrid threats depends on transforming its security architecture from a predominantly military-territorial model to an integrated, cyber-aware, resilient, and human-centred national security framework.*
Key Contribution to Knowledge: *This study provides the first systematic Securitisation Theory-driven analysis of Nigeria's cyber threat environment. It proposes a reconceptualised framework that integrates cyber power as a strategic domain, broadening security referent objects to include human security, economic resilience, and critical national information infrastructure.*

Recommendation: *The study recommends expanding security refernt objects, strengthening inter-agency coordination, developing a coherent national cyber strategy, enhancing public-private partnerships, and ensuring democratic oversight of cybersecurity measures.*

INTRODUCTION

The traditional understanding of national security has been largely centred on strong military capacity, protection of territorial integrity, and safeguarding state sovereignty against external aggression. This approach assumes that security threats are identifiable, geographically defined, and distinct from the state's normal political and social activities. Although this conception was suitable for an international environment characterised by conventional interstate conflict, it has become less sufficient in an era of rapid digitalisation. The emergence of cyberspace as a strategic domain has changed the nature, sources, and forms of contemporary security threats. In this study, cyber-enabled threats refer to threats whose effectiveness depends substantially on digital technologies and cyberspace, while digitally mediated threats refer to threats whose communication, mobilisation, coordination, or societal impact are enhanced through digital platforms. Contemporary scholarship therefore has recognised the need for national security to extend beyond territorial defence to account for digital interconnectedness, cyber vulnerabilities, economic systems, information ecosystems, and technological infrastructure (Williams, 2018; Drezner, 2024).

The limitations of traditional security paradigms are evident in addressing cyber-enabled and digitally mediated threats, which often cross territorial boundaries and are difficult to attribute or respond to through conventional means (Egloff, 2020). Unlike conventional warfare, cyber operations can take place below the threshold of armed conflict, creating blurred distinctions between crime, espionage, warfare, and political coercion, while non-state actors such as terrorist groups, criminal networks, and insurgents can exploit cyberspace to achieve effects beyond their material capabilities (Valeriano & Maness, 2015; Kello, 2017). Consequently, national security now extends beyond territorial sovereignty and regime survival to include critical infrastructure, financial systems, electoral institutions, government information systems, and citizens' digital security, reflecting the growing recognition of cyberspace as a strategic domain alongside land, sea, air, and space (NATO, 2016).

Despite these developments, Nigeria's national security architecture has not fully integrated cyber power as a strategic component of national power. Although the National Security Strategy (NSS) 2019 and the National Cybersecurity Policy and Strategy (NCPS) 2021 recognise cybersecurity and information-related threats, responsibilities remain fragmented across technical, regulatory, law-enforcement, intelligence, and defence institutions (FRN, 2019; FRN, 2021). The gap lies between recognising cyber threats in policy and effectively integrating cybersecurity into national defence and strategic security planning. Existing Nigerian and African studies have contributed significantly to the understanding of cybercrime, cyberterrorism, information security, digital mobilisation, institutional capacity, and cybersecurity governance, but many focus mainly on operational, technological, regulatory, or law-enforcement issues. Consequently, limited attention has been given to how Nigeria's prevailing conception of national security shapes the

identification, prioritisation, and institutional management of cyber threats, particularly within the political, institutional, and historical realities of a developing state.

This situation creates both a conceptual and an empirical gap in the literature. Conceptually, limited attention has been paid to how the securitisation of cyber threats shapes their place within Nigeria's national security priorities. Empirically, few studies have systematically examined how government security discourse, institutional structures, and policy frameworks address cyber-enabled threats such as terrorism, insurgency, banditry, and electoral disinformation. This concern is also relevant to the Human Security paradigm developed by the United Nations Development Programme (UNDP, 1994), which broadened the concept of security from protecting the state to protecting individuals from threats to their survival, livelihood, and dignity. In Nigeria, national security has focused more on state stability, territorial integrity, regime security, and conventional threats.

The problem is therefore both strategic and institutional, as the rapid digitalisation of government institutions, financial systems, critical infrastructure, electoral processes, and social communication has increased Nigeria's exposure to cyber-enabled disruptions. However, institutional fragmentation, overlapping responsibilities, limited cyber expertise, weak inter-agency coordination, and the absence of an integrated national cyber doctrine continue to constrain the state's ability to respond effectively. Cyber threats may be recognised in policy but still lack the coordination, resources, planning, and political attention given to conventional threats. Securitisation Theory, developed by the Copenhagen School, provides a useful framework for understanding this situation by explaining how political and institutional actors present certain issues as existential threats requiring prioritised security responses (Buzan, Wæver, & de Wilde, 1998). In Nigeria's digital security environment, the Theory examines who defines cyber threats as security issues, what is considered under threat, how such claims are received, and how they shape institutional responses. This approach moves the analysis beyond the mere existence of cyber threats to an understanding of why some threats receive greater national security attention while others remain largely treated as technical, criminal, or regulatory matters.

Against this backdrop, the study argues that the evolving nature of Nigeria's security environment requires reconceptualising national security to recognise cyber power as a key component of national power. This entails expanding the referent objects of security to include citizens, economic systems, democratic institutions, and Critical National Information Infrastructure (CNII), while strengthening coordination among defence, intelligence, law enforcement, regulatory, and private-sector institutions. However, the securitisation of cyberspace should be guided by democratic accountability, constitutional safeguards, and human security principles to prevent cybersecurity measures from leading to excessive state control. The study therefore examines how cyber-enabled threats expose the limitations of Nigeria's traditional military and territorial security paradigm and proposes a framework for effectively integrating cyber power into the country's national security architecture.

Research Objectives

The study specifically seeks :

i. To examine how cyber-enabled threats, including terrorism, insurgency, banditry, and electoral disinformation, expose the limitations of Nigeria's traditional military-territorial national security paradigm using Securitisation Theory.

ii. To propose a reconceptualised national security framework that integrates cyber power into Nigeria's national security architecture.

LITERATURE REVIEW

Conceptual Clarification

National Security: The protection of a state's vital interests against threats deemed sufficiently serious to require exceptional government attention and resource allocation, encompassing not only military threats but also economic, technological, and political challenges (Drezner, 2024)

Cyber Power: The capacity of a state to use cyber technologies and cyberspace resources strategically to gather intelligence, defend critical infrastructure, disrupt adversaries, shape public opinion, and protect national interests (Nye, 2010).

Cybersecurity: Cybersecurity refers to the collection of technologies, processes, policies, and practices designed to protect networks, computer systems, data, and digital infrastructure from unauthorised access, attacks, damage, or disruption (International Telecommunication Union [ITU], 2008).

Securitisation Theory: Securitisation Theory explains how state or non-state actors transform an issue into a matter of security by framing it as an existential threat that justifies exceptional measures outside normal political procedures (Buzan, Wæver, & de Wilde, 1998).

National Security Strategy: A government's integrated plan that identifies national security objectives, assesses threats and opportunities, and establishes the policies and capabilities required to protect and advance the nation's interests (Yarger, 2006).

Empirical Review of Literature

Limitations of Traditional National Security Paradigms in Addressing Cyber-Enabled Threats in Nigeria

Empirical evidence indicates that traditional national security approaches, which focus on territorial defence, military power, and state sovereignty, are progressively inadequate for addressing cyber-enabled threats. Mwangi (2024), drawing on secondary data from cybersecurity reports, official documents, and scholarly literature, found that digital technologies have expanded the security environment, exposing critical infrastructure, financial systems, and government networks to cyberattacks that can undermine state authority and economic stability. Thus, traditional security frameworks cannot solely address the speed, anonymity, and transnational nature of cyber threats, leading the author to advocate for cybersecurity governance, digital resilience, and inter-agency collaboration. However, its broad global focus gives limited attention to the institutional and governance realities of Nigeria and West Africa, where cyber threats are also influenced by technological vulnerabilities, weak institutional capacity, fragmented governance, and limited regional cooperation (African Union, 2014; ECOWAS, 2020; FRN, 2021).

Kente and Ishaku (2024), through an integrative review of empirical studies, policy documents, and cybersecurity incident reports, found that terrorist and insurgent groups in Nigeria now use digital platforms for recruitment, propaganda, fundraising, and operational coordination. The study also identified institutional fragmentation, inadequate technological infrastructure, and limited cybersecurity expertise as major constraints on Nigeria's response. Although the authors recommended stronger cybersecurity legislation, digital infrastructure,

and institutional capacity, their analysis is largely operational and does not sufficiently examine how Nigeria's traditional military-territorial conception of national security limits the recognition of cyberspace as a strategic security domain.

Both studies show that cyber-enabled threats expose weaknesses in Nigeria's conventional security approaches. This study addresses this gap by applying Securitisation Theory and proposing a reconceptualised national security framework that integrates cyber power into Nigeria's national security architecture.

Reconceptualising Nigeria's National Security Framework to Effectively Integrate Cyber Power as a Strategic Domain in Response to Evolving Threats.

Empirical scholarship has recognised cyber power as an integral component of national security, requiring states to move beyond the conventional military-centred approaches. Nye (2017), through a qualitative review of global cyber incidents, policy documents, and national cybersecurity strategies, argues that cyber power has become an important element of national power alongside military, economic, and diplomatic capabilities, especially for intelligence, deterrence, strategic communication, and critical infrastructure protection. The study therefore calls for integrating cyber capabilities, public-private partnerships, and international cooperation into national security strategies. However, its broad global focus provides limited insight into how developing countries such as Nigeria can adapt cyber power to their national security frameworks.

Maurer (2018) investigated the institutionalisation of cybersecurity governance through a comparative analysis of national cybersecurity frameworks. The study found that effective cyber governance depends on coordinated institutions, specialised cybersecurity agencies, and clear strategic frameworks that support whole-of-government and whole-of-society responses to threats such as terrorism, insurgency, and disinformation. The study also shows that failure to integrate cyber capabilities into national security structures increases vulnerability to threats that can affect political stability, economic activity, and public trust. However, its focus on advanced and institutionally developed states provides limited insight into how developing countries such as Nigeria can adapt such governance models to their own political, institutional, and security realities.

These studies show that integrating cyber power into national security requires institutional reform, clear policy direction, and effective coordination. However, they give limited attention to the political, historical, and institutional factors that influence security policy in developing countries. This study addresses this gap by examining how Nigeria's national security framework can be reconceptualised to incorporate cyber power in responding to emerging threats.

Synthesis and Research Gap

The empirical literature shows that Nigeria's traditional military-territorial approach to national security is insufficient to address cyber-enabled threats. Studies by Mwangi (2024), Kente and Ishaku (2024), Nye (2017), and Maurer (2018) demonstrate that cyberspace has become a strategic domain in which cyberattacks, cyberterrorism, disinformation, and other hybrid threats can affect state security, economic stability, and critical infrastructure. The studies also emphasise the need for effective cybersecurity governance, institutional coordination, strategic policies, and stronger cyber capabilities. However, while international studies focus more on the strategic role of cyber power and cybersecurity governance,

Nigerian studies largely emphasise operational challenges and institutional weaknesses.

Despite these contributions, research remains limited on how security discourse, state-centred assumptions, and institutional arrangements shape Nigeria's response to cyber threats. There is also insufficient attention to how Nigeria's national security framework can be restructured to integrate cyber power within its political, institutional, and security realities. This study addresses these gaps by applying Securitisation Theory to examine the limitations of Nigeria's traditional national security paradigm and the integration of cyber power into its national security architecture.

Theoretical Framework

Different theoretical perspectives offer complementary explanations of cyber threats and national security. Realism, particularly neorealism, views cyber power as an additional instrument of state power used to pursue national interests, strengthen deterrence, and compete with other states. However, its state-centred approach gives limited attention to non-state actors, societal vulnerabilities, and how digital issues become recognised as security threats. Constructivism holds that cyber threats are socially constructed through political interpretations, norms, institutional practices, and shared understandings rather than having fixed meanings. Nevertheless, it offers limited explanation of the specific process by which cyber issues become recognised and prioritised as national security concerns. While these perspectives provide useful insights, Securitisation Theory offers a more direct framework for examining how particular cyber threats are defined, prioritised, and institutionalised as national security concerns.

This study adopts Securitisation Theory, developed by the Copenhagen School, to explain why cyber threats have not been fully integrated into Nigeria's national security architecture despite their growing strategic significance. According to Buzan, Wæver, and de Wilde (1998), security threats are not merely objective realities but are socially and politically constructed through discourse. An issue becomes a national security concern when political actors successfully frame it as an existential threat to a valued referent object and the relevant audience accepts this framing, thereby legitimising exceptional policy measures and institutional responses. Balzacq (2011) extends this perspective, arguing that securitisation is shaped not only by speech acts but also by institutional settings, audience perceptions, and socio-political context. This is particularly relevant to Nigeria, where fragmented institutions, uneven cyber capacity, overlapping mandates, and competing security priorities shape how cyber threats are interpreted and prioritised.

The theory is highly applicable because cyber-enabled threats, including online radicalisation, electoral disinformation, cyber-financial crime, digital mobilisation, and the coordination of terrorism and organised crime, are often treated as ICT or law-enforcement issues rather than strategic national security concerns. Consequently, cybersecurity governance remains fragmented, limiting political commitment, institutional coordination, and strategic investment. Securitisation Theory helps explain that this challenge is not merely a consequence of technological incapacity; it also stems from how cyber threats are framed and positioned within the national security hierarchy. Its concepts of securitising actors, referent objects, audience acceptance, and exceptional measures provide a framework for examining how cyber-enabled terrorism, insurgency, banditry, and electoral disinformation challenge Nigeria's traditional military-territorial security paradigm. It also provides a conceptual basis for broadening the scope of national security to include individuals,

economic systems, democratic institutions, and CNII as legitimate security referents.

Securitisation Theory has, however, been criticised for being state-centric, elitist, and overly reliant on discourse, offering limited normative guidance on whether securitisation yields desirable security outcomes. Floyd (2010, 2016), for example, argues that securitisation should be assessed against genuine threats and the consequences of extraordinary security measures for democratic values. This concern is particularly relevant to Nigeria, where measures adopted to counter digital threats may affect privacy, freedom of expression, and other constitutional rights. The study therefore recognises that effective cyber securitisation should strengthen national resilience and human security rather than become a mechanism for excessive state control or regime protection. This study extends Securitisation Theory by applying it to Nigeria's cybersecurity governance, thereby testing its relevance beyond its traditional European context. It contributes to Securitisation Theory by applying it to the under-researched context of cybersecurity governance in Nigeria, a developing state, thereby testing the Theory's applicability beyond the traditional Westphalian and post-Cold War European settings in which it was primarily developed. Securitisation Theory is therefore adopted as the main analytical framework because it best explains how cyber threats are framed, prioritised, and integrated into Nigeria's national security architecture.

MATERIALS AND METHODS

Research Design and Data Sources

This study adopts a qualitative research design based on systematic analysis of secondary documentary evidence. It examines how cyber-enabled threats are framed, prioritised, and institutionalised within Nigeria's national security architecture. The analysis covers 2015–2025, corresponding broadly with the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and the subsequent development of Nigeria's cybersecurity policy architecture. The NCPS 2014 is retained as a foundational baseline because it preceded and informed the 2021 policy revision. The secondary data comprised national security and cybersecurity policy documents, legislation, institutional and regulatory reports, electoral documents, regional and international cybersecurity publications, and peer-reviewed scholarly literature. Key sources included the National Security Strategy 2019, NCPS 2014 and 2021, Cybercrimes Act 2015 and its 2024 amendment, and relevant publications from the Office of the National Security Adviser (ONSA), National Information Technology Development Agency (NITDA), Nigerian Communications Commission (NCC), Nigeria Computer Emergency Response Team (ngCERT), and Independent National Electoral Commission (INEC).

Table 1: Summary of Secondary Data Sources

Source Type	Sources	No. of Documents analysed	Purpose
National Security and Policy Documents	NSS 2019; NCPS 2014 & 2021	3	Examine national-security framing, cyber threats, and strategic priorities
Legal and Regulatory Instruments	Cybercrimes Act 2015 & 2024 Amendment	2	Assess legal authority, cybersecurity governance, and enforcement

Institutional and Government Reports	INEC 2022 and CDD 2023	2	Assess institutional responses, coordination, governance, and digital security
Regional and International Reports	AU, ECOWAS, GNET, ITU, NATO, UNDP and related publications	7	Contextualise Nigeria's cyber-threat environment
Scholarly Literature	Peer-reviewed articles, books and book chapters	21	Provide theoretical, empirical, and critical perspectives
Total	All selected documentary sources	35	Triangulate evidence on cyber securitisation and cyber power

Source: Authors' Compilation Based on Purposive Documentary Selection, 2015–2025.

Document Selection Criteria

Documents were selected purposively against five criteria: (i) relevance to the 2015–2025 study period, except for foundational documents; (ii) focus on Nigeria's national security, cybersecurity, cyber power, digital threats, critical infrastructure, or related governance issues; (iii) produced by recognised government institutions, statutory agencies, international or regional organisations, research institutions, or peer-reviewed publishers; (iv) substantive information on cyber threats, policy responses, institutional arrangements, or governance; and (v) sufficient evidence to address the research objectives. The study excluded commercial, promotional, duplicative, unverifiable, and irrelevant materials.

Qualitative Content Analysis

The study employed a directed qualitative content analysis, guided deductively by Securitisation Theory (Buzan, Wæver, & de Wilde, 1998; Balzacq, 2011). A coding framework was developed around six analytical categories: (i) securitising actors, (ii) referent objects, (iii) threat construction and policy framing, (iv) audience acceptance, (v) institutional responses, and (vi) exceptional or prioritised security measures. Relevant passages from the selected documents were systematically identified and classified according to these analytical categories. The classified evidence was then compared across institutions and document types to identify recurring patterns, contradictions, institutional gaps, and changes in the framing of cyber threats between 2015 and 2025. The analysis consequently assessed the extent of cyber securitisation in Nigeria and its implications for integrating cyber power into the national security architecture.

RESULTS

The Digital Transformation of the Nigerian Threat Landscape

Nigeria's current security environment reflects the dynamics of hybrid warfare, which combines conventional violence with cyber operations, disinformation, and digital communication to achieve strategic objectives. As a result, groups such as Boko Haram Terrorists (BHT), the Islamic State West Africa Province (ISWAP), and the Indigenous People of Biafra (IPOB) employ physical violence alongside online propaganda, recruitment, financing, and information warfare. Although cyberspace has not replaced kinetic violence, it complements it, enabling non-state actors to expand their influence, shape narratives, and challenge state authority beyond conventional battlefields.

Terrorist Groups

Terrorist organisations in Nigeria now exploit digital technologies for radicalisation, recruitment, financing, propaganda, and operational coordination (Aina & Ojo, 2023; Global Network on Extremism and Technology [GNET], 2023). For instance, BHT and ISWAP use social media, encrypted messaging applications, and online forums to disseminate extremist ideology, recruit supporters, and sustain networks beyond conflict zones (Mustapha, 2025). These platforms also amplify grievances linked to marginalisation and the perceived illegitimacy of the government, thereby accelerating recruitment for terrorist groups (Conway, 2017; Hansen & Nissenbaum, 2009). Furthermore, cyber-enabled financing strengthens the organisations through mobile money services, informal value transfer systems such as hawala, and, in some instances, virtual currencies, challenging conventional counterterrorism financing mechanisms (Makinde & Akinwale, 2021). The extensive use of digital propaganda serves operational and psychological purposes by intimidating communities and projecting influence beyond its immediate area of operations. Although Nigeria has responded through public information campaigns and media engagement, such efforts are insufficient, fragmented, and largely reactive, reflecting the asymmetry between state and non-state actors in the digital information environment.

Insurgency

The IPOB-led separatist movement has used cyberspace for political mobilisation and transnational advocacy. Social media platforms such as Facebook, X, and YouTube facilitate mobilisation, the dissemination of sit-at-home directives, and organisational coordination, while reducing exposure to direct state repression (Uwalaka, 2021). Diaspora networks strengthen IPOB through online fundraising, advocacy, encrypted communications, and technical support, making organisational disruption very difficult (Akinwale, 2022). IPOB also deploys disinformation and narrative warfare, stoking sentiment among the populace and producing emotionally charged digital content to question state legitimacy and amplify allegations of human rights abuses. Government responses to cyber activism have raised concerns about democratic freedoms. The absence of a comprehensive digital engagement strategy has further limited the effectiveness of these responses.

Banditry and Organised Crime

Banditry and organised criminal groups have also adopted digital technologies to enhance coordination, intelligence gathering, and operational flexibility. They have used mobile phones, messaging apps, email, and other communication tools to enable decentralised planning across wide geographical areas while reducing operational costs (Mustapha, 2020). Kidnapping-for-ransom has become cyber-enabled, with negotiations conducted via mobile networks and ransom payments often transferred electronically through digital platforms or via intermediaries. These practices complicate financial surveillance and expose weaknesses in Nigeria's capacity to monitor illicit digital financial flows.

Election Security and Disinformation

Nigeria's electoral process is not immune to cyber-enabled threats. During the 2019 and 2023 general elections, digital platforms were used to spread widespread disinformation, false narratives about political opponents and election results, and to run coordinated online influence campaigns that undermined public trust (Centre for Democracy and Development [CDD], 2023). Although there was no evidence of foreign cyber interference, concerns persist about transnational actors and

diaspora networks amplifying polarising content (CDD, 2023). By introducing digital voter databases, biometric systems, and electronic results transmission, the INEC has introduced new cybersecurity vulnerabilities. Despite significant investments by INEC in digital electoral technologies, preparedness for cyberattacks remains constrained by technical limitations, inadequate resources, and weak institutional coordination (INEC, 2022).

Analysing the Current Securitisation of Cyber Threats in Nigeria

Nigeria's cybersecurity landscape reflects a partial, uneven, and contradictory process of securitisation. Although cyber threats are widely discussed in official matters, they have not been fully integrated into national security strategy. Rather, securitisation is driven by institutional rivalry, shifting political priorities, and crises, rather than a collective, coherent strategic framework.

Securitising Actors

The Presidency, particularly the ONSA, is the principal securitising actor. The NSS 2019 and the NCPS 2021 frame cybercrime, terrorism, and information warfare as threats to national stability, sovereignty, economic prosperity, and critical infrastructure (FRN, 2019; FRN, 2021). These policy documents serve as primary securitising texts. However, despite presenting cyber threats as existential risks, they largely assign operational responsibility to civilian regulators, law enforcement, and technical agencies, revealing a disconnect between security rhetoric and institutional practice. While Nigeria has developed institution-specific military cyber capabilities, including the Nigerian Army Cyber Warfare Command, the absence of a clearly articulated and publicly identifiable overarching national cyber doctrine limits the integration of these capabilities across the wider national security architecture. Likewise, legislation such as the Cybercrimes Act (2015) and regulatory frameworks administered by agencies such as the EFCC and NITDA reflect a multi-institutional approach that remains insufficiently integrated within a unified national cybersecurity framework.

Referent Objects and Audience Acceptance

Nigeria's cyber securitisation is unclear about what it is protecting. Official discourse refers to national sovereignty, economic stability, critical infrastructure, and public safety, yet policy responses prioritise regime stability and state security. This lack of clarity gives online separatism, electoral disinformation, and digital activism greater security attention than citizen-centred threats such as data breaches and online fraud, leading to selective securitisation, in which issues become security priorities only when they align with elite interests (Buzan et al., 1998). Another limitation concerns audience acceptance, a central element of Securitisation Theory. While the Presidency frames cyber threats as national security issues, acceptance among the National Assembly, security agencies, the private sector, and citizens remains uneven. Weak legislative prioritisation, limited inter-agency coordination, and inconsistent private-sector compliance suggest that cyber securitisation has not achieved broad institutional or societal support.

Exceptional Measures and Remaining Gaps

Exceptional cybersecurity measures further illustrate Nigeria's securitisation process. The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 provides important legal tools to investigate cyber offences but raises concerns regarding surveillance powers and freedom of expression. Similarly, attempts to regulate social media and restrict digital communication during periods of insecurity demonstrate elements of hypersecuritisation, where digital spaces are treated as existential

threats requiring extraordinary state intervention. Although such measures may produce short-term security benefits, they risk undermining democratic legitimacy and public trust. In other words, Nigeria's cyber securitisation remains fragmented, characterised by competing institutions, selective referent objects, and inconsistent audience acceptance. Without a coherent framework that integrates cyber power across state, economic, and human security priorities, responses to digitally enabled threats will remain reactive, contested, and strategically incomplete.

Integrating Cyber Power into Nigeria's National Security Framework.

To respond effectively to the hybrid threats of the digital age, Nigeria must integrate cyber power as a vital component of its national security architecture.

Expanding the Referent Object

To reconceptualise national security, Nigeria must change its focus from territorial integrity and regime stability to include individuals, the economy, and CNII. While the state remains central, cyber threats continue to target citizens through online fraud, identity theft, data breaches, and digital exploitation, undermining public trust and societal resilience. In line with post-Cold War security scholarship, individuals must be recognised as legitimate referent objects alongside the state (Buzan, Wæver, & de Wilde, 1998). Economic security is equally important, as Nigeria's growing dependence on digital finance, e-governance, telecommunications, and online commerce increases vulnerability to cyberattacks. Protecting CNII across sectors such as energy, finance, transport, telecommunications, and elections is therefore essential to national resilience. A citizen-centred approach also promotes public trust, participation, and democratic accountability while reducing the risk of over-securitisation.

Institutional Adaptation

For cyber power to be effectively integrated, sound institutional reform is essential. For now, Nigeria's cybersecurity governance remains fragmented across multiple agencies with overlapping mandates and weak coordination, reflecting broader post-colonial patterns of bureaucratic competition rather than integrated security planning. A coordinated framework, anchored in the NCPS 2021, will clarify mandates, strengthen legal authority, improve information sharing, and combine central coordination with decentralised implementation. Because cyberspace blurs traditional civil-military boundaries, effective governance requires collaboration among defence, intelligence, law enforcement, regulatory agencies, the private sector, and critical infrastructure operators. Intelligence institutions could also mainstream cyber threat intelligence, data analytics, and real-time monitoring into national security planning. Addressing political rivalry, resource competition, and institutional duplication is essential if coordinated cyber governance is to move beyond policy aspiration.

Strategic Doctrine

Institutional reform must be underpinned by a coherent national cyber strategy that clearly defines Nigeria's cyber power objectives in defence, resilience, deterrence, and governance. The absence of such a doctrine reflects limited strategic cyber expertise, fragmented policy ownership, and an underdeveloped strategic culture that has not recognised cyberspace as a core domain of national power. Cyber power could be embedded within the national security strategy rather than treated as a separate technical issue. Priority could be given to deterrence through resilience, system protection, and credible strategic signalling, consistent with contemporary cyber deterrence thinking (Nye, 2017). Nigeria's cyber strategy could also

align with regional and international frameworks, including ECOWAS, the African Union, and broader global cyber governance initiatives (Valeriano & Maness, 2015). Expanding cyber securitisation must remain consistent with democratic accountability, transparency, and constitutional rights, enhancing human security rather than reinforcing regime protection.

Table 1: Cyber-Enabled Threats, Digital Manifestations and National Security Implications in Nigeria, 2015–2025

Cyber-Enabled Threat	Key Digital Manifestations	Major National Security Implications
Terrorism	Online radicalisation/ recruitment, propaganda, encrypted communication, digital financing	Expanded reach; recruitment; operational coordination; psychological insecurity.
Insurgency/Separatist Mobilisation	Social-media mobilisation, online advocacy, encrypted networks, diaspora platforms	Weakened state legitimacy; cross-border mobilisation; social instability, esclations of political grievances.
Banditry/Organised Crime	Mobile communication, digital coordination, ransom negotiation and payments	Greater criminal flexibility; intelligence and financial-tracking challenges.
Electoral Disinformation	False information, coordinated campaigns, impersonation, polarising narratives	Reduced public trust; electoral disruption; political polarisation, threats to democratic institutions.
Cybercrime/Digital Fraud	Online fraud, identity theft, financial scams, unauthorised access	Economic losses; financial vulnerability; reduced trust in digital services
Critical Infrastructure Attacks	Malware, ransomware, attacks on government, financial and telecommunications systems	Service disruption; economic instability; compromised sensitive information, reduced national resilience.
Information Warfare	Narrative manipulation, strategic disinformation, influence operations	Public confusion; societal division; weakened democratic resilience

Source: Authors' Compilation from Reviewed Literature, Policy Documents, Institutional Reports and Cybersecurity Publications, 2015–2025.

DISCUSSION OF FINDINGS

Objective One: Examining How Cyber-Enabled Threats Expose the Limitations of Nigeria's Traditional Military-Territorial National Security Paradigm

The findings demonstrate that cyber-enabled threats have fundamentally altered Nigeria's security environment, exposing the limitations of a national security paradigm that remains predominantly centred on territorial defence, military power, and regime stability. The study shows that terrorism, insurgency, banditry, and electoral disinformation operate in digitally mediated environments, where cyberspace serves as an operational domain for recruitment, financing, propaganda, intelligence sharing, and strategic communication. Contemporary security threats transcend physical borders and conventional

military responses, thereby challenging the assumptions underpinning Nigeria's traditional national security architecture.

A major finding is that cyber threats in Nigeria's existing security discourse are only partially securitised. Although policy documents such as the National Security Strategy (2019) and the National Cybersecurity Policy and Strategy (2021) recognise cybercrime, terrorism, information warfare, and critical infrastructure protection as national security concerns, institutional responses remain fragmented. Cybersecurity continues to be viewed primarily as a technical, regulatory, or law-enforcement issue rather than as a strategic national security priority. This finding supports Mwangi (2024) and Kente and Ishaku (2024), who argue that conventional security paradigms are becoming inadequate for addressing cyber-enabled threats. However, this study complements existing scholarship by demonstrating that the principal challenge is not simply technological or institutional weakness but the incomplete securitisation of cyber threats within Nigeria's national security architecture. This is further borne out by Securitisation Theory, which shows that cyber threats have not been fully accepted as existential security issues requiring coordinated national responses.

The analysis reveals that Nigeria's securitisation process is marked by fragmented securitising actors, selective referent objects, and uneven audience acceptance. While the Presidency and the ONSA frame cyber threats as threats to sovereignty and national stability, operational responsibility remains dispersed across regulatory, civilian, and law-enforcement institutions with overlapping mandates. This fragmentation limits strategic coherence and reinforces a reactive rather than a preventive approach to cybersecurity governance. Security responses continue to prioritise regime stability and public order over citizen-centred concerns such as data protection, digital privacy, and societal resilience. These findings support Balzacq's (2011) argument that securitisation is shaped by institutional and political contexts rather than discourse alone.

This study shows that Nigeria's traditional military-territorial security paradigm is inadequate for a digitally mediated threat environment. From a Securitisation Theory perspective, limited audience acceptance and fragmented institutional responses constrain the full integration of cyber threats into national security priorities, resulting in partial securitisation despite their implications for national sovereignty, stability, and societal security.

Objective Two: Proposing a Reconceptualised National Security Framework that Integrates Cyber Power into Nigeria's National Security Architecture

The second objective examined how Nigeria's national security framework could be reconceptualised to integrate cyber power as a strategic domain. The findings reveal that effective integration requires a broader understanding of national security, extending beyond military defence to encompass human security, economic resilience, CNII, and strategic cyber governance. The study emphasises that cyber power could be embedded within national security planning as an essential component of state capacity and resilience.

A key finding is that broadening the referent objects of security provides a stronger conceptual foundation for cybersecurity governance. The study shows that individuals, economic systems, democratic institutions, and critical infrastructure have become legitimate security referents because they are increasingly vulnerable to cyber-enabled threats. This finding aligns with Buzan, Wæver, and de Wilde (1998), who argue that security

extends beyond the protection of the state, and supports Nye's (2017) position that cyber power has become an essential element of contemporary national power. However, this study advances the literature by showing that widening referent objects alone is insufficient without the corresponding institutional and strategic reforms needed to operationalise cyber power within Nigeria's security architecture.

Further findings indicate that institutional adaptation and strategic doctrine are indispensable to integrating cyber power. Fragmented mandates, bureaucratic rivalry, and limited cyber expertise continue to undermine coordinated governance despite the NCPS (2021). Effective integration therefore requires stronger inter-agency coordination, intelligence-led cybersecurity, collaboration with the private sector, and a clearly articulated national cyber strategy that embeds cyber power across defence, governance, deterrence, and resilience planning. These findings align with Maurer (2018), who emphasises coordinated cybersecurity institutions, while also broadening existing scholarship by demonstrating that institutional reform must be accompanied by a transformation in strategic thinking.

In Securitisation Theory terms, this reconceptualised framework requires a broader identification of referent objects and stronger institutional responses to translate the securitisation of cyber threats into effective national security practice. It also requires sustained acceptance among government institutions, the private sector, and citizens, so that cyber power becomes a legitimate and integrated component of Nigeria's national security architecture.

CONCLUSION AND RECOMMENDATIONS

Conclusion

This study examined the limitations of Nigeria's traditional military-territorial conception of national security in addressing cyber-enabled threats and proposed a reconceptualised framework for integrating cyber power into the national security architecture. Guided by Securitisation Theory and informed by qualitative analysis of policy documents, legal instruments, institutional reports, cybersecurity publications, and scholarly literature, the study demonstrates that rapid digitalisation has transformed Nigeria's contemporary threat environment. Terrorism, insurgency, banditry, organised crime, and electoral disinformation increasingly operate in digitally mediated environments, exposing weaknesses in a security architecture still largely oriented towards conventional military threats.

The findings establish that Nigeria's cybersecurity environment reflects partial and uneven securitisation. Although the NSS (2019) and NCPS (2021) recognise cyber threats as national security concerns, institutional responses remain fragmented and largely confined to technical, regulatory, law-enforcement, and ICT institutions. Analysis of securitising actors, referent objects, audience acceptance, and institutional responses reveals a persistent gap between the recognition of cyber threats in national security discourse and their effective integration into national security planning. Cyber threats are therefore securitised rhetorically to a greater extent than they are institutionally and strategically integrated.

Empirically, the study shows that terrorism, insurgency, banditry, electoral disinformation, cybercrime, and threats to critical infrastructure operate in digitally mediated environments. Cyberspace does not replace

conventional security threats; rather, it amplifies their reach, coordination, financing, propaganda, mobilisation, and societal impact. Nigeria therefore requires a more integrated approach that links physical insecurity with its digital dimensions.

Theoretically, the study contributes to Securitisation Theory by extending its application to cybersecurity governance in a developing-state context. It shows that cyber securitisation is shaped not only by security discourse but also by institutional fragmentation, uneven capacity, competing mandates, and the relationship between state and human security. This strengthens the theory's application to non-traditional security by linking threat construction to the strategic integration of cyber power.

The study further concludes that national security must extend beyond territorial sovereignty and regime stability to encompass individuals, economic systems, democratic institutions, and CNII. This requires stronger inter-agency coordination, cyber threat intelligence, public-private collaboration, critical infrastructure protection, and a coherent national cyber strategy. These measures must remain consistent with democratic accountability and human security. Ultimately, Nigeria's capacity to address hybrid and cyber-enabled threats depends on transforming its security architecture from a predominantly military-territorial model towards an integrated, cyber-aware, resilient, and human-centred framework, recognising cyber power as a strategic dimension of national power.

Recommendations

1. Reconceptualise National Security to Incorporate Cyber Power

The Federal Government of Nigeria (FGN) should formally revise Nigeria's National Security Strategy to recognise cyberspace as a strategic operational domain alongside land, maritime, air, and space. National security policy should explicitly integrate cyber power into defence planning, intelligence, critical infrastructure protection, strategic communication, and national decision-making.

2. Strengthen Institutional Coordination and Cyber Governance

The FGN should strengthen the ONSA's coordinating role by clarifying legal authority, harmonising institutional mandates, and establishing formal inter-agency coordination mechanisms involving defence, intelligence, law enforcement, regulatory agencies, technology institutions, and critical infrastructure operators.

3. Develop a Comprehensive National Cyber Strategy

The FGN should develop and maintain a coherent national cyber strategy that clearly defines national cyber objectives, strengthens cyber resilience and threat intelligence, promotes public-private partnerships, and aligns national cybersecurity policy with relevant ECOWAS, African Union, and international frameworks.

4. Promote Democratic and Human-Centred Cybersecurity Governance

The FGN should ensure that cybersecurity policies balance national security requirements with democratic accountability, constitutional rights, and human security. The government should strengthen public awareness, digital literacy, data protection, and stakeholder participation, while ensuring that exceptional cybersecurity measures are lawful, necessary, proportionate, and subject to effective legislative and judicial oversight.

Suggestions for Future Research

Future research could adopt comparative and empirical approaches to examine how

African states are reconceptualising national security by integrating cyber power, with particular attention to institutional capacity, securitisation processes, and democratic accountability. Further studies could use primary data, including elite interviews, expert surveys, and institutional case studies, to assess how securitising actors and relevant audiences perceive cyber threats and how these perceptions shape policy implementation. Research could also assess the effectiveness of Nigeria's proposed cyber-national security framework in addressing emerging hybrid threats, including artificial intelligence-enabled disinformation, cyberterrorism, attacks on critical infrastructure, and digital financial crime.

REFERENCES

African Union. (2014). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). African Union.

Aina, F., & Ojo, J. S. (2023). The webification of jihadism: Trends in the use of online platforms before and after attacks by violent extremists in Nigeria. Global Network on Extremism and Technology.

Akinwale, A. A. (2022). Digital activism and separatist mobilisation in Nigeria. African Security Review, 31(3), 287–304.

Balzacq, T. (Ed.). (2011). Securitisation theory: How security problems emerge and dissolve. Routledge.

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner Publishers.

Centre for Democracy and Development. (2023). Disinformation and elections in Nigeria. Centre for Democracy and Development.

Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism. Studies in Conflict & Terrorism, 40(1), 77–98. https://doi.org/10.1080/1057610X.2016.1157408

Drezner, D. W. (2024). How everything became national security. Foreign Affairs.

Economic Community of West African States. (2020). ECOWAS regional cybersecurity and cybercrime strategy. ECOWAS Commission.

Egloff, F. J. (2020). Public attribution of cyber intrusions. Journal of Cybersecurity, 6(1), tyaa012. https://doi.org/10.1093/cybsec/tyaa012

Federal Republic of Nigeria. (2014). National cybersecurity policy and strategy. Office of the National Security Adviser.

Federal Republic of Nigeria. (2015). Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. Government Printer.

Federal Republic of Nigeria. (2019). National security strategy. Office of the National Security Adviser.

Federal Republic of Nigeria. (2021). National cybersecurity policy and strategy. Office of the National Security Adviser.

Floyd, R. (2010). Security and the environment: Securitisation theory and US environmental security policy. Cambridge University Press.

Floyd, R. (2016). Extraordinary or ordinary emergency measures: What, and who, defines the 'success' of securitisation? Cambridge Review of International Affairs, 29(2), 677–694. https://doi.org/10.1080/09557571.2016.1202870

Global Network on Extremism and Technology. (2023). Research digest on extremist use of online platforms.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. International Studies Quarterly, 53(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Independent National Electoral Commission. (2022). Election technology and results management framework. Independent National Electoral Commission.

International Telecommunication Union. (2008). Overview of cybersecurity: Recommendation ITU-T X.1205. International Telecommunication Union.

Kello, L. (2017). The virtual weapon and international order. Yale University Press.

Kente, J. S., & Ishaku, J. (2024). Issues and perspectives on cyberterrorism and information security in Nigeria. ALSYSTECH Journal of Education Technology, 2(3), 174–190. https://doi.org/10.58578/alsystech.v2i3.3237

Makinde, O., & Akinwale, A. A. (2021). Terrorist financing and digital platforms in Nigeria. Journal of Money Laundering Control, 24(4), 897–912.

Maurer, T. (2018). Cyber mercenaries: The state, hackers, and power. Cambridge University Press.

Mustapha, A. R. (2020). Banditry and insecurity in northern Nigeria. African Affairs, 119(477), 660–675.

Mwangi, P. (2024). Cybersecurity threats and national security in the digital age. American Journal of International Relations, 9(1), 26–35. https://doi.org/10.47672/ajir.1938

North Atlantic Treaty Organisation. (2016). Cyber defence pledge. NATO.

Nye, J. S. (2010). Cyber power. Belfer Center for Science and International Affairs, Harvard Kennedy School.

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. International Security, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

United Nations Development Programme. (1994). Human development report 1994: New dimensions of human security. Oxford University Press.

Uwalaka, T. (2021). Social media, separatism and state response in Nigeria. Journal of Asian and African Studies, 56(6), 1401–1418.

Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press.

Williams, P. D. (Ed.). (2018). Security studies: An introduction (3rd ed.). Routledge.

Yarger, H. R. (2006). Strategic theory for the 21st century: The little book on big strategy. Strategic Studies Institute, U.S. Army War College.