COGNITIVE WARFARE: DEFENDING NIGERIA'S "HUMAN DOMAIN" AGAINST AI-DRIVEN PERCEPTION MANAGEMENT AND INDUSTRIALIZED DISINFORMATION

ANTHONY CHINEDUUGWU, PhD
Department of Political Science, Federal University of Lafia
Chinedugwu5@gmail.com

AHMADU OCHOCHE ENEJE, PhD
Department of Political Science, University of Abuja-Nigeria
enejeochoche@gmail.com

DOI: https://doi.org/10.64633/wissj.v10i4.06

Keywords

Cognitive warfare; Securitisation theory; Artificial intelligence; Disinformation; Digital resilience

Abstract

Research Problem: *This study examines cognitive warfare as an emerging national security threat in Nigeria, particularly in the context of AI-driven perception management and industrialised disinformation within the human domain. It investigates how platform dynamics, identity politics, institutional trust deficits, and low digital literacy increase vulnerability to coordinated media manipulation.*

Methods/theory: *The study is anchored on Securitisation Theory, reinterpreted to focus on the securitisation of manipulative informational processes such as synthetic media production, algorithmic amplification, and coordinated inauthentic behaviour. A qualitative approach is adopted using secondary data from policy reports, governance documents, and peer-reviewed literature. Interpretive policy analysis is used to strengthen contextual understanding of governance responses.*

Results: *Findings indicate that cognitive warfare has evolved into a technologically enabled form of strategic competition targeting trust, emotions, and decision-making. Nigeria's institutional frameworks remain fragmented, reactive, and poorly coordinated, with significant gaps in strategic communication, AI detection capacity, and digital literacy. These weaknesses collectively heighten national vulnerability to disinformation ecosystems. Attention is also given to the role of platform algorithms in amplifying polarisation.*

Conclusion: *The study concludes that safeguarding Nigeria's human domain requires a comprehensive resilience-based framework that integrates technological, institutional, and civic dimensions of information security.*

Key Contribution to Knowledge: *The paper extends Securitisation Theory to digital psychological conflict and introduces an integrated resilience model for understanding AI-enabled cognitive warfare in Nigeria.*
Recommendation: *It recommends enhanced digital literacy programmes, inter-agency coordination, strategic communication reforms, investment in AI-driven detection systems, and strengthened civic resilience mechanisms to protect democratic trust and cognitive autonomy. Urgent policy coordination is required across security and communication institutions.*

Introduction

The twenty-first century has seen a significant change in the strategic environment. Conventional security theories that emphasise military deterrence, territorial defence, and infrastructure protection are becoming less and less adequate to describe modern threats. States now have to deal with enemies that want to undermine societies by influencing people's thoughts, feelings, identities, and collective behaviour rather than by using traditional violence. The human domain, where attitudes, perceptions, trust systems, and decision-making processes become targets of strategic contestation, is a typical description of this developing battlefield (NATO Innovation Hub, 2021). In this regard, one of the most significant security issues of the digital era is cognitive warfare.

The intentional use of information, psychological strategies, digital technologies, and behavioural impact tools to mould people's thoughts, emotions, perceptions of reality, and behaviours is known as cognitive warfare. Artificial intelligence, machine learning, predictive analytics, synthetic media, algorithmic targeting, and large-scale data extraction all contribute to cognitive warfare, in contrast to traditional propaganda. With previously unheard-of speed and scope, these technologies allow adversaries to industrialise disinformation, automate deception, and personalise persuasion (Kello, 2022). In addition to disseminating lies, the goal is to weaken societal cohesiveness, undermine institutional credibility, exacerbate identity conflicts, skew democratic choice, and hinder national decision-making.

An especially important case for researching cognitive warfare is Nigeria. Nigeria holds a key role in continental politics as the most populous state in Africa, the biggest democratic market, and a significant regional force. However, it also has a number of weaknesses that make the human domain extremely debatable. Election-related tensions, youth unemployment, digital inequality, insurgent narratives, secessionist agitation, rapid social media penetration, and ethnoreligiouspolarisation are a few of these. Nigeria's growing digital population has given citizens access to previously unheard-of chances for civic engagement, but it has also exposed them to coordinated influence campaigns, hate speech, false narratives, manipulated videos, bot-driven propaganda, and both domestic and foreign disinformation networks (Ibrahim &Aduloju, 2024).

This risk is demonstrated by recent political developments. Conspiracy theories, falsified endorsements, distorted ethnic narratives, and fraudulent assertions regarding voting procedures have all proliferated on message platforms throughout election cycles. Misinformation impaired adherence to health

precautions during public health emergencies. Fake casualty statistics and staged material increased mistrust and anxiety during security emergencies. These trends imply that Nigeria's security issue now encompasses protecting cognition, trust, and social resilience in addition to defending land.

Even while misinformation and cyber security are receiving more attention, there are still a lot of holes in the literature. First, without conceptualising these phenomena within the larger strategic logic of cognitive warfare, many studies on Nigeria concentrate only on hate speech, fake news, media ethics, or cybercrime. Such fragmentation makes it difficult to see how organised initiatives aimed at strengthening national resilience may include isolated information disorders. Second, a large portion of the worldwide literature on cognitive warfare comes from security organisations in the Euro-Atlantic region and frequently focuses on the rivalry between Russia, China, NATO, and Western democracies (Claverie& du Cluzel, 2020). The sociopolitical complexity of plural societies like Nigeria, where identity cleavages and developmental disparities intersect with digital manipulation in distinctive ways, is not well captured by these models.

Third, the importance of artificial intelligence in Nigeria's information environment has not received enough attention in scholarly research. Older fake news frameworks are unable to adequately account for the additional threats brought about by the emergence of generative AI, deepfakes, automated content farms, microtargeting systems, and sentiment analysis tools. Fourth, little research has been done on the relationship between cognitive threats and Nigerian national security doctrine, civil military strategy, electoral governance, education policy, and community resilience. As a result, practical solutions continue to be fragmented, reactive, and technologically behind.

The practical gap is just as crucial. Nigeria has agencies that deal with intelligence, election management, broadcasting regulation, cyber security, and strategic communication. These organisations, however, are still unprepared for AI-enabled perception management campaigns, frequently function in silos, and lack cohesive doctrine on cognitive defence. Legal frameworks are unable to keep up with automated manipulation and synthetic media, public digital literacy initiatives are inconsistent, and platform accountability is still lacking. Instead of developing resilience in advance, current approaches frequently appear after harm has been done. Therefore, by redefining misinformation, psychological influence, and AI-mediated narrative warfare into the strategic framework of cognitive warfare, this study tackles both academic and practical inadequacies. Through coordinated policy, institutional innovation, democratic protections, technological capability, and civic resilience, it aims to create a paradigm unique to Nigeria for protecting the human realm. By extending cognitive warfare theory beyond Euro-Atlantic contexts and offering practical tactics appropriate for Nigeria's diverse and quickly digitising society, the paper advances research.

Statement of the Problem

Historically, territorial concerns including insurgency, banditry, separatist violence, piracy, and organised crime have been given top priority in Nigeria's national security architecture. Even though these risks are still serious, there is another, less obvious concern that has grown in the information world. Disinformation networks made possible by AI, synthetic media,

algorithmic amplification, and well-planned psychological operations are all progressively influencing public opinion, escalating social unrest, and undermining institutional trust.

The issue is that Nigeria does not have a clear framework for identifying and addressing cognitive warfare as a threat to national security. Current initiatives frequently address misinformation as a media, cyber, or electoral problem separately. The way hostile actors strategically exploit cognitive vulnerabilities across sectors at the same time is not addressed by this disjointed approach. False narratives consequently proliferate more quickly than corrections, public trust erodes, and democratic processes become more susceptible. These developments could worsen societal division, impair crisis management, undermine government, and lessen Nigeria's strategic clout if they are not handled. Therefore, the pressing issue is how Nigeria can use a coordinated, democratic, and technologically informed strategy to protect its human domain against AI-driven perception management and manufactured disinformation.

Objectives of the Study

The paper has the following objectives:

1. To examine the nature and evolving dimensions of cognitive warfare in the contemporary digital environment.
2. To analyse Nigeria’s structural vulnerabilities to AI driven perception management and industrialised disinformation.
3. To assess the limitations of current institutional, legal, and policy responses in Nigeria.

Operational Clarification of Related Key Concepts

Cognitive warfare: The strategic manipulation of perceptions, logic, emotions, and behaviour to sway populations and decision-makers without necessarily employing physical force is known as cognitive warfare.

Human Domain: The social and psychological environment made up of people's identities, beliefs, values, trust systems, morale, and behavioural patterns is referred to as the human domain.
Perception management: is the process of using framing, symbolism, emotional triggers, and selected information to affect how viewers see actors, events, and realities.

Industrialised Disinformation: Using bots, troll farms, AI tools, and coordinated networks, false or misleading narratives are produced and disseminated in a methodical, scalable, and frequently automated manner.

Artificial intelligence: is the term used to describe computational systems that are able to carry out activities that have historically required human intelligence, such as pattern recognition, prediction, language generation, and automated decision support.

National resilience: The ability of a society or state to withstand shocks, adjust to upheaval, and preserve functional legitimacy in times of crisis is known as national resilience.

Review of Related Literature:

Disinformation has evolved from isolated lies, rumours, and amateur deceit into a complex system of coordinated strategic impact, as the literature on information disorder increasingly acknowledges. Previous research frequently

conceptualised false news as a result of individual wrongdoing, partisan contestation, or subpar journalism. However, more recent research shows that coordinated infrastructures including data analytics, algorithmic amplification, psychological profiling, synthetic media generation, and cross-platform dissemination networks are being used in digital manipulation. Disinformation has thus taken on an industrial nature, a strategic purpose, and a political outcome.

Bradshaw and Howard's (2023) concept of computational propaganda offers one of the most significant interpretations of this shift. They contend that in order to affect public opinion, modern influence operations rely more and more on automated accounts, bot networks, coordinated inauthentic activity, and algorithmically tailored communications. Their main contribution is to show that persuasive speech and state broadcasting power are no longer the only sources of propaganda in the digital age. Instead, it increasingly depends on platform architectures that favour material that is sensational, divisive, and emotionally charged. This discovery is especially pertinent to Nigeria, where social media ecosystems with high involvement but uneven fact checking capacity are frequently used for political mobilisation. However, Bradshaw and Howard focus primarily on global trends and regime comparisons, leaving open the question of how particular states with multiple identities and low institutional trust might develop customised resilience mechanisms.

Although their work clarifies the issue, it provides little advice on how nations like Nigeria should protect the human domain. By situating artificial intelligence within the larger evolution of strategic competition, Kello (2022) expands the discussion. Kello claims that AI significantly increases the accuracy of influence tactics while reducing the operational expenses of deception. Actors can use machine learning algorithms to predict behavioural responses, identify vulnerable audiences, customise narratives, and continuously improve persuasion tactics based on real-time feedback. This is different from conventional propaganda, which was frequently abrasive and mass-oriented. AI-enabled manipulation is scalable, adaptive, and selective. This realisation is particularly important in Nigeria, where digital growth has outpaced investments in institutions that foster trust, platform regulation, and civic education. Personalised lies can earn credibility through social proximity rather than factual correctness in settings where a large number of people rely on peer-to-peer forwarding services like Telegram and WhatsApp. However, great power rivalry and strategic competition among advanced states continue to be the main focus of Kello's research. It does not adequately address the weaknesses of emerging democracies, where deficiencies in governance, identity contestation, and economic precariousness foster cognitive intrusion.

Ibrahim and Aduloju (2024) contribute significantly to Nigerian scholarship by analysing disinformation during election processes. According to their research, false narratives regarding candidates, ethnic blocs, voting technology, and electoral violence are widely disseminated via WhatsApp, Facebook, TikTok, and increasingly short video platforms. They show that false information is rarely random in Nigeria. Rather, it often takes advantage of preexisting divisions based on religion, race, regionalism, and mistrust of governmental institutions. Their work is important because it domesticates the discussion and demonstrates how local political realities interact with global digital trends. Nonetheless, campaign communication and election seasons

continue to be the study's primary focus. It does not adequately conceptualise these deceptive tactics as a component of a more comprehensive theory of cognitive warfare that can be used in times of peace, public health emergencies, security crises, or economic reforms. As a result, the literature runs the risk of considering misinformation as episodic rather than systemic. By highlighting media and information literacy as a basis for democratic resilience, UNESCO (2023) advances yet another important line of research. According to UNESCO, citizens must be able to evaluate sources critically, confirm statements, comprehend platform incentives, and fend off deceptive content. This strategy is particularly pertinent in Nigeria, where young people are strongly connected online and where public opinion is being shaped by online activity. Being media literate helps lessen one's vulnerability to emotionally manipulated lies, conspiracies, and frauds. However, when faced with large-scale influence operations carried out by structured domestic networks, transnational actors, or politically supported organisationsutilising sophisticated automation techniques, literacy-based frameworks might not be adequate. While individual critical thinking is still important, it cannot take the place of national coordinating structures, platform responsibility, or institutional detection systems. Therefore, when it comes to high-intensity cognitive conflict, UNESCO's contribution is fundamental but insufficient. Adeyemi and Okonkwo (2025) investigate cyber governance and digital institutional coordination in Nigeria, focusing on the governance aspect of the issue. According to their results, public communication organs, telecommunications companies, electoral authorities, intelligence agencies, and regulatory entities are all fragmented. The Nigerian state's capacity to react cogently to quickly changing digital threats is weakened by overlapping missions, bureaucratic rivalries, inconsistent legislative frameworks, and uneven technical capacity. This diagnosis provides compelling evidence that the problem of misinformation cannot be resolved by a single ministry or authority acting alone. Instead, a whole-of-society and government approach is needed. However, even while the study identifies governance flaws, it does not adequately incorporate the behavioural and psychological aspects that set cognitive warfare apart from traditional cyberthreats. To put it another way, protecting computers and networks does not automatically protect people's thoughts and perceptions.

Beyond these findings, new worldwide research on deepfakes and synthetic media emphasises how serious the problem is. Chesney and Citron (2024) caution that by making deceit inexpensive and truth disputable, realistic AI-generated audio and video can threaten the evidentiary foundation of public life. phoney speeches, phoney endorsements, or faked disaster footage can cause panic in societies already characterised by mistrust before verification systems react. Due to Nigeria's history of quick message dissemination and emotionally charged political mobilisation, synthetic media may be especially unstable during elections, intercommunal conflicts, or security situations.

In a similar vein, Bennett and Livingston (2023) contend that when institutions lack legitimacy, misinformation thrives. In Nigeria, where historical grievances, perceptions of corruption, unequal service delivery, and elite contestation frequently erode trust in official communication, this idea strikes a deep chord. In these situations, people might accept rumours that support past grievances while mistrusting verifiable information. This implies that government change and cognitive defence are

inextricably linked. A state needs to increase its credibility in addition to improving its communication.

NATO Innovation Hub (2021) defines cognitive warfare from the standpoint of security studies as an attempt to weaponise information, psychology, neuroscience, and behaviouralscience in order to affect how people think and make decisions. This concept shifts study away from content alone and toward the deeper goal of behavioural disruption, which helps provide light on the Nigerian instance even though it was designed in Euro Atlantic strategic circumstances. However, rather than emphasising democratic resilience in diverse African countries, the majority of applications of this framework concentrate on state rivalry, military preparedness, and alliance security.

When considered collectively, the evaluated literature identifies significant gaps that support the current investigation. First, misinformation, cyber security, psychological operations, media literacy, and governance change are addressed as distinct issues rather than as interrelated aspects of cognitive warfare due to a continuous conceptual fragmentation. Second, applications in Africa, and particularly in Nigeria, are still in their infancy. A large portion of the underlying theory was established in Western security environments, whose institutional capacities are very different from Nigeria's. Third, a lot of research concentrates on diagnosis rather than integrated remedies, giving little consideration to the ways in which institutional reforms, technology instruments, civic education, democratic safeguards, and strategic communication might be integrated into a cohesive national security model.

Fourth, the human sphere as the principal battlefield is not given enough emphasis in the literature. The majority of current solutions aim to control platforms, penalise violators, or rectify misinformation after it has been shared. Building social cohesiveness, trust, emotional resilience, and critical thinking skills—all of which reduce a population's initial susceptibility to manipulation—receives far less attention. Fifth, there aren't many studies that specifically link Nigeria's national security doctrine, electoral integrity systems, and community-level peace architecture to AI-driven perception management. This study aims to fill in these gaps. The study goes beyond specific discussions about fake news and suggests a multifaceted approach to protecting the human domain by placing Nigeria's information vulnerabilities within the larger framework of cognitive warfare. By doing this, it adds to the growing body of knowledge on AI-enabled strategic influence in emerging democracies from a theoretical and practical standpoint.

Theoretical Framework

Securitisation Theory, which was first created by Buzan, Waever, and de Wilde (1998) within the Copenhagen School of security studies, is adopted in this work. The theory describes how political rhetoric, elite framing, and institutional acceptance lead to the recognition and treatment of particular situations as security risks. Essentially, a problem becomes securitised when powerful players are able to persuade pertinent audiences that it presents an existential threat necessitating extraordinary and immediate action that goes beyond ordinary politics. Securitisation theory has historically been applied extensively to issues where governments justify drastic measures in the name of collective survival, such as migration, terrorism, environmental degradation, pandemics, and energy instability.

This theory's ability to describe how new dangers are socially formed, prioritised, and regulated makes it relevant to the current investigation. Many security organisations in Nigeria continue to focus primarily on physical threats such organised crime, banditry, insurgency, and separatist violence. However, the emergence of coordinated false narratives, AI-driven manipulation, and digitally created mistrust shows that risks to national stability are increasingly coming from the realm of perception, cognition, and public consciousness. Although they might not directly destroy infrastructure, these threats have the potential to erode legitimacy, polarise communities, skew elections, incite violence, and compromise the state's ability to effectively govern. Therefore, this work extends securitisation theory to the intangible domain of cognition in a unique and novel way. The study advocates for the securitisation of manipulative processes themselves rather than populations, dissent, or valid criticism. These include deepfake operations, algorithmic radicalisation, bot-driven propaganda systems, coordinated AI deception, synthetic influence campaigns, and industrial misinformation infrastructures intended to undermine confidence and destabilise society. In this way, safeguarding the integrity of democratic communication and public thinking takes precedence over policing opinion.

The referent object of security is expanded under this reading. It is no longer restricted to maintaining a regime or maintaining geographical sovereignty. Rather, democratic trust, citizen autonomy, electoral credibility, institutional legitimacy, and social cohesiveness are the things that need to be protected. The long-term security of the state is also jeopardised when these underpinnings are routinely undermined. It is possible for a nation to maintain its borders while losing the trust, cohesion, and ability to make logical decisions required for efficient government. This theoretical modification advances knowledge in a number of significant ways. First, by acknowledging that contemporary dangers frequently target minds before they target land, it extends securitisation theory into the arena of digital psychological conflict. Second, it shifts policy and scholarly focus away from specific censorship discussions and toward resilience-centered governance, where technology readiness, education, transparency, and strategic communication become essential defence mechanisms. Third, it provides a normative framework for striking a balance between civil freedoms and security requirements in democracies like Nigeria, making sure that reactions to misinformation do not turn into tools of oppression. Fourth, it provides insights from Nigeria's diverse social structure, democratic experience, and quickly developing digital ecosystem to enhance global security studies by localising a primarily Western theoretical framework inside an African setting.

Methodology

Because the topic of cognitive warfare, AI-driven perception management, and industrialised disinformation is best understood through interpretation of patterns, narratives, institutional responses, and strategic behaviours rather than through numerical measurement alone, the paper takes a qualitative research approach using secondary data sources. The study's use of qualitative analysis allows it to investigate how disinformation campaigns function, how institutions and citizens react, and how Nigeria's digital environment shapes political beliefs, identity, fear, and trust.

Because the phenomenon is current, multidisciplinary, and well documented in

academic journals, policy reports, government publications, cybersecurity assessments, media studies, and reports from international organisations, the use of secondary sources is especially relevant. These resources offer reliable information on new trends, case studies, technical advancements, and comparative experiences that would be challenging for one researcher to produce quickly through primary fieldwork.

In order to create a thorough framework for protecting Nigeria's human domain, the article also synthesises insights from political science, communication studies, security studies, and digital governance thanks to secondary qualitative data. As a result, it is both practically effective and methodologically appropriate for dealing with the intricate and dynamic character of cognitive warfare.

Evolution and Mechanisms of Cognitive Warfare in Global Strategic Competition

Conflict has expanded beyond the conventional domains of land, sea, air, and cyberspace into the sphere of cognition, where perception, judgement, trust, and behaviour become contested assets, as the literature on modern strategic competition increasingly shows. Previous security research tended to conceptualise combat in material terms, gauging power by army strength, weaponry, economic capability, and geographical control. Recent research, however, suggests that influencing how societies perceive reality and react to events may be more important in today's competition than eliminating an adversary's forces (Rid, 2020). Although this change is fundamental to the idea of cognitive warfare, it is frequently treated in the literature as a new event unrelated to historical continuity. Analytically, such a view is lacking. This paper contends that although cognitive warfare's technology is novel, its strategic reasoning is based on long-standing attempts to affect legitimacy, morale, and decision-making. The ability to exert such influence through digital systems has changed in terms of speed, scale, accuracy, and persistence. The historical development of influence operations from traditional propaganda to technologically assisted cognitive warfare is a first significant problem in the literature. Conventional propaganda studies focused on state broadcasting, censorship, symbolic message, and mass persuasion through newspapers, radio, and television, particularly those rooted in twentieth-century warfare communication (Jowett & O'Donnell, 2022). These models used the assumption that audiences were passive recipients in comparatively centralised communication networks. Recent research casts doubt on this notion by demonstrating how people are now both consumers and creators of influence content thanks to digital platforms. According to Bradshaw and Howard (2023), modern propaganda today spreads via networked participation, where individuals unintentionally magnify deceptive narratives by sharing, commenting, and emotional involvement. Their contribution is important since it shows that influence is no longer merely passed from state to citizen. The continuity between old and modern forms is still undervalued in the literature, nevertheless. This paper argues that cognitive warfare should be viewed as an algorithmically accelerated mutation of propaganda rather than its replacement. While the delivery infrastructure has become decentralised, adaptable, and behaviourally aware, the persuasive purpose is still the same.

Whether cognitive warfare is essentially a state tactic or a more widespread phenomenon involving several players is the subject of a

second question. Previous strategic analyses frequently linked influence operations to military and state intelligence agencies. This position is complicated by recent findings. According to Pomerantsev (2024), information manipulation is currently carried out by private contractors, data analytics companies, ideological networks, criminal organisations, and international activist groups. Due to the difficulty of assigning guilt, this pluralisation of players undermines traditional deterrence approaches. Deniability is made possible by attribution issues, which also make it difficult to distinguish between foreign meddling and domestic chaos. However, some scholarship continues to highlight powerful nations like the US, China, and Russia as the main perpetrators of cognitive war. Although these actors are still significant, this focus runs the risk of ignoring the action of domestic elites, nonstateorganisations, and regional forces that use the same weapons for local gain. Thus, by seeing cognitive warfare as an ecosystem rather than a state monopoly, this study takes a more comprehensive stance. These days, hybrid assemblages of political, commercial, ideological, and criminal players are involved in strategic competition, and their interests may momentarily align behind manipulation tactics.

The use of artificial intelligence as a force multiplier is a third worry in the literature. According to existing research, artificial intelligence (AI) has revolutionised influence operations by facilitating automation, predictive targeting, and the creation of synthetic content (Kello, 2022). Machine learning algorithms are capable of producing compelling material at scale, identifying vulnerable communities, analysing audience sentiment, and optimising message timing. Additionally, realistic visuals, audio, and video that mimic authority and authenticity can be produced via deep learning algorithms. Chesney and Citron (2024) caution that because citizens can no longer readily discern between authentic and fake records, such technologies undermine the factual underpinnings of democratic discourse. Although this diagnosis is convincing, a large portion of the research presents AI mainly as a technology problem that calls for platform moderation and detection tools. The frame is too limited. According to this study, AI is a political amplifier of pre-existing societal divisions rather than just a technical tool. The most harmful consequences arise not from machines lying on their own, but rather from their exploitation of societal tensions, grievances, and mistrust. The policy conclusion is that without social rehabilitation, technical responses will continue to be inadequate.

The methods via which cognitive warfare results in behavioural impacts constitute a fourth problem. Communication researchers frequently highlight agenda-setting, repetition, and exposure to false information as means of persuasion. However, more recent behavioural research indicates that identity reinforcement and emotional activation are more effective ways for influence to succeed than factual conversion (Pennycook& Rand, 2023). When lies fit with preexisting worldviews or group allegiances, people usually reject corrections. This discovery is significant because it casts doubt on the notion that deception can only be defeated by truth. However, by suggesting that populations are easily controlled, some studies exaggerate psychological determinism. These interpretations run the risk of depicting citizens as helpless victims. This study takes a more nuanced stance, contending that although audiences have agency, social cohesiveness, media literacy, and institutional trust are necessary for their resilience. Therefore, rather than being unilateral, cognitive warfare is

relational. Although manipulators take calculated risks, their success hinges on weaknesses in the target environment. The strategic goals of cognitive warfare represent a fifth concern. Disinformation is defined by numerous studies as an attempt to convince audiences of misleading claims. This understanding underestimates the larger objectives of contemporary campaigns, even though it is somewhat correct. According to Rid (2020), effective active measures frequently aim for immobility, cynicism, and bewilderment rather than persuade. Decision-making gets dispersed and democratic accountability deteriorates if citizens stop trusting any source. This is an important distinction. The goal can be to persuade people that the truth is unknown rather than to persuade them that a false narrative is true. This tendency has been noted in the literature, but its governance implications have not received enough attention. According to this study, communities that experience persistent epistemic ambiguity are more difficult to rule, more prone to polarisation, and more vulnerable to authoritarian reactions. Thus, cognitive warfare simultaneously jeopardises state efficacy and liberal openness.

The connection between platform architecture and strategic manipulation is a sixth problem. According to Bennett and Livingston (2023), scholars are increasingly observing that digital platforms are not neutral conduits but rather settings shaped by recommendation algorithms, engagement incentives, and monetisation logics that promote indignation and virality. These algorithms unintentionally favour content that is contentious and emotionally intense, which benefits deceptive actors. However, platforms are sometimes given undue responsibility in the prevailing literature. Although platform design is important, this study argues that platforms are not only causes but also enabling structures. Cognitive weaknesses are also maintained by elite opportunism, sensationalist media cultures, political polarisation, and inadequate civic education. If platforms are overregulated without addressing more significant democratic deficiencies, manipulation may simply move to fringe channels, encrypted networks, or offline mobilisation.

The militarisation of cognition is a seventh problem in international strategic struggle. According to NATO Innovation Hub (2021), cognitive warfare is an attempt to use data analytics, behavioural science, psychology, and neuroscience to hack the human. Because it acknowledges the human mind as a strategic landscape, this approach is valuable. However, military-centric frameworks may minimise the civic aspects of cognitive defence and frequently emphasise the rivalry between superpowers. The first burden of resilience is often placed on civilian institutions, schools, journalists, electoral bodies, religious organisations, and local communities. Therefore, by placing defence of cognition inside a whole of society model, this study deviates from simply military interpretations. Social trust may be more important in plural democracies than intelligence alone.

Measurement and evidence are an eighth problem. A large portion of the research on cognitive warfare is based on anecdotal evidence of viral lies, platform takedown reports, or descriptive case studies. These sources are informative, but they frequently fail to prove that exposure and behaviourare causally related. For instance, not all people who come across manipulative content alter their political views or employ violence. Tucker et al. (2023) urge more context-sensitive analysis and warn against making deterministic assumptions about media

effects. This prudence is essential, but too much cynicism might sometimes mask actual dangers. This study adopts the stance that direct conversion results alone should not be used to gauge the effects of cognitive warfare. Even while behavioural changes are hard to measure, agenda distortion, trust erosion, emotional weariness, and institutional delegitimation are important repercussions. Cumulative strategic damage may be underestimated by a strict requirement for quantifiable causality.

The normative conflict between preventing manipulation and defending civil freedoms is the eighth issue. Content limitations are often justified by governments as a means of preventing misinformation. However, academics caution that anti-disinformation legislation may be misused to restrict opposition voices, journalists, or critics (Freedom House, 2024). In competitive political systems, where incumbents may characterise disagreement as lies, this issue is particularly pressing. While existing scholarship correctly highlights these risks, some narratives present the issue as a binary option between authoritarian repression and unrestricted expression. That dichotomy is rejected in this investigation. Transparent platform regulations, independent fact-checking, algorithmic accountability, civic education, targeted penalties for coordinated inauthentic activity, and due process protections can all help to strengthen democratic resilience. Rather than simple repression or permissiveness, the problem is institutional design.

The geography of knowledge production is a tenth concern. The majority of the most influential research on cognitive warfare comes from North American and European settings, frequently concentrating on Chinese influence, Russian meddling, or the security of Western elections. Although not always transportable, these contributions are significant. Multilingual publics, unofficial media networks, limited computer literacy, youth unemployment, and diminished institutional trust are among the unique challenges facing developing democracies. Therefore, when existing frameworks are used globally without modification, they run the risk of conceptual overreach. According to this study, cognitive warfare needs to be understood in the context of regional political economy and social divisions. Strategic manipulation is influenced by the vulnerabilities and histories of every civilisation; it does not function in a vacuum. The cumulative review indicates that the literature has advanced significantly in identifying tools, actors, and risks associated with cognitive warfare. However, there are still a number of gaps. First, technology explanations frequently overlook the sociopolitical circumstances that facilitate manipulation. Second, the significance of hybrid nonstate networks is undervalued by state-centric methods. Third, democratic and civic resilience are not sufficiently engaged by military systems. Fourth, indirect consequences like institutional fatigue and erosion of trust are often ignored in measurement discussions. Fifth, in order to accommodate plural societies in the Global South, Western-centered models must be modified. up order to fill up these gaps, this work conceptualises cognitive warfare as a technologically mediated conflict over meaning, legitimacy, and collective behaviour, the results of which rely on how hostile capabilities and domestic vulnerabilities interact.

Who controls narratives, defines reality, and maintains trust in the face of uncertainty may become the key fight in global strategic competitiveness. Although material power is still significant, it can be politically neutralised in the absence of cognitive

resilience. Thus, this study supports the idea that protecting the human domain is no longer a secondary objective of communication policy. In the digital age, it is essential to both democratic survival and national security.

Nigeria's specific vulnerabilities within the human domain, including identity politics, institutional trust deficits, and platform dynamics

Kinetic threats like insurgency, banditry, communal violence, piracy, and organised crime have historically been given priority in the literature on Nigeria's security environment. Even if these issues are still important, more recent research is beginning to acknowledge that the human domain where identities, perceptions, emotions, and trust relationships influence political behaviour and national resilience is the deeper terrain of contestation. In this situation, military measurements or evaluations of cyber infrastructure are insufficient to comprehend Nigeria's vulnerabilities. Cognitive disruption is especially powerful because it is entwined with historical divisions, governance deficiencies, communication ecologies, and digital platform structures. Although some of these issues have been discovered in previous research, many of them are still analytically compartmentalised. This section contends that rather than being the result of a single factor acting alone, Nigeria's human domain vulnerability is systemic, resulting from the interplay of identity politics, institutional mistrust, economic precarity, and platform-driven amplification.

Identity politics as a structural weakness is one of the most enduring problems in the literature. Nigeria's postwar state construction resulted in a politically cohesive region with a variety of ethnic, linguistic, and religious groups that had unequal access to resources and power. Scholars have long maintained that identity categories, rather than ideological programs or alternative policies, are frequently used to frame struggle for state power (Suberu, 2023). Appealing to region, ethnicity, religion, and indigenousness is a common strategy used in electoral mobilisation. According to recent research, digital communication has not replaced existing divisions but rather created new avenues for their quick mobilisation (Ibrahim &Aduloju, 2024). Because they appeal to preexisting concerns, false narratives that depict groups as dangers, victims, or conspiracies can spread swiftly. Although identity boundaries are frequently treated as unchanging cultural truths, this literature persuasively highlights identity as a driver of vulnerability. A view like that is insufficient. According to this study, identity cleavages are not inherently determinative but rather politically activated. When they are deliberately weaponised through digital narratives by elites, influencers, and coordinated networks, they become hazardous. Therefore, the issue is not diversity per se, but rather the manipulability of unresolved identity issues in an information environment with inadequate mediation.

Historical trauma and ethnoreligious memory are closely related issues. According to a number of studies, the interpretation of modern communications is still influenced by memories of the civil war, recurrent occurrences of communal violence, and regional mistrust (Osaghae, 2022). Rumours don't enter neutral space in these situations. They are mediated by symbolic memories and inherited phobias. Because it resonates with prior experiences, a false allegation of attacks, marginalisation, or dominance may consequently gain credence. The literature currently in publication accurately recognises the permanence of historical memory, yet it frequently ends at a descriptive explanation. This study supports the claim that when institutions are unable to offer convincing

narratives of reconciliation and a common civic identity, memory becomes a strategic vulnerability. Manipulative actors might constantly reawaken dormant worries for current political advantage in areas where national storytelling is still contested.

Deficits in institutional trust are another important problem. Because citizens are more likely to reject lies when they believe official communication to be credible, trust in public institutions is essential to resilience. Due to allegations of corruption, selective law enforcement, election disputes, insecurity, and uneven service delivery, Nigerian academia is progressively documenting a decline in trust in state institutions (Adeosun&Nwangwu, 2025). Regardless of their veracity, unofficial sources gain credibility when people believe that public institutions act partisan or withhold the facts. This discovery is important because it moves the focus from content verification to messenger validity. However, rather than framing trust shortfalls as security concerns, some research simply describe them as governance results. This essay makes the case that mistrust is a tactical advantage for adversaries. Cognitive attacks become more affordable and quicker as baseline trust in institutions declines. Disinformation just needs to validate suspicions in such circumstances; sophistication is not necessary.

This issue is clearly shown in the literature on electoral governance. According to studies of recent elections in Nigeria, political allegations, legal issues, logistical delays, and ambiguity surrounding the transmission of results all contributed to the development of disinformation campaigns (Yahaya&Chukwuemeka, 2024). Conflicting stories about institutional bias, ethnic targeting, technical sabotage, and rigging frequently spread more quickly than accurate information. This study contends that persistent election mistrust builds up into long-term cognitive fragility, despite the fact that electoral academics typically perceive these dynamics as transient campaign phenomena. Elections are not one-time occurrences. These are frequent occasions when the public's relationship with the state is put to the test. Every opaque communication cycle increases susceptibility to manipulation in the future.

Social annoyance and economic instability are additional problems. Political volatility is frequently linked to unemployment, inflation, inequality, and young exclusion in development literature on Nigeria (World Bank, 2024). However, nothing is known about the relationship between economic stress and cognitive susceptibility. People who are struggling can be more receptive to stories that blame scapegoated groups, offer quick fixes, or depict democratic institutions as fundamentally dishonest. Emotional stress lowers cognitive capacity and makes people more receptive to oversimplified ideas. This study contends that material scarcity and narrative manipulation are mutually reinforcing, despite the fact that existing literature frequently distinguishes between economic governance and information disorder. While disinformation diverts justifiable complaints into channels that are divisive or hostile to institutions, economic dissatisfaction prepares audiences for mobilisation based on rage.

Another significant problem is the demographics of young people. Nigeria has one of the youngest populations in the world, and its citizens use social media and digital devices at high rates. With an emphasis on activism, entrepreneurship, and civic participation, scholars typically hail young connectedness as a democratic potential (Ojebode et al., 2023).

Though limited, this optimism is warranted. Influencer politics, viral outrage cycles, meme-based propaganda, and monetised attention economies are all ways to take advantage of the same demographic dynamic. Younger consumers could be technically proficient but lack institutional trust or media literacy. Previous research has occasionally confused resilience with digital nativity. This study challenges that presumption. Being accustomed to technology does not immediately make one immune to manipulative behaviour. Constant connectedness may sometimes increase emotional contagion and exposure.

Another important aspect of vulnerability is platform dynamics. Platforms like WhatsApp, Facebook, X, TikTok, and YouTube are structured environments with algorithms that prioritise interaction, speed, and emotional response, as the prevailing research increasingly acknowledges (Bennett & Livingston, 2023). Because they function through reputable social networks of family, religious organisations, professional circles, and community associations, encrypted messaging platforms are particularly powerful in Nigeria. Interpersonal trust is frequently inherited by messages sent over private networks. This sets Nigeria's platform ecology apart from environments where open public feeds predominate. Global literature currently in publication frequently concentrates on public political advertising, bot identification, and Twitter-style visibility. The power of semi-private communication systems, where verification is challenging and forwarding standards are strong, is undervalued by such emphasis. According to this study, Nigeria may be more vulnerable to relationally trusted misinformation spreading under public scrutiny than to overt propaganda.

The emergence of venues for short videos adds to the complication. According to recent research, audiovisual content elicits a stronger emotional response and is more likely to be remembered than text-based claims (Akinwale& Hassan, 2025). With little time for confirmation, viewers' perceptions can be quickly shaped via edited videos, decontextualised talks, fake subtitles, and symbolic imagery. While acknowledging virality, current platform studies frequently overlook linguistic variety. Nigeria's multilingualism makes it possible to adapt stories into regional slang, idioms, and culturally significant symbols, which makes manipulation more personal and convincing. This study makes the case that language localisation greatly enhances cognitive effect and ought to be a major focus of further studies on platform vulnerability.

The literature also frequently addresses the function of religious networks and traditional authority. Clergy, community leaders, and cultural authority are among the powerful influence structures that Nigerian society still has outside of official governmental organisations. According to some academics, these players are stabilising middlemen who can use moral legitimacy to refute false information (Mustapha, 2023). Others point out that when leaders become political or lack appropriate knowledge, these networks can likewise magnify divisive notions. Previous research frequently depicts traditional actors as either threats or protectors. This study takes a more dependent stance. Their influence is influenced by media literacy, incentive systems, and the legitimacy of the state. They can improve resilience when incorporated into reliable municipal communication systems. They can exacerbate divisiveness when they become politicised.

Another understudied topic is communication in the security sector. Research on Nigeria's police and military establishments usually emphasises operational capability above narrative credibility. However, rumours and hostile narratives might fill the void left by delayed pronouncements, inconsistent casualty reports, and unclear investigations during times of crisis (Okoli&Olayoku, 2024). Capacity limitations are mentioned in certain publications, whereas secrecy culture is blamed in others. Both explanations are true, but they fall short. This paper makes the case that crisis communication should not be viewed as a public relations afterthought, but rather as a fundamental security capacity. Silence and inconsistency are not neutral in the human realm; rather, they are calculated compromises to manipulators.

The topic of diaspora and transnational story flows is also brought up in the literature. Nigerian politics are being discussed more and more on international digital networks, where advocacy organisations, expatriate communities, foreign media, and transnational influencers take part in local discussions. According to academics, diaspora participation can encourage democratic pressure and accountability (Nwankpa, 2024). Distance, however, can sometimes promote emotionally charged perceptions that are unconstrained by local verification. Studies that have already been done praise digital transnationalism but don't go far enough in examining how external narrative nodes can exacerbate polarisation. According to this study, diaspora communication is neither intrinsically good nor bad. When emotional unity surpasses factual discipline, it becomes fragile.

The insufficiency of regulatory responses is another problem. Nigerian policy discussions frequently vacillate between demands for unrestrained expression and requests for more stringent content restriction. Legal experts caution that badly crafted anti-disinformation legislation puts journalists and opposition figures at risk of abuse (Ezeani, 2025). It's crucial to use cautious. Laissez-faire methods, however, overlook the extent of coordinated manipulation. All too frequently, the literature that is currently available creates a false dichotomy between freedom and censorship. This study rejects that dichotomy and advocates for a governance paradigm based on civic education, independent oversight, platform transparency requirements, targeted disruption of coordinated inauthentic activity, and due process protections.

The body of research indicates that disinformation is not the only factor contributing to Nigeria's vulnerability in the human realm. Politicised identities, unresolved historical memory, institutional mistrust, economic stress, young exposure, relational platform systems, communication gaps, and regulatory ambiguity all come together to make it. While many earlier studies accurately identify individual components, they hardly ever theorise how they combine. The argument put out in this study is that these factors produce a compound vulnerability structure where each weakness intensifies the others. Rumours gain credibility when there is mistrust. They become flammable due to identity cleavages. They are scalable due to platform incentives. They are emotionally appealing due to their economic dissatisfaction. Correction is challenging when institutions are weak.

Because of this, fact-checking initiatives and episodic platform bans are insufficient to protect Nigeria's human domain. Rebuilding institutional credibility, bolstering inclusive civic

identity, enhancing crisis communication, funding media literacy, encouraging economic inclusion, and creating platform accountability appropriate for regional communication cultures are all necessary. The lack of an integrated resilience framework based on Nigeria's unique sociopolitical realities is the main gap in the literature. This study aims to close that gap by redefining vulnerability as the interplay between unsolved structural deficiencies in society and digital manipulation rather than just technological weakness.

Evaluation of Nigeria's Current Legal and Institutional Responses to Misinformation and Cyber Threats

A policy framework marked by slow legal growth, growing institutional mandates, and ongoing implementation flaws is revealed by the literature on Nigeria's responses to disinformation and cyber threats. Although Nigeria has passed a number of laws and set up organisations to control digital communication, cybercrime, and national information security, academic evaluations increasingly indicate that the nation's response architecture is still reactive rather than proactive. The strategic logic of modern cognitive threats necessitates preventive resilience, quick coordination, and public legitimacy, but current approaches frequently handle apparent occurrences after they happen. Although a large portion of the literature acknowledges this divide, it usually addresses legal and institutional issues independently. This paper contends that Nigeria's problem is the lack of an integrated governance ecosystem that can protect the human domain while upholding democratic freedoms, rather than just inadequate legislation or weak institutions in isolation.

The suitability of Nigeria's legal structure for cyberthreats is one of the most often debated topics. In academic debates on digital security, the Cybercrimes (Prohibition, Prevention, etc.) Act continues to be the most frequently cited legislative tool. Because the law made crimes including identity theft, illegal access, online fraud, cyberstalking, and meddling with vital systems illegal, researchers agree that it was a major turning point (Oluwatobi&Eze, 2024). Additionally, it established a foundation for digital evidence procedures and interagency collaboration. More recent research, however, raises concerns about whether a legislation largely focused on cybercrime is adequately prepared for more contemporary dangers like algorithmic manipulation, coordinated influence operations, AI-generated deceit, and synthetic media. Because cognitive warfare usually targets perception rather than infrastructure, this objection is compelling. While public trust is purposefully undermined, a system may nonetheless be technically secure. Therefore, this study argues that while current concerns increasingly encompass behavioural impact and information integrity, Nigeria's legal framework still represents an earlier generation of threats focused on intrusion and fraud.

This is closely related to the contentious topic of false information provisions and cyberstalking. Due to its potential for abuse against journalists, activists, critics, and opposition voices, statutory provisions pertaining to abusive or fraudulent online communication have caused ongoing concern, according to a number of academics (Ezeani, 2025). Concerns have been voiced by courts and members of civil society that ambiguous language may allow for discretionary enforcement. The conflict between preventing damaging lies and defending constitutional freedom is accurately noted in existing literature. However, a lot of research presents the problem as a dichotomous struggle between liberty and regulation. That limited framing is rejected in

this investigation. Legal accuracy, procedural protections, and institutional independence are the true obstacles. Nigeria suffers from unclear legislation and unequal enforcement, which can erode public confidence, rather than from the presence of regulations. Even well-meaning anti-misinformation legislation may lose credibility in settings with poor institutional legitimacy if they are seen as tools of political control.

The function of industry regulators, in particular the Nigerian Communications Commission and the National Information Technology Development Agency, is another important problem. Because these organisations oversee data ecosystems, digital policy, telecommunications standards, and cyber resilience, scholars widely acknowledge them as essential to Nigeria's digital governance (Adebayo & Musa, 2024). Their actions have enhanced cyber risk awareness, licensing policies, and sector collaboration. Nonetheless, a growing body of research notes that telecom regulatory strength has not always equated to cognitive security readiness. Coordinated misinformation, bot activity, platform opacity, and behavioural targeting cannot be addressed by technical network, bandwidth, and compliance regulations alone. Therefore, this study contends that while strategic information integrity receives somewhat less systematic attention, Nigeria's institutional architecture is nevertheless technically orientated. There has also been a lot of scholarly interest in the creation of the National Cybersecurity Policy and Strategy. The policy is praised by analysts for fostering whole-of-government initiatives and acknowledging cyber security as a national development and security priority (Federal Republic of Nigeria, 2021). It covers international cooperation, essential infrastructure, incident response, and capacity building. However, recent scholarly criticisms indicate that funding constraints, disjointed mandates, a lack of specialised staff, and low public awareness continue to hinder implementation (Adeyemi&Okonkwo, 2025).

Previous research frequently views implementation limitations as regular administrative issues. This study takes a more critical stance, contending that strategic signalling costs result from cyber governance implementation failure. While citizens may see persistent digital disorder as proof of institutional weakness, adversaries may assume inadequate state readiness when rules are mostly on paper. When considered collectively, the literature shows that Nigeria has not been idle. There are laws, agencies function, strategies have been released, and collaborations are still growing. Coherence, however, is the more fundamental issue. Some legal tools are still based on outdated theories of cybercrime. There are several institutional mandates. The legitimacy of enforcement is disputed. The governance of the platform is lacking. Initiatives for public literacy are inconsistent. The advancement of technology is outpaced by judicial procedures. Current research frequently assesses each domain independently, ignoring how they connect. This paper contends that in the absence of a cohesive theory linking law, technology, communication, intelligence, and civil liberties, dispersed competence might nevertheless result in collective weakness.

The lack of a human domain-centered paradigm for assessing responses is the fundamental gap in the literature. The majority of research questions Nigeria's ability to safeguard networks, control platforms, and punish violators. Fewer enquire as to whether the existing solutions enhance story credibility, lessen incentives for manipulation, restore trust,

and bolster democratic resilience. Thus, these papers promotes the idea that effective responses to disinformation and cyberthreats should be evaluated not only by arrests, laws, or shutdown capabilities, but also by institutions' capacity to maintain credibility under duress, communicate openly, coordinate quickly, and defend rights while thwarting organised deception. In this way, Nigeria's problem goes beyond just controlling the internet. Its purpose is to regulate thought within the bounds of the constitution. This necessitates shifting from suspicion-based control to trust-based legitimacy, from fragmented mandates to coordinated strategy, and from reactive enforcement to anticipatory resilience.

Practical Framework for Defending Nigeria through Strategic Communication, AI Detection Systems, Interagency Coordination, Digital Literacy, and Civic Resilience

States can no longer rely solely on censorship, episodic law enforcement, or technical cyber security, according to the expanding body of research on responses to cognitive warfare. Threats to meaning, trust, identity, and behaviour now necessitate multifaceted frameworks that integrate social resilience, technological prowess, and governance legitimacy. This problem is especially severe in Nigeria because politicised identities, disjointed institutions, low confidence in official communications, unequal digital literacy, and quickly changing platform ecosystems all contribute to vulnerabilities. Many of these components have been studied independently in previous research, but there is still little integration of how they may be put together into a cohesive national defence model. This section makes the case that protecting Nigeria's human domain necessitates a multi-layered architecture based on institutional coordination, digital literacy, AI-assisted detection, strategic communication, and civic resilience that function as interdependent systems rather than discrete actions.

Strategic communication as the first line of defence is a major topic in the literature. Misinformation thrives in places where authoritative institutions communicate slowly, inconsistently, or without credibility, according to security and governance specialists. Rumours, political assertions, or emotionally compelling stories are frequently used by citizens to fill up information gaps during times of crisis (Yahaya&Chukwuemeka, 2024). Strategic communication is often defined narrowly in existing research as media messaging, branding, or public relations. For modern cognitive threats, such interpretations are inadequate. According to this study, strategic communication should be viewed as a governance competence based on institutional trustworthiness, accuracy, speed, coherence, and empathy. The issue in Nigeria is not only those agencies don't communicate enough, but that communication frequently happens after narratives have solidified. Later factual correction has little impact after mistrust is ingrained in society.

As a result, the reactive focus of the literature needs to be changed to anticipatory communication that provides information before conjecture closes the gap. This view is supported by relevant research on crisis communication. According to studies, reputable organisations preserve their credibility in times of crisis by providing frequent updates, admitting uncertainty, fixing errors openly, and speaking in a language that the public can comprehend (Reynolds & Seeger, 2023). However, rather than coming from contentious political circumstances, a large portion of this literature

comes from public health and disaster settings. Nigeria faces a different problem since some audiences may interpret official communications through regional, ethnic, or party filters. This implies that confidence may not be guaranteed by accuracy alone. Therefore, rather than depending only on central state broadcasting, this research contends that strategic communication in Nigeria needs to be decentralised and relational, encompassing local authorities, community influencers, civil society networks, and multilingual media.

AI detection systems as instruments for spotting coordinated deceit, deepfakes, bot networks, and altered material represent another significant problem. Rapid advancements in machine learning algorithms that can identify unusual posting behaviour, synthetic imagery, coordinated amplification, and sentiment manipulation have been documented by international academia (Chesney & Citron, 2024). These technologies are useful because they can handle data volumes that are too large for human monitoring to handle. However, detecting systems are frequently treated as technologically neutral solutions in the literature now under publication. This is a faulty assumption. The training data, language sensitivity, and institutional deployment environment of detection tools determine how effective they are. The performance of imported models that were predominantly trained on Western datasets may be diminished by Nigeria's multilingual environment, code switching patterns, vernacular language, and regionally imbedded symbols. Thus, this study argues that local adaptation is necessary for AI defence systems. Automated systems may overflag acceptable speech while missing hazardous narratives if they are not contextually calibrated.

Concerns like algorithmic bias, privacy, and false positives are also brought up in the research. According to some academics, automated monitoring could mistakenly label dissent, satire, or minority language expression as dangerous content (Gorwa&Binns, 2024). These cautions are important because mishandled detection technologies have the potential to erode civil freedoms and increase mistrust. This is frequently framed in current discussions as a trade-off between privacy and security. This study takes a more sophisticated stance. Institutional design is the true obstacle. Transparent legislative requirements, impartial auditing, judicial protections, and unambiguous appeal procedures should all be in place for AI detection. Legitimacy is just as crucial as technical precision in democracies.

Another persistent problem is interagency coordination. Security agencies, telecommunications regulators, electoral entities, judicial players, intelligence services, and ministries in charge of education and communication are all involved in Nigeria's responses to disinformation and cyber threats. Research consistently points to bureaucratic rivalry, delayed information exchange, and overlapping mandates as barriers to effective response (Adeyemi&Okonkwo, 2025). A large portion of the literature suggests memoranda of understanding, task forces, or collaboration. These suggestions are helpful, but they frequently undervalue the political economy of fragmentation. Agencies vie with one another for authority, fiscal resources, and relevance. Therefore, this study contends that coordination failure is a structural incentive issue rather than merely administrative inefficiencies. Unified doctrine, interoperable systems, collaborative training, and performance metrics that prioritise teamwork over bureaucratic autonomy are all necessary for long-lasting reform.

The body of research indicates that Nigeria's human domain cannot be protected by a single tool. Without trust, strategic communication turns into propaganda. Without accountability, AI detection turns into surveillance. Without incentives, interagency cooperation becomes into symbolism. Without emotional intelligence, digital literacy turns into technocracy. Without governmental competence, civic resilience devolves into romanticism. Previous research frequently gives priority to one tool based on disciplinary preferences. A systems approach, according to which every mechanism depends on every other mechanism, is presented in this study.

Therefore, five interconnected pillars should be part of a workable structure for Nigeria. First, dependable strategic communication built on local partnerships, speed, transparency, and multilingual reach. Second, rights-based oversight of context-sensitive AI detection systems. Third, ongoing interagency cooperation with common operational capabilities and shared doctrine. Fourth, community and educational institutions should incorporate lifelong digital literacy. Fifth, responsive governance, bridge building, and inclusiveness all contribute to increased civic resilience. The lack of such integrated sequencing that is suited to Nigeria's diverse political landscape is the main gap in the body of current research. Therefore, this study suggests that preventing false content is not enough to protect Nigeria from cognitive warfare. It is the more comprehensive effort of making institutions publicly trusted, communities interconnected, truth socially credible, and governance strategically responsive. Even before hostile narratives are officially eliminated, they become less popular in those situations.

Discussion of Findings

The study's conclusions show that cognitive warfare has grown to be a major non-kinetic security threat in Nigeria, fulfilling the first goal, which was to investigate the characteristics and changing aspects of cognitive warfare. According to the study, rather than focusing only on physical territory, modern warfare increasingly targets perceptions, emotions, trust systems, and collective behaviour. Hostile actors can influence citizens' perceptions of national reality and political events through algorithmic amplification, coordinated false narratives, artificial intelligence-enabled deceit, and synthetic media. This demonstrates that in today's security fight, the human domain has evolved into a strategic battlefield.

Regarding the second goal, the study discovered that Nigeria is vulnerable to cognitive threats due to unique structural vulnerabilities. Manipulation is made easier by identity politics, ethnoreligious divisions, historical grievances, youth unemployment, inadequate institutional credibility, and unequal digital literacy. Because they appeal to preexisting mistrust and societal concerns, these vulnerabilities allow misleading narratives to proliferate quickly. According to the report, Nigeria's biggest vulnerability is not just its lack of technology but also its unresolved sociopolitical divisions, which adversaries might take advantage of.

The results show that Nigeria's current institutional and legal solutions are still mostly reactive and dispersed. AI-driven perception management and industrial disinformation are not adequately addressed by current laws and authorities, despite advancements in cybercrime control and digital governance. In contrast to prevention, resilience building, and trust

restoration, regulatory solutions frequently concentrate on punishment after harm has been done. This suggests that the current approach is less appropriate for modern cognitive warfare and more appropriate for older cyberthreats.

According to the study, artificial intelligence dramatically increases manipulation by improving precision targeting and reducing the cost of deceit. Mass content creation, deepfakes, behavioural profiling, automated bot activity, and quick story modification to regional languages and emotions are all made possible by AI technologies. These tools can amplify anti-institutional narratives, communal conflicts, and electoral misinformation in Nigeria, where digital verification procedures are still inadequate. As a result, AI amplifies preexisting vulnerabilities.

According to the study, protecting Nigeria's human domain calls for a multifaceted strategy as opposed to discrete measures. Strategic communication centred on speed and credibility, locally tailored AI detection systems, robust interagency coordination, digital literacy initiatives, community involvement, and more extensive governance reforms that restore public confidence are all necessary for an effective response. Because societies with better networks of trust are less susceptible to manipulation, civic resilience was found to be particularly significant.

The results provide compelling evidence for the use of securitisation theory. Threats to democratic legitimacy, trust, and cognition are now legitimate security issues, according to the report. However, this study discovered that securitising manipulative processes rather than populations is more appropriate, in contrast to traditional securitisation, which frequently justifies enormous state authority. Democratic trust, citizen autonomy, electoral credibility, and social cohesiveness should all be considered the reference object of security. In this way, the idea is expanded to include threats to the digital psychological realm in addition to physical and territorial ones. Overall, the study suggests that safeguarding minds, trust, and democratic consciousness would be just as important to Nigeria's security future as preserving infrastructure and borders. Thus, in the twenty-first century, cognitive resilience is just as crucial as military preparedness.

Conclusions and Policy Recommendations

This study comes to the conclusion that because cognitive warfare manipulates perception, trust, identity, and behaviour, it poses one of the biggest new risks to Nigeria's national security. AI-driven disinformation and coordinated influence operations undermine democratic legitimacy, social cohesiveness, and institutional confidence from within, in contrast to traditional threats that target infrastructure or territory. Identity politics, poor governance, unequal digital literacy, and disjointed institutional solutions all exacerbate Nigeria's vulnerabilities.

The results support the applicability of Securitisation Theory as the study's analytical framework. According to the notion, when dangers are identified through institutional and political processes, they become security priorities. The study shows that, in the Nigerian context, cognitive manipulation should be securitised by safeguarding democratic trust, citizen autonomy, electoral credibility, and national cohesion rather than by suppressing speech or controlling citizens. This expands the theory to include the digital psychological domain of contemporary conflict in addition to conventional physical dangers.

These results lead to a number of policy recommendations. Nigeria should create a national cognitive security plan that incorporates democratic resilience, cyber security, and strategic communication. To avoid information gaps during emergencies, government agencies should enhance open and quick public communication. AI-based detection systems ought to be implemented with independent monitoring, local language adaption, and unambiguous legal protections. Through long-term cooperative procedures, interagency coordination between security services, regulators, electoral bodies, and civil society should be institutionalised. To improve critical thinking and resistance to manipulation, digital literacy should be included into educational institutions, community organisations, and schools. Finally, since reliable institutions continue to be the best line of defence against misinformation, more comprehensive governance reforms that enhance accountability, inclusivity, and service delivery are crucial. In conclusion, Nigeria cannot fight future challenges by relying just on military might or legal sanctions. One of the main tenets of national security policy must be the defence of minds, trust, and democratic consciousness.

References

Adebayo, S., & Musa, H. (2024).Telecommunications regulation and digital governance in Nigeria.*Journal of African Technology Policy, 10*(2), 61–89.

Adeosun, K., &Nwangwu, C. (2025). Governance legitimacy and citizen trust in contemporary Nigeria. *African Journal of Political Studies, 18*(1), 55–79.

Adeyemi, T., &Okonkwo, J. (2025).Digital governance and cyber institutional coordination in Nigeria.*African Journal of Governance Studies, 12*(1), 44–67.

Akinwale, T., & Hassan, M. (2025).Short video politics and digital persuasion in West Africa.*Journal of Media and Democracy, 11*(2), 101–126.

Akinyemi, R., &Durojaiye, P. (2024).International cooperation and cyber security capacity in West Africa.*African Security Review, 33*(1), 22–46.

Bamidele, O. (2025). National security framing and digital regulation in Nigeria.*Journal of Strategic African Studies, 7*(1), 101–129.

Bennett, W. L., & Livingston, S. (2023). *The disinformation age: Politics, technology, and disruptive communication*. Cambridge University Press.

Bradshaw, S., & Howard, P. N. (2023).*Computational propaganda and the manipulation of public opinion*. Oxford Internet Institute.

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

Chesney, R., & Citron, D. (2024).Deepfakes and the future of truth in democratic societies.*Journal of Information Policy, 14*(2), 77–101.

Claverie, B., & du Cluzel, F. (2020).*Cognitive warfare: The future of cognitive dominance*. NATO Innovation Hub.

European Union Agency for Cybersecurity.(2024). *Whole of society resilience against hybrid threats*.ENISA.

Ezeani, E. (2025). Regulating false information in fragile democracies: Lessons from Nigeria.*International Review of Law and Society, 9*(1), 33–58.

Ezeani, E. (2025). Regulating false information in fragile democracies: Lessons from Nigeria.

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

Freedom House. (2024). *Freedom on the net 2024: The struggle for trust online*. Freedom House.

Gorwa, R., &Binns, R. (2024).Algorithmic moderation, fairness, and democratic accountability.*New Media & Society, 26*(2), 401–423.

Graves, L., & Cherubini, F. (2024).Fact checking, journalism, and public trust in the platform era.*Digital Journalism, 12*(1), 1–22.

Ibrahim, M., &Aduloju, K. (2024).Social media misinformation and electoral behaviour in Nigeria.*Journal of African Political Communication, 9*(2), 88–110.

Jowett, G. S., & O'Donnell, V. (2022).*Propaganda and persuasion* (7th ed.). Sage.

Kello, L. (2022). *The virtual weapon and international order*.Yale University Press.

Mustapha, A. R. (2023). Religious authority and political communication in Nigeria.*African Affairs Review, 17*(3), 210–234.

NATO Innovation Hub. (2021). *Countering cognitive warfare: Awareness and resilience*. NATO.

Nwachukwu, P., &Salisu, A. (2024).Interagency coordination and cyber crisis response in Nigeria.*Public Administration and Security Journal, 14*(3), 90–118.

Nwankpa, M. (2024).Diaspora activism and digital politics in Nigeria.*Journal of Transnational African Studies, 6*(2), 74–98.

Ojebode, A., Aiyede, E., &Salawu, A. (2023).Youth citizenship and digital participation in Nigeria.*Information, Communication & Society, 26*(9), 1821–1840.

Okafor, J., & James, T. (2025).Digital evidence and cybercrime adjudication in Nigeria.*Nigerian Law and Technology Review, 6*(2), 55–84.

Okoli, A., &Olayoku, P. (2024).Security communication and public trust during crises in Nigeria.*Conflict Trends in Africa, 8*(1), 14–39.

Oluwatobi, K., &Eze, C. (2024). Assessing the Cybercrimes Act and emerging digital threats in Nigeria. *Journal of Cyber Law in Africa, 8*(1), 14–39.

Osaghae, E. E. (2022). Historical memory, identity conflict, and nation building in Nigeria.*Nigerian Journal of Social Theory, 15*(4), 1–24.

Pennycook, G., & Rand, D. G. (2023).The psychology of misinformation and interventions to reduce it.*Nature Reviews Psychology, 2*(3), 162–175.

Reynolds, B., & Seeger, M. W. (2023). Crisis communication and public trust in complex emergencies. *Journal of Risk Research, 26*(4), 355–372.

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.

Suberu, R. T. (2023). Federalism, identity politics, and democratic contestation in Nigeria.*Journal of Modern African Governance, 12*(2), 65–92.

Tucker, J. A., Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., &Nyhan, B. (2023). Social media, political polarization, and democratic vulnerability.*Annual Review of Political Science, 26*, 347–369.

UNESCO.(2023). *Media and information literacy for resilient societies*.UNESCO Publishing.

World Bank. (2024). *Nigeria development update: Building trust amid economic transition*. World Bank.

Yahaya, M., &Chukwuemeka, R. (2024).Electoral misinformation and institutional credibility in Nigeria.*Journal of Democratic Governance in Africa, 11*(2), 72–99.