IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

NEW MEDIA, DIGITAL PROPAGANDA, AND THE RECONFIGURATION OF NATIONAL SECURITY DISCOURSE IN NIGERIA

IBORIDA, EMMANUEL
Department of Mass Communication, Caleb University , Imota, Lagos State

Solomon Abiodun Oyeleye (PhD)
Department of Mass Communication, Caleb University, Imota, Lagos State

Abstract

The rapid expansion of new media has transformed how national security information is produced, circulated and interpreted. In Nigeria, where terrorism, banditry, kidnapping, separatist agitation, communal conflict and political tension remain pressing concerns, social media has become a powerful arena for conveying, contesting and distorting security narratives. Unlike the traditional media environment, in which professional journalists and state institutions largely controlled security information, today's digital landscape enables government, security agencies, journalists, political actors, insurgents, activists and citizens to construct these narratives simultaneously. This paper conceptually examines the relationship between new media, digital propaganda and the reconfiguration of national security discourse in Nigeria. It argues that digital platforms have democratized security communication while simultaneously opening channels for misinformation, disinformation, algorithmic amplification and emotional manipulation of official narratives, and that national security in the digital age extends beyond physical territory to the integrity of the national information environment. Drawing on Nigerian and international scholarship published between 2016 and 2026, the paper examines how social media has reshaped agenda-setting, framing, gatekeeping and public reception of issues including terrorism, banditry, elections, protest movements and separatist agitation.

It concludes that although new media have expanded access to security information and broadened participation, their vulnerability to propaganda and distorted content threatens social cohesion, public trust and effective security governance. The paper recommends strengthened strategic communication, digital and media literacy, professional verification mechanisms, institutional transparency, platform accountability and rights-respecting regulation to build a resilient national information environment.

Keywords: New media, digital propaganda, national security, social media, disinformation, security discourse, Nigeria

1.0 Introduction

How information control impacts national security The historical relationship between media and national security has always revolved around the ability of communication institutions to shape what people know about the threat to the nation, how they think about that threat, and how governments and security authorities are held accountable in response. In traditional mass communication, television, radio, and newspapers, through their gatekeeping functions, held enormous power. In mass media systems, professional institutions largely determined what security stories were covered and how they were told. New media and their recent rapid reach across Nigeria have destabilized this communication structure. Information about national security is circulating in a decentralized, interactive, and increasingly contested arena, in which blogs, instant messaging platforms, social-media networks, online news sites, video-streaming platforms, and other digitally distributed communication systems are present. In Nigeria, this development is deeply significant. Nigeria faces a convergence of threats to its security, including terrorism, kidnapping, violent extremism, and community conflicts, among others. These challenges have physical, discursive, and communicative dimensions.

Images and reports of security incidents are disseminated instantly, often within minutes, creating many competing versions of security events for citizens. Citizens no longer rely solely on security organizations, state news media, or their own reports on insecurity in their locality. Activists, eye-witnesses, bloggers, diasporans, and anonymous social-media accounts now compete to define security events for citizens. New media are not simply additional mediums through which existing security messages are transmitted.

These have produced a changed communication and discourse about security, where more and more actors have the authority to define such a context (Howard et al., 2023; Luczak-Roesch & Johnstone, 2025). This is because digitally disseminated communication can be manipulated more rapidly, anonymously, and precisely, and on a larger scale with more interaction than ever before. Automated accounts, organized networks, algorithm-recommendations, micro-targeting, and recently developed AI are a powerful arsenal for any political/strategist aiming to manage public perceptions towards security and beyond.

Government control of communication is therefore no longer just between governments and professional news media outlets alone. Because numerous actors can produce conflicting representations for security incidents using new media. Government may present a security incident as a security mission, a perfectly secured operation, whereas an eyewitness could send another representation illustrating a differently; an political opponent could label security operation a failure, whilst activists frame such as human rights violations and so on. So, many conflicting and competing explanations on just the one incident. Nigeria case-study illustrates what impact new media had on the public communication environment in regard to state's securities. A case in point is the work by Igwebuike and Chimuanya (2021), it was established how WhatsApp, Facebook and Twitter were used in propagating fake and deceitful political information in regard to elections 2019 general elections in Nigeria. This study is meaningful and relevant to security discussion as in Nigeria politics, election and security are frequently interlinked with factors including ethnography, regionalism and religions. In effect, the capacity of such falsehood is not to mislead electorates to choose particular options, but rather to shape views about political institutions, communities, and the nation as a whole.

Recent evidence from Nigeria suggests that the proliferation of online fake and false news is woven into the overall digital communication ecology. A study by Ogbodo et al. (2026) on the users encounter with online disinformation revealed the ways in which citizens comprehend and respond to false and misleading news in Nigeria's online space. Similarly, Lawal (2025) pointed to the implications of AI and social media fake news on Nigerian public and national security.

All these suggests that information disorder may be more than just a peripheral aspect to governance and its role in the life of a state. ' The rise of digital propaganda makes this more complicated as a contemporary communication mechanism that no longer has to originate from organized state communication structures to exert influence. Instead, digitally communicated propaganda increasingly has dispersed networked properties wherein numerous producers of information reproduce, modify, and amplify certain ideas/messages. Scholars

have recently used concepts of computational propaganda to understand communications between political elites, digital platforms, data, automation, users, and algorithms (Howard et al. 2023; Luczak-Roesch & Johnstone, 2025). International scholars view digital propaganda in terms of its evolving and interdependent dynamics, whereas others have demonstrated that some state propagandas may span across several media platforms simultaneously (DiResta & Goldstein, 2025). In a networked society, the boundaries between propagators and audiences are blurring as citizens play multiple roles: consumers and distributors of information. This has serious implications for societies with deeply divided public spheres, such as those with a high degree of political polarization, institutional distrust, and ethnoreligious sensitivity.

Most digital propagations exploit societal divisions rather than forging entirely new ones. Hence, a misreported account of a violence incident, election, or government operation has a high likelihood of being interpreted along established political, racial, or religious fault lines by members of the public. In addition, many digital media are not neutral avenues through which these messages are conveyed. Instead, their technological architecture impacts visibility. Algorithme-driven media tend to rank content based on criteria such as engagement levels and relevancy, as well as user behaviors; hence, emotional and sensational security issues often generate high interaction levels, which gives them greater visibility. Research on how digital platforms and algorithms work has increasingly identified how technological structures (platform design, algorithms, and automated actions) reinforce this phenomenon. This shift challenges us to consider the context in which the communication happened rather than purely the content delivered and the intent of the sender of the message alone to analyze these security contents. In addition, fundamental questions are being addressed regarding the notion of national security, as traditionally national security was notioned on the bases of military prowess, sovereignty, protection from internal/external aggression, etc.

However, in modern thinking, the range of securities has broadened to include political, social, cyber, and human security. Information (dis)order increasingly became a dimension of national security, not least because of the political impact of distorted reality on an audience, which may include distrust in security agencies, animosity among ethnic groups, citizen panic, devaluation of political organizations, or disruption of relief efforts during disasters. Nigeria's digital public sphere has been noted to have these two opposing characteristics of new media. In a way, social media assist with the rapid distribution of news alerts, documentation of abuses, and mobilization of assistance to victims of disaster and security agents' maltreatment, which contributes to better democratic accountability since governments cannot solely 'manage' information regarding national security performance. However, social media equally contributes to the acceleration of rumors, false images, distorted visuals, and sensationalized messages, which political propagandists can easily exploit. For example, a study examined the role of social media during Nigeria's 2020 #EndSARS protests and concluded that social media promoted not only citizen organization and accountability but also provided a ground where false reports and grievances related to security could rapidly spread and multiply. The tension presented by the capacity of digital technologies to enhance or compromise the safety of the public, security integrity, and democratic rights represents one of the most significant dilemmas concerning public communication on national security in present-day Nigeria. Although it is seen as a means to prevent government restrictions, the digital space also presents security challenges due to its open and unregulated nature, whereby malicious actors, such as extremist groups, criminal organizations, and political propaganda, take advantage of the opportunity to spread false rumors and propaganda.

The issue now is not only whether and to what extent to control new media but also how Nigeria can promote a functional information environment that respects democratic freedoms and human rights without suppressing media reportage, criticism of government, or restricting democratic access to information. Another issue, important in this connection, is public trust, as no national security communication would be convincing without trust. People's willingness to believe is critically impacted by the level of their trust towards the government and security institution/agents. Conversely, if authorities present their security reports accurately, transparently, and timely, it might restrict the space for the prevalence of rumors and propaganda.

Thus, security organizations must not only work towards unmasking deceptive messages but also create a trustworthy environment that makes propaganda unsuccessful. The advancement of artificial intelligence (AI) has added other concerns to this aspect of security; the technology can lower the technical know-how needed to create and disseminate text, visual representation, or voice to look like real, thus creating deceptive and sophisticated propaganda. Lawal (2025) mentions AI as a component of modern false and deceptive messages targeting Nigeria's public safety and national security. At this age, it should be a primary concern of citizens and officials not only to check whether messages are true but also how realistic they look or are presented. In light of all these, the paper argues that the emergence of new media has dramatically reconfigured the dynamics of national security discourse in Nigeria; decentralized the authority on security matters; debilitated the structures of traditional gatekeeping; and created a highly competitive new media ecosystem where government agencies, independent news organizations, citizens, political actors, and propagandists compete in constructing security reality. The key argument here is that digital propaganda takes full advantage of the participation of new media, their networks, and algorithm-driven technologies to shape the perspectives of threat actors, institutions, and events. The paper discusses new media and digitally propagated information as key sites of contestation that reshape how national security has conceptualized, produced, and disseminated in Nigeria, not simply as neutral technological tools. It examines the power relations within such context, interplay of mis/disinformation with security discourse, and how citizens and institutions may address the challenges posed by new and digital propaganda without compromising freedom of communication. In final term, the paper believes that the security of a nation can no longer be ensured solely through the means of armed forces, police, or intelligence agencies. The resilience and integrity of the country's national informational integrity, just like its traditional military and police forces, is a critical and increasingly significant component to protecting national security in what seems to become a wired network society.

2.0 Literature Review

The rise of new media has considerably reshaped the linkages between communication, power, and national security. While communication has historically been integral to forging national identity and political legitimacy and informing the public about the risks to national security, digital technologies have increased both the number of actors involved and the rate at which competing security narratives are spread. The current context of national security discourse occurs in a communication ecology characterized by decentralized content creation, networked participation, algorithmic mediation, information glut, and increasing potential for strategic manipulation. Therefore, an analysis of the relationships between new media, digital propaganda, and national security in Nigeria requires an unpacking of key conceptual terminology and an analysis of the convergences between them.

New Media and the Remodeling of the Communication Ecology New media, in a broad sense, refers to digitally enabled and networked communication technologies that enable interactive and instantaneous production, distribution, and consumption of information. Unlike traditional mass media, which tends to be centralized and largely institutionalized, and with professional journalists or editors serving as gatekeepers, new media allow users to act simultaneously as both content producers, communicators, and consumers. Social-media platforms, blogs, podcasts, online newspapers, and instant messaging applications have been seen as key examples of this reshaped communication space. The unique characteristics of new media are not just about digital technology but about interactivity, connectivity, user-generated content, convergence, and network distribution. This digital communication has moved away from the "many to one" or one-to-many relationships typical of mass communication towards networks of multidirectional communication flows, where individuals previously played passive roles as viewers or readers but now play active roles as eyewitnesses, critics, video makers, political organizers, or even participants in public discussions. This transition has significant implications for communication concerning politics and national security. According to Woolley and Howard (2018), social media has drastically changed the way political information is communicated and the infrastructure through which it flows. The implications of this change directly impact the practice of national security practice because of the very nature of security discourse that thrives on information-who produces it, whose narrative becomes dominant, who quickly countered these narratives, and the credibility with which these narratives are perceived by the audience.

In the Nigerian context, the impact of social media has gained momentum as a tool for conflict and security communications. Uwalaka and Nwala (2022) note that social-media platforms enable military establishments to have direct interactions with their stakeholders while bypassing traditional media gatekeepers. This signifies a radical shift in the communication strategies of the security establishment in Nigeria because, a social-media platform can be used for simultaneous communication about a particular security event by the military, other government institutions, citizenry, journalists, and even non-state actors. As such, new media disrupts the traditional hegemony of the security information network; thus, the ability to create, distribute, and disseminate information about a given security scenario by state agents no longer assures them of exclusive claims to defining the security environment; for now, citizens and non-state actors with access to digital technologies can instantly verify, question, or challenge their official security accounts through images, videos, satellite information, testimonies, and other narratives disseminated through social-media platforms. Although the advantage of the proliferation of information is greater transparency of security-related activities, it unfortunately exacerbates the verification process by allowing unsubstantiated claims to compete for legitimacy with professionally verified news. The Nigerian Armed Forces acknowledges this dichotomy in its social-media policy of 2018 by considering social media for psychological warfare, open-source intelligence, counter-narratives, and other operational support functions, whilst simultaneously warning that personnel's communication could be compromised and accessed by adversary to obtain operationally sensitive information that could be used against Nigeria. This means that new media offers both strategic advantages and significant vulnerabilities in the communication landscape of the security forces. Given this, it is crucial to conceptualize Nigeria's security environment as increasingly mediatized and digitally networked; the security forces and institutions now have to manage, not just the physical threat but their narratives, reputations, visibility, and public perceptions in a digital space, at an unprecedented speed and on an amplified scale.

Understanding Propaganda in the Digital Age

Propaganda refers to a systematic and coordinated effort using communication for a range of strategic objectives, typically to influence perceptions, beliefs, or actions to support the aims of the propagandist. Although propaganda is a familiar phenomenon to societies throughout history, technological innovation has transformed the production, distribution, dissemination, amplification and audience targeting of propagandistic content. ' Such propaganda may include truthful information, information that is selectively curated or presented, deliberately misleading information, or outright falsehoods, depending on the goals of the propagandist. The difference between digital and more traditional propaganda is significant. Traditional propaganda was typically communicated through more centralized mass-media systems. Digital propaganda occurs within a more interactive communication system and can be further processed and re-transmitted by those who receive it; it is frequently reproduced and distributed by secondary propagators who may be unaware of its original source and intent. Woolley and Howard describe such technologically-mediated political communication as 'computational propaganda' and emphasize that it is characterized by the use of algorithms, automated accounts (or bots), and human curation of material that deliberately spreads misinformation through social networks. Computational propaganda illustrates that influence operations in the contemporary period are no longer purely rhetorical but are increasingly technological, iterative, and data-driven; digital propaganda is often characterized by the following qualities, which distinguish it from much previous propaganda: speed, scalability, anonymity, microtargeting, interactivity, replicability, and algorithmic amplification. A piece of propaganda can travel across the globe and be reproduced hundreds of thousands of times in mere seconds or minutes, long before traditional sources, such as professional news outlets or public authorities, have had an opportunity to verify or debunk it. This effect is particularly crucial during times of security crises. When information is scarce and the public is concerned about what is happening, compelling but unverified narratives are readily available to fill the vacuum.

Whoever introduces the first credible interpretation of an event will likely frame the public debate, even after evidence contradicting such a narrative has emerged.

Misinformation, Disinformation and Digital Propaganda

However, a conceptual distinction between misinformation, disinformation, and propaganda is important because the terms are related but not the same. Wardle and Derakhshan (2017) distinguish between misinformation and disinformation based on the element of intention. For them, 'Misinformation is false content that spreads between people or within societies, though its creator is not intentionally spreading it. Disinformation is the false content designed with the intention to deceive others and is being strategically produced and shared for some outcome.' They also coined another term: malinformation, which is defined as 'true content that is produced and shared in order to cause harm.

These are useful definitions for unpacking discourses concerning national security. A civilian who inadvertently re-tweets an erroneous alert about an attack might be disseminating misinformation. A malicious actor that intentionally produces exaggerated casualty figures intended to cause widespread public panic and distrust of the security agencies or ethnic tensions is engaged in disinformation. Likewise, an advocacy group that deliberately combines strategically selective facts and emotionally appealing imagery to influence public perception of security is engaged in political propaganda. Thus, digital propaganda is far more complex than fake news. Indeed, propaganda may well be composed of facts that are accurately rendered and presented, it just omits any inconvenient facts from an opposing view, employs sensationalist emotional rhetoric, and persistently stresses and promotes particular views of these 'facts,' while cultivating an adversarial other. Simply equating digital propaganda with factitious inaccuracy risks overlooking its political and ideological character.

This differentiation remains important in the Nigerian context because many political narratives that become entangled with security unfold in contexts that are hotly contested arenas of fact and interpretation, and also involve diverse political interests. Thus, warnings about terrorist incidents, information on military campaigns, reports of communal violence, statements on secessionist movements, and election campaign propaganda may all include factual elements but be deployed strategically for the political purpose of denigrating particular people or political institutions.

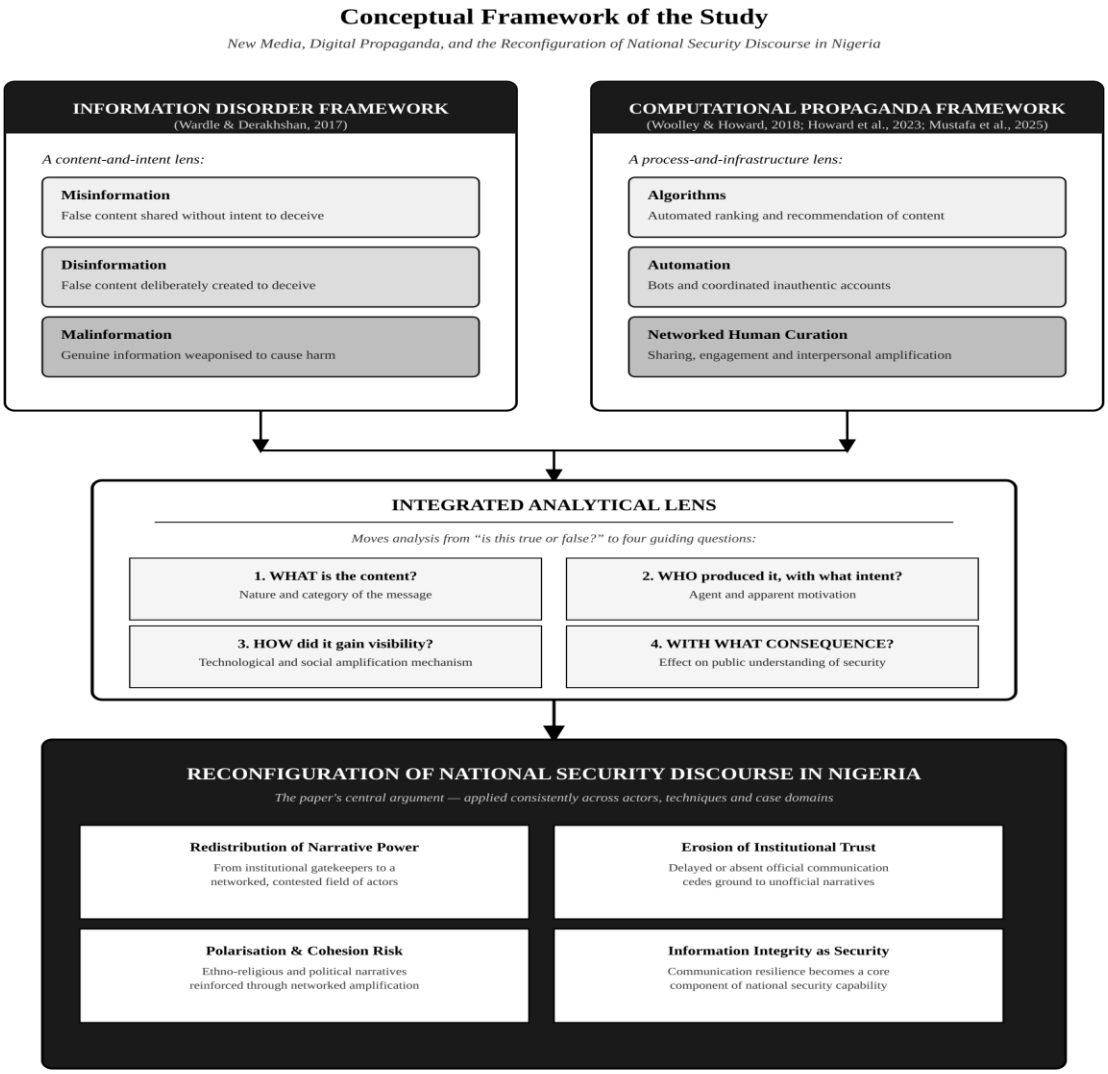

Figure 1. Conceptual Framework of the Study, integrating the Information Disorder Framework and the Computational Propaganda Framework.

Digital Propaganda as a Contest for Narrative Power

Central to the weaponization of digital propaganda is a contest over the narrative power of the nature of our threats. Citizens understand security threats only through our direct experience of them, we understand them through communication. Whether we call an event terrorism, insurgency, banditry, communal riots, separatist movements, riots, or criminal acts has profound political and security implications. Words matter politically and affect security in the ways that government, journalists, activists, and digital communities use them to construct collective meanings. The advent of new media has significantly shifted the distribution of this narrative power. State actors and legacy media organizations previously had considerable control over dominant public narratives around threats. Now, new digital actors are able to compete with government and legacy media in offering immediate counter-narratives, resulting in a world of competing security narratives. Uwalaka's (2023) analysis of Nigerian military communications following the terrorist attack on the Nigerian Defense Academy in Nigeria serves as an example; Uwalaka's study shows that the Nigerian Military was unsuccessful in employing its social media account to push back on the narrative of the online frenzy that followed the attack. The Nigeria Military remained silent in the aftermath of the incident, which contributed to public backlash against the military and government. This does not apply only to the situation analyzed by Uwalaka (2023); in many situations, in the digital space, silence within national security communication can create an absence of official narrative, which creates the space for rumors, speculation, partisanship, and

outright hostile propaganda to fill the void left behind by communication delay. Effective security communications entail the need for national security institutions to invest in communicative capacity, not just physical operational capacity, at the fastest possible rate. This includes speed, reliability, transparency, and engagement with digitally connected publics.

Concept of National Security in the Digital Era

Historically, the focus of national security has been on military and territorial issues. It has been viewed as a state's ability to safeguard its sovereignty, territorial integrity, and political independence from internal and external threats. However, the evolving global environment reveals that military and territorial aspects are insufficient to address the issues of security in the twenty-first century.

Today, national security can be said to entail the relationship between three levels of analysis: military (or strategic); political or state; and non-military (or social). The state may become insecure from threats not only from a conventional military invasion but also from terrorism, organized crime, cyberwarfare, internal destabilization, economic upheavals, manipulation of social groups or ethnic identities, disinformation programmes, and so on. In Nigeria, this book's expanded understanding of security is especially appropriate, having regard to the proliferation of non-military issues that threaten national security, such as insurgency in the North-East, banditry and kidnapping, inter-communal conflicts, long-drawn-out agitations for separation, cybercrimes, electoral, and other election-related tensions, and politically-motivated conflicts. The convergence of all these security problems with digital modes of communication is also very significant because malefactors, victims, security agencies, journalists, and people rely on digital media to convey and share views about them.

Wellington, Adetola and Agbiti-Douglas (2026) observe that the use of social media for national security has some positive and negative implications for Nigeria. On the positive side, digital forums help promote civic engagement and enhance national cohesion. On the negative side, they can serve as mobilizing spaces for instigating social unrest and increased insecurity. Because of this seeming contradiction, one cannot simply dismiss the idea of social media as a danger or an aid to security. In a digital society, therefore, national security should mean the ability of governmental agencies and individuals to continuously access reliable information and to effectively confront a deliberate distortion of reality, engendering mass panic or widening insecurity through the deliberate distortion of social realities. This notion of security is here called information security resilience.

Social Media and Security Communication in Nigeria

Nigeria offers a particularly interesting place to study this process as its security challenges occur alongside widespread digital communication and significant political, ethnic, and religious contestation. Security incidents generate considerable discussion on social media, with users discussing causes, casualties, government culpability, and appropriate responses. The Nigerian military is increasingly using social media for conflict communication, circumventing legacy media to engage directly with the population(Uwalaka and Nwala, 2022).This represents a fundamental shift in the nature of the relationship between traditional media and security. Security forces can now communicate directly with citizens without the mediation of the news media, which previously relied on to disseminate or interpret government statements. However, this does not inherently lend official communications authority. Citizens are able to directly dispute official statements, compare them against other evidence, and circulate alternative narratives almost instantly.

Hence, a new communicative environment is characterized by the constant negotiation of credibility between official narratives and those emerging from unofficial sources. Social media, rumors, and information disorder The greatest security challenge presented by new media is the swift dissemination of unverified information. During a crisis, individuals turn to social media for information, but reliable accounts may initially be sparse, creating fertile conditions for rumors. A large-scale study by Vosoughi, Roy and Aral (2018) on how information spreads on Twitter found that false content spread farther, faster, and deeper than true content. Although the study was not conducted in Nigeria, it provides an interesting perspective on how emotionally

novel, attention-grabbing, or surprising claims, regardless of their truthfulness, are more likely to attain significant online reach before verification efforts can catch up. In Nigeria's multiethnic and multi-religious society, inaccurate accounts of incidents, victims, or perpetrators can potentially exacerbate social tensions. What initially may appear to be an act of criminality, for instance, may be reinterpreted as motivated by ethnic, religious, or political affiliation through social-media framing and subsequent dissemination. Once such associations have been formed, retractions and factual accounts may be insufficient to alter the perceptions. Therefore, misinformation poses a national security risk not merely because of its falsity but because of its consequences for actions, trust, and intra-group relations.

Digital Platforms, Algorithms and the Amplification of Security Narratives

You cannot understand the current information atmosphere only from users. Digital platforms are characterized by technological architectures that define content visibility and circulation. Information encounters are shaped by recommendation algorithms, trending features, and engagement dynamics. Computational propaganda scholarship clearly shows how infrastructures can be deliberately misused. Woolley and Howard (2018) show that political actors in various national contexts utilized communication automation and social media manipulation to shape political discourse. When a certain narrative is artificially amplified, visibility does not always reflect authentic public opinion. This is important for national security issues. A coordinated network can continuously recirculate a certain version of security events and create a sense of social consensus.

Hash tags, misleading videos and response tactics to overwhelm dissenting opinions, can strategically be intensified, leading the visibility to turn to be a means of communicative power. Therefore, it has become increasingly difficult to distinguish genuine opinions from constructed visibility. Politics and national security are closely linked in Nigeria. Political leaders measure the success or failure of their government based on public perception of security performance, while state officials use security arguments to justify their policies. Digital platforms exaggerate this phenomenon by allowing the rapid dissemination of political viewpoints between segments of highly partitioned audiences. Special vulnerable are electoral seasons. Political misinformation campaigns can frame an opposition figure as an antagonist of certain ethnic, religious, or regional communities, thus transforming non-violent political struggles into struggles for the survival of an identified group. When citizens are subjected to security-driven narratives of survival, domination, or marginalization during elections, this propaganda will only increase societal tension.

Digital propaganda has far-reaching impacts, affecting views of state legitimacy, inter-group trust, institutional confidence, and national concord in Nigeria. A key feature of contemporary terrorism is comms. Terrorists aim not only to deliver a physical impact, but also a psychological one, extending far beyond the individual victims. Hence, publicity, fear, and feelings of state vulnerability can be among the strategic impacts they intend to provoke. Digital platforms can multiply these effects. Images of attacks can be instantly disseminated, and feelings of fear can extend well beyond the vicinity of the attack. Extremists may use digital platforms for propaganda, recruitment, ideological proselytization, and intimidation. In response, security institutions use the same technologies, deploying countermeasures, comms, and indigence.

In Nigeria, this is evident in response to counter-insurgency efforts. Sule et al. (2023) note that Nigerian security actors employ strategic communication and a range of non-kinetic measures, including digital engagement, to mitigate the ongoing insurgency. As such, security efforts against terrorism are also a fight for the narrative regarding who appears legitimate and competent between the state and the insurgents.

Digital Propaganda and Public Trust

Trust is a key issue that connects communication with national security. Decisions about whether to heed security alerts, pay attention to instructions, and take government warnings seriously will depend largely on the level of trust citizens place in individual or institutional sources. Low levels of trust in public institutions, for example, may lead citizens to make greater use of unreliable sources to inform their beliefs on issues of security. This can create an environment in which propaganda and rumors flourish alongside verified

information and, at worst, may even cause an 'epistemic crisis," in which citizens become skeptical of all information. In this context, when citizens do not trust institutions such as the media or government, an ineffective response to digital propaganda, according to Uwalaka (2023), the 'lack of institutional response is as dangerous' to society as the propaganda itself. Unsuccessful responses and institutional silence are detrimental to public trust and can have direct security repercussions, as can be seen in the Nigerian military's response to a bombing at the Nigerian Defence Academy (NDA), where they have been heavily criticized and suspected online for their lack of immediate communication. Therefore, the fight against this form of propaganda must focus not on simple deletion but on building stronger institutional credibility through reliable, honest communication at the right time and backed by evidence. Artificial Intelligence, Deepfakes, and Emerging Security Threats With the rise of generative AI, the issue of digital propaganda and national security is entering complex new territories.

These applications of AI can create text, images, audio, and video that are indistinguishable from human-created content, all with minimal effort and cost. Deepfake technology is of particular concern regarding national security because it can easily produce video and audio recordings that appear to capture real events, when in fact they never happened. Videos or audio recordings, for instance, could depict political, military, or public figures making outrageous statements that were never actually made. If disseminated effectively during elections or times of unrest, deepfakes could quickly create confusion before verification can take place. These will also make it harder to claim evidence is real in the face of such realistic synthetic content. New Media, Democratic Accountability, and the Security Dilemma However, while we need to acknowledge the threats posed by digital content, there are real advantages in treating new media not solely as threats. These platforms have empowered citizens by allowing them to report violence, expose injustice, hold power to account, and push back against official disinformation. Citizen-generated evidence can be the only accessible information when formal media channels are either unable to operate at the scene of a conflict. Therefore, the dilemma is to balance two things: the state's legitimate role in responding to information directly linked to violence, terror, or other significant threats, and democratic freedoms such as free speech, journalism, political expression, and the right to hold security agencies accountable. An overbroad view of national security, by focusing too heavily on restrictions, could quickly be turned into suppression of free speech. Conversely, the state's inaction could allow coordinated, harmful information campaigns to manipulate the national information environment. Instead, what is required is a thoughtful blend of transparent strategic communications, media literacy, professional journalism, reliable fact-checking services, accountable platform governance, proportional regulation, and robust protections for lawful expression.

The Emerging Gap in the Literature

Existing literature offers valuable insights into social media, misinformation, computational propaganda, military communications, and national security. There is a rich stream of international literature on computational propaganda, bots, algorithmic amplification, information disorder (Wardle & Derakhshan, 2017; Woolley & Howard, 2018; Vosoughi et al., 2018). Similarly, Nigerian scholarship has started to engage with military social-media communications, strategic communications, and the social-media and security relationship (Uwalaka & Nwala, 2022; Uwalaka, 2023; Sule et al., 2023; Wellington et al., 2026). However, these streams of study often remain insular. The literature on misinformation tends to focus on information accuracy, propaganda on political persuasion, national security on threat perceptions and institutional responses, and social media on technological affordances and citizen participation.

What needs more conceptual examination is how these interact to remold the way that national security is discursively constructed. The core question is no longer whether new media help or hinder national security but who now holds the epistemic authority to construct the realities of national insecurity within a networked digital Nigeria, and by which communication strategies these realities are established, where digital propaganda is crucial for orchestrating political attention around specific constructions of insecurity and for ensuring that certain narrative frameworks gain ascendancy within the public debate.

It is on this conceptual axis that this paper is positioned. Its argument is that new media has reshaped Nigerian national security discourse away from being primarily state-mediated through traditional media into a

consultatory ecosystem of digitally mediated interactions involving the state, security institutions, traditional journalists, political actors, the public, activists, influencers, algorithms, and even malicious digital players. Digital propaganda plays an integral role in this transition, as it allows organized actors to leverage new media's speed, interactivity, emotional content, and architecture to manipulate how insecurity is perceived, interpreted, and debated politically.

From Gatekeeping to Networked Security Discourse: The Reconfiguration of Information Power in Nigeria

One of the many fundamental consequences of new media on the discourse around Nigerian national security is the redistribution of communicative power. In the old days of the mass media, security information generally travelled down an institutional path. Major public sources included government ministries, military and police units, and the intelligence community; media outlets were intermediaries that, in theory, assessed the value of security information for public consumption. The conceptual template (to be supplied below) illustrates the significance of the old order by arguing that a key journalistic function is to monitor government's commitment to security and update the citizen. This has shifted radically with new media. Security information may come from any person using a smartphone device near an event, from a military spokesman, an anonymous source using social media, a journalist, an activist, or an insurgent organization. Different parties could claim authorship of different but similar analyses of the same event. This has moved the process from institutional gatekeeping to networked gatekeeping.

The power has not dissipated. Instead, it has been redistributed among network users, platforms, institutions, and algorithmic agents. While conventional journalists chose which stories would make headlines in papers and bulletins, a digitally networked logic of sharing and connectivity increasingly determines prominence or visibility on social media, facilitated by the spread of recommendations, trending events, and user engagement metrics. This new democratic openness, of course, carries risks because news and views from citizens document ignored stories, provide new accounts to government claims, and challenge security misconduct. However, the challenge the network poses has been documented, especially regarding the role of inaccurate information within a network, by Vosoughi et al. (2018:639) when arguing that "falsehood diffused" News and other information disseminated on Twitter "farther, faster, and more broadly than the truth in all categories of information. Such phenomenon have major implications, when an attack occurs on Nigeria or during inter-communal skirmishes where rumors concerning the perpetrator, the casualty, and motive for violence disseminate before any facts emerged from the media or security apparatus". Now, the key question is, who Controls visibility, Credibility and dominance in the network in?

Digital security narrative? "Digital Propaganda Actor in Nigerian Security Information Environment" The nature of these digital spaces demands that we move away from a monolithic characterization of actors as simply " propagandists" but recognize a number of interacting groups with distinctive aims, strengths, and interests. One category comprises state-actor agencies. Governments have historically conducted campaigns aimed at securing political legitimacy through strategic communications to defend policies and create support for governance. Modern digital technologies afford governments and their institutions to bypass traditional journalistic channels and communicate directly to citizens, often in support of their institutional agenda. Nigeria's various security institutions have social-media presences that they use to announce operations, rebut negative claims, and communicate institutional progress. It has been shown that the communication strategies within Nigerian security forces, including the Nigerian military, have strategically integrated social media into their operations thereby making it indispensable in conflict communication. However, where states communicate with a selective and unbalanced presentation of facts, strategic communications can degenerate into propaganda through the emphasis on success and downplaying of failure or systemic delegitimating of opposition critics.

Another group comprises politicians and activists, as well as political party networks. Increasingly, in Nigeria, political campaigns are routed through a network of politically driven digital supporters and their leaders. Such social media activities promote the election of partisan candidates and shape public perceptions of the

government's effectiveness, as well as views of the security situation. Thus, security events are a useful part of the politics of attacking or defending candidates in Nigeria.

A third category encompasses violent extremist organizations and terrorist groups engaged in waging a war against Nigerian and state power. They employ strategic communications designed to terrorize, recruit, intimidate, gain the legitimization for their ideology, and demonstrate its relevance. This process is amplified by digital media technologies, which extend the potential psychological reach of their attacks beyond local geography. A fourth category is what we call citizen's propagators and influencers, some of whom spread specific, clearly partisan messages, while others passively amplify narratives without realizing their propagandistic nature or impact. This indicates that the audience for propaganda on digital media can be any users, active in reposting, commenting, or forwarding, even without acknowledging propagandistic intent. We need to consider other foreign actors, such as national governments engaged in overseas information operations targeting Nigeria. Similarly, Nigerian diaspora communities and transnational networks may engage in spreading narratives that shape domestic security perceptions and political discourses. In short, the complexity of these networks makes it difficult for observers to know who started what story, its initial motivation, and intent.

Techniques and Instruments of Digital Propaganda

The efficacy of digital propaganda derives not only from the content alone but also from the technical and psychological techniques by which a message may be disseminated. Some of these methods include:

Selective framing: Propaganda does not necessarily have to be untrue. An actor can include particular facts and deliberately omit contextualizing details to create the desired interpretation. For instance, visuals of security casualties can be true, but the description may wrongly assign blame to a location and/or event.

Emotional amplification. It is hardly surprising that security communication revolves around the topics of death, fear, injustice, identity, victimhood, and survival, which lend themselves very well to being used in powerful emotional ways, and that these can work their way into social communication prior to the evidence being checked. 25). Repetition increases familiarity and the likelihood of recall. This becomes more effective in a digital medium as exact replicas and/or subtly altered posts circulate between accounts, as between platforms. Coordinated amplification. This refers to an orchestrated (often automated) activity of either humans or automated systems to artificially amplify one or more messages.

(Woolley & Howard 2018. 36). Hashtags As an aggregation tool, they serve both political and security communication purposes, facilitating mobilization and raising awareness; however, they are also open to co-option as tools for promoting specific narratives or drowning them out. Undisguised de-contextualization of images and videos as much older content will sometimes be repurposed to reflect the 'story' of a present Nigerian security event. Since we tend to trust images/and videos more than written text, the dissemination of such manipulation can cause very strong reactions.

Misinformation, Disinformation and the Construction of Security Threats

The link between information disorder and national security is particularly crucial when misinformation impacts group perception of each other. Using the distinction made by Wardle and Derakhshan (2017), information disorder, as mis-, dis-, and malinformation, is a concept understood along axes of falsity, intention, and potential for harm. For instance, these categories may be useful in structuring the understanding of Nigerian security discourse. For instance, misinformation can arise naturally within security emergencies, with citizens resorting to the sharing of unconfirmed reports by considering them to be authentic and thereby believing them to be factual due to uncertainty and confusion.

However, disinformation can be the result of conscious manipulation, where one individual or organization publishes made-up information on the nature of an attack, governmental process, or plans, specifically to harm the integrity and credibility of the institutions of governance or to fuel animosity towards a group. Again,

malinformation is a different form of information disorder, with the intentional misuse of authentic information, such as the publication of secret documents, photographs of casualties, or personal information of security officials to pose a threat. All the processes that transform mundane events into security events are of grave consequence, especially for a society as complex and heterogeneous as Nigeria, where criminal actions can be readily reconstructed and framed online as ethnic aggression; a conflictual issue can be presented as religious prosecution, and an isolated event can be portrayed as part of systematic political suppression. Digital dissemination works effectively in this environment, as it links the emerging with the established narrative, for ethnic, religious suspicions, political animosities, and historical grievances serve as the frameworks within which such information is injected and interpreted.

Misinformation should not only be analyzed in terms of factual accuracy, but its security implications lie in its capacity to influence public opinion and action. In the context of the battle for narrative supremacy in Nigeria's struggle with terrorism and insurgency, acts of terrorism are arguably a communicative act that goes beyond physical harm to its immediate victims to psychological impact on larger audience, demonstrating power, reinforcing the symbolic capital of violence groups, and challenging the political authority and public perception of power. Nigeria's experiences with the insurgency of Boko Haram and associated terrorist organizations highlights why the management of national security communications is inherently related to controlling the discourse of contest. The struggle to position terrorist organizations as powerful and resistant, while the state endeavors to display control and supremacy over operations, is impacted by digital communication, as it enables the circulation of information about incidents before security institutions can communicate.

The dissemination of photographs, eyewitness accounts, estimations of victims, and speculative analyses can establish an earlier narrative than that provided by official communications. The significance of the application of strategic communication is underscored by Sule et al. (2023), who noted the role of communication alongside other forms of kinetic strategy in Nigeria's anti-insurgency approach, the relevance being that, security bodies need to triumph over violent groups on operational grounds as well as prevent the groups from dictating the interpretation of conflict. The study conducted by Uwalaka (2023) on the aftermath of the attack on the Nigerian Defence Academy provided good evidence on how institutions fail in creating counter narrative, as on social media this included massive amounts of Facebook post and comment that displayed discontent and suspicion of military explanation without effective counter-narrative that effectively addresses the issues thereby leaving institutions to be perceived as insincere and dishonest. It highlights a core lesson in contemporary security discourse that no information vacuum ever lasts, for as soon as it exists, it gets filled.

Ethno-Religious Narratives and National Security

Another prominent aspect of Nigerian national identity is ethnic and religious diversity. Unfortunately, when leveraged as a weapon in the form of propaganda, these can present a national security concern. Security threats, especially, are prone to identity framing, where facts of ethnicity or religion of the culprits used in the narration, transmute criminality of individuals into an existential issue of entire ethnic or Religious group. The violence perpetrated by a few individuals would be represented as proof of animosity of an ethnic or Religious group against another or against the state. Social Media enhances the rapidity of the process because emotions laden with the narratives of ethnic or Religious antagonism can easily circulate through networks built by shared identities (e., Facebook, WhatsApp groups of tribal or religious affiliations) where the stories and information might reach the reader through his religious or community leader, in-laws, etc. Making it appear genuine, and thus amplifying threat perceptions. The threat to National Security, in this context, is when the circulation of stories of antagonism digitally converts emotions from the level of fear to total distrust of the suspected groups.

This can also lead to further social polarization. The security organs of a state need to differentiate real discourse from intentional propaganda targeting a particular ethnic or religious group. Digital propaganda, separatist agitations, and counter-narratives of separatists and self-determination agitations in Nigeria are another domain of national security discourse that digital communications have altered. Social media, as well

as digital technologies, provide a veritable platform for secessionist movements to bypass traditional media and communicate their ideas directly to potential supporters within the country and members of the Nigerian Diaspora. The most noticeable consequence of this is in the area of agenda-setting; issues and campaigns that might not ordinarily receive adequate attention in the traditional media have been amplified online through community participation and transnational connections. This might also fuel separatist agitations if not well managed. Attempts to clamp down on this communication might turn into another round of propaganda battles, as separatist movements might portray any government action to curb them as an attempt to suppress them, while the state might frame similar actions as essential to national unity and the prevention of violence. The fundamental analytical and practical point is that with digital communication, the opposite actors are able to define and conceptualize the same phenomenon in fundamentally different ways; thus, that which the state sees as a threat to national security and which it tries to manage, the activists define it as self-determination and the use of the internet to convey it.

Political propaganda, elections, and national security often provide fertile ground for digital propaganda because of its inherent interaction with identity politics, legitimacy, and power relations of the state. Online misinformation targeting candidates, electoral processes, and authorities, and even ethnic groups, has the capability to influence not only voting choices but also the perceived legitimacy of the entire political system. Igwebuike and Chimuanya (2021) have shown how the circulation of political fake news during Nigeria ’s2019 electoral elections via social media-influences perception and can manipulate through linguistics or discursive devices to make narratives authoritative. The national security implications become especially dire if the electoral propaganda frames political competition as an existential challenge to a particular group: The claims that the victory of one group somehow implies the conquest or annihilation of another exacerbate fear and hostility.

Another aspect of digital electoral disinformation relates to the undermining of confidence in the democratic process, where misinformation can include the premature release of election results, fraudulent documents, or allegations presented without proof. The perceived illegitimacy of democratic institutions can lead to the transformation of politicized disputes into security problems. In short, electoral disinformation can and does have serious national security implications beyond simple politics and influence public confidence, institutional integrity, and social harmony.

.

#EndSARS and the Transformation of Citizen Security Narratives

The 2020 #EndSARS protests serve as an effective example of how the influence over narratives about security in Nigeria has been reallocated into new media. The protests reveal how Nigerian citizens may utilize online platforms to record apparent police misconduct, organize demonstrations, coordinate humanitarian efforts, share accounts of their experiences, and leverage international networks. However, the #EndSARS events demonstrate how citizen information sharing has effectively undermined the long history of the Nigerian state’s dominance of the narrative space surrounding its security forces, as citizens have obtained new tools to record and broadcast their encounters with law enforcement directly to huge networks. This highlights the complexity of the contemporary digital environment, where verified and decontextualized material and conflicting accounts are quickly disseminated, with the dual capabilities of digital accountability and widespread information disorder characterized by contemporary new media.

The lesson of #EndSARS is not that citizen security information is inherently more trustworthy, nor that of the state should be prioritized – however, national security discussions increasingly require verification from several sources to ascertain a higher likelihood of reliability. The impact of the protests shows that even if a citizen generates factual security information, algorithms decide whether it remains obscure or widely distributed across networks of the population. Algorithms, virality, and the political economy of attention are explanations of digital phenomena that only consider user actions, failing to account for the influence and shaping of information delivery by the tech architecture of social media platforms. Digital platforms have

attention and an economic resource because their contents generate comments and views, through which the platforms profit through ad campaigns.

Because security information and content creates strong emotional reactions such as fear, anger, and pity, such contents have commercial value. This often results in exaggerated and dramatic content being amplified more, because it can easily cause widespread reactions and produce more hits and engagement on social media. The content made viral by bots and automated systems that are utilized to manage propaganda systems also influence political narratives, due to algorithms and artificial intelligence-powered. The source of the information is just one element that determines whether and to what degree its story is circulated; in fact, the platforms structure determines whether the narrative appears or is distributed to millions of internet users (Woolley and Howard, 2018).

Thus, the analysis of national security requires an understanding of the political economies of digital attention; that is, information disorder is not a problem derived only from the irresponsibility of users, but can be found in systems structured to promote engagement regardless of information quality and veracity.

Artificial Intelligence, Deepfakes and the New Crisis of Authenticity

Artificial intelligence that can 'create' original output seems to be one of the most profound recent developments in the sphere of digitally propagandized materials. Previous forms of falsified content, such as photoshopped photos, often required a degree of expertise and time. Emerging tools now make it relatively easy for anyone to create synthetic media that can mimic almost all previous tools. For instance, it is now possible to create synthetic text that emulates journalistic reports, synthetic photographs that can be made to show events that never occurred, technologies that can voice clone, which may seem to be reporting by public leaders, and deepfake video technologies that would fool users into thinking that they are looking at footage of public leaders in action or speaking at public occasions, which will now be totally fictionalized.

The impacts of all of this for Nigerian National Security include the fact that someone will now have the power to generate synthetic audio recording purporting to have come from a known public, religious, or political figure who at the time of the generation of the announcement may perhaps be involved in efforts to de-escalate ethnic or tribal tension, and this could generate further unrest and anger. The recording may be proven to be fake, but by then the damages would be irreparable, or at best, it would take a couple of hours before they can be debunked. Lawal (2025) makes a salient point about the relationship between AI, fake news, social media, public safety, and Nigerian security as a field. The challenge to national security does not lie only with the quality of evidence presented, but also whether people and institutions can be truly and confidently assess their authenticity.

Additionally, generative AI's capacity for falsification gives the "liar's dividend": with a general understanding of deepfakes, actors presented with irrefutable evidence can claim that the real content is fake and thus continue to sow doubt. Thus, generative media can undermine public trust, even regarding real media. The Nigeria security system will therefore need to invest more in digital forensics, as well as rapid authentication of security information and communication materials.

Government Regulation and the National Security–Freedom Dilemma

Digital propaganda has brought about a host of unavoidable problems, and calls for the introduction of rules to regulate it have naturally emerged. After all, if such chaotic phenomena are left unregulated, ordinary people will bear the brunt of the impact, and the public will naturally hope for binding regulations to rein them in. Governments around the world already have a legitimate responsibility to protect their citizens from harm caused by terrorism, incitement to unrest, organized violence, and other serious security threats. This is a perfectly reasonable and inherent duty, and no one can argue that this responsibility should not be shouldered.

However, if the scope of regulation is improperly opened, chaos is likely to arise if the definition of national security is framed too broadly, even legitimate public criticism is categorized as dangerous speech that endangers society, then this set of regulations, originally intended to protect the general public, will lose its legitimacy and may instead turn into a tool to suppress normal voices.

When viewed in the context of Nigeria, this concern is particularly prominent. This issue is not flagged as severe out of thin air; the Nigerian government and media have had complex, decades-long unresolved grievances, which makes the aforementioned regulatory risks especially glaring when placed against this backdrop. The reference template used in this analysis notes that the Nigerian government has historically held excessive discretion to define what constitutes national security and has at times required the media and the public to endorse the official interpretation of this concept. Over the past few decades, this one-sided control has created persistent, unresolvable tensions between the government and the media.

Even in the digital age, where almost everyone uses digital networks, the years of accumulated conflicts between the government and the media have not been resolved. Those long-standing problems have simply moved online along with the shift in communication methods and have not disappeared naturally because the way information spreads has changed.

Professional Journalism and the Recovery of Verification Authority

The proliferation of citizen communication does not render professional journalism obsolete or unnecessary. Instead, an abundance of information may amplify the importance of a credible verification process. Professional media organizations can establish distinct value through investigative reporting, rigorous source verification, contextual analysis and transparent mechanisms for correction. During national security emergencies, journalists serve as intermediaries, connecting official communications with fragmented online narratives.

However, traditional media outlets operate under economic and political pressures. The provided template illustrates how ownership structures, financial instability, and political interference can compromise media independence in Nigeria. These vulnerabilities persist in the digital age. Consequently, the credibility necessary to counteract digital propaganda cannot be achieved solely through the assertion of professional status. Nigerian journalism must consistently substantiate this authority through accuracy, independence, transparency, and verification.

Reconfiguring national security discourse necessitates parallel adjustments to security policy. Nigeria's national security framework should not be solely dedicated to territorial defense, intelligence acquisition, policing, and military capacity, while relegating information integrity to a secondary concern. An information-resilient national security architecture would acknowledge that hostile narratives, organized disinformation campaigns, and synthetic media can erode public trust, strain intergroup relations, and undermine institutional legitimacy.

Achieving such resilience demands collaboration among security agencies, professional journalists, fact-checking organizations, academic researchers, civil society groups, educational institutions, and digital platforms. The aim should not be to establish a singular, officially sanctioned national narrative, as such an approach would contravene democratic pluralism. Instead, the objective should be to enhance the information ecosystem, making it more difficult for demonstrably deceptive and harmful manipulation to eclipse verified information. Therefore, the core issue is resilience, rather than absolute control.

Nigeria cannot eradicate propaganda, rumors, or misinformation from digital communications. However, it can strengthen its institutions and citizenry to mitigate the effectiveness of manipulative communications. In this context, national security in the digital era encompasses not only safeguarding the national territory but also protecting the conditions that enable citizens to make informed judgments about societal threats. The transition from traditional media gatekeeping to networked digital communication presents both opportunities and vulnerabilities for journalists. It democratizes the national security discourse by granting citizens

unprecedented communicative agency, while simultaneously creating new avenues for propaganda, manipulation, and social polarization. Nigeria faces the challenge of preserving the democratic advantages of this transformed information environment while simultaneously cultivating institutional, technological, and societal resilience against its exploitation.

Implications of the Reconfigured Security Discourse for Nigeria's National Security

The integration of new media and digital propaganda into national security discourse has significant consequences for Nigeria. This transformation extends beyond increased information flow via digital platforms to a fundamental alteration in how national security is understood. Security institutions, political figures, journalists, activists, ordinary citizens, online personalities, and those disseminating misinformation now simultaneously vie to shape perceptions of insecurity. This dynamic impacts public confidence, social harmony, intelligence gathering, democratic processes, crisis management, and the state's legitimacy.

Public Trust in Security Agencies Declines

A primary consequence of digital propaganda is the potential undermining of public trust in security agencies. National security relies on both enforcement capabilities and public confidence in institutions responsible for citizen protection. When individuals are repeatedly exposed to conflicting accounts of security-related events, their certainty regarding reliable information sources may decrease. Digital environments exacerbate this issue, as official information is subject to immediate public scrutiny and comparison with eyewitness accounts, user-generated media and alternative narratives. If official communications are delayed, inconsistent, or demonstrably inaccurate, the public may become more receptive to unofficial explanations of the event.

Research on the Nigerian Defence Academy attack (Uwalaka, 2023) highlights this challenge, indicating that the military's insufficient social media engagement contributed to public criticism and perceptions of information being withheld. This suggests that institutional silence during security crises can erode credibility and allow alternative narratives to gain traction in the media.

Trust is crucial, as citizens who distrust government messaging may disregard valid security alerts, resist emergency directives, or favor information from unverified sources. Consequently, the credibility of national security institutions should be considered a strategic asset.

Social Polarization Intensifies

Digital propaganda can exacerbate existing political, ethnic, religious, and regional divisions. Nigeria's diverse society has a history in which identity influences political and security narratives. Digital communication can reinforce this by enabling users to engage in highly fragmented information communities. Algorithmic processes and social networks can repeatedly expose individuals to narratives that confirm pre-existing biases about opposing groups. When security incidents are viewed through ethnic or religious prisms, criminal actions can be generalized into broader narratives of collective animosity. Wardle and Derakhshan (2017) argued that information disorder thrives by exploiting existing social divisions, which is pertinent to Nigeria. Propaganda does not necessarily need to create new grievances; it can amplify pre-existing ones.

The national security implications are substantial. As communities increasingly interpret insecurity through the lenses of collective victimhood and shared blame, the likelihood of retaliatory violence, mutual distrust, and political instability increases.

National Cohesion Weakens

National cohesion depends on a baseline of shared commitment to common political institutions and a collective national identity. Digital propaganda can weaken this cohesion by repeatedly depicting the country

as being fragmented into antagonistic communities. Political actors may present security failures as evidence that state institutions serve specific ethnic, regional or partisan interests. Likewise, extremist or separatist communicators might frame state actions as indicative of systematic exclusion and persecution.

Such narratives can gradually undermine the legitimacy of national institutions, potentially leading to a fragmented national discourse in which disparate groups operate with conflicting understandings of the nation's history, institutions, and security landscape. The concern is not with disagreement itself; democratic societies inherently involve competing viewpoints. The security issue arises when propaganda transforms political disagreement into existential animosity and frames compromise as disloyalty.

Complexities for Intelligence and Security Operations

Digital communication also affects intelligence gathering and operational security. Security agencies can leverage open-source intelligence from social media, including eyewitness accounts, images, videos and public statements. However, the sheer volume of online information presents significant challenges in distinguishing reliable intelligence from deliberate misinformation. Malicious actors may disseminate false reports to misdirect security forces, conceal their movements, or sow confusion. Coordinated disinformation campaigns can thus impose operational burdens by compelling institutions to verify extensive data. The Nigerian Armed Forces' acknowledgment of social media as both a strategic communication tool and an operational risk illustrates this duality. Digital platforms can aid intelligence collection and counter-narrative efforts; however, inadvertent online disclosures can expose sensitive information.

This necessitates digital literacy not only among the general public but also within security institutions such as the police. Personnel must understand the interplay between open-source intelligence, digital deception tactics, and information manipulation in conventional security operations.

Crisis Communication and Information Velocity

A significant implication of new media is the compression of response time during crises. In the pre-digital era, security institutions typically had ample time to formulate official statements before their widespread public release. Digital media has drastically shortened this period. The public now expects immediate access to information. If official communication is delayed, unofficial accounts may quickly establish a prevailing narrative.

Vosoughi et al. (2018) indicated that false information can propagate faster than accurate information online. This suggests that crisis communication can no longer rely solely on delayed press conferences or conventional public relations methods. Security institutions require communication frameworks capable of prompt acknowledgments, verified preliminary information, and consistent updates. This does not entail divulging operationally sensitive details but rather providing sufficient credible information to preempt speculative narratives from dominating public discourse.

Democratic Accountability and Citizen Oversight of the State

The reshaping of the security discourse also has positive democratic implications. Citizens now possess an enhanced capacity to document the conduct of security institutions. Mobile devices and social media facilitate the independent recording and circulation of incidents involving law enforcement, military personnel, and other state actors, bypassing official channels. The #EndSARS movement exemplified this capability. User-generated content played a role in elevating allegations of police misconduct to a significant national and international issue. Digital platforms provide avenues for citizens to share their testimonies, document events, and demand accountability. This constitutes a notable redistribution of surveillance power. Historically, the

state has had considerable capacity to monitor its citizens. New media increasingly empowers citizens to monitor the state.

While this development can bolster democratic accountability, it also complicates national security operations when partial or decontextualized recordings are presented as comprehensive accounts of events. The challenge lies in maintaining citizen oversight while promoting the verification and contextual interpretation of the information.

Erosion of Traditional Media's Dominance

Another consequence is the diminishing hold of traditional media outlets on interpreting national security events. Newspapers, radio, and television retain influence but increasingly operate within a broader information ecosystem. Journalists may discover security-related stories through social media rather than traditional reporting channels. Social-media trends can shape mainstream news agendas, while mainstream reports are simultaneously disseminated and reinterpreted online.

This results in a hybrid media environment characterized by continuous interaction between legacy and new media. The effect on professional journalism is considerable. Media organizations can no longer rely solely on institutional authority to maintain credibility. Their competitive edge increasingly depends on verification, contextualization, expertise, and in-depth investigation.

When traditional media outlets recirculate unverified digital claims, they risk further eroding public trust. Conversely, rigorous fact-checking can strengthen their position as trusted intermediaries in an increasingly complex information environment.

Challenges to Democratic Governance

Digital propaganda also poses challenges to democratic governance, as public consent is significantly contingent on access to reliable information. Citizens must evaluate governments, political parties, and public institutions based on information pertaining to their performance. If digital manipulation systematically distorts this informational environment, democratic decision-making processes can become impaired. Political actors may employ fabricated claims to discredit opponents, exploit ethnic anxieties, or undermine electoral bodies. This is particularly problematic during elections, as political misinformation can have consequences extending beyond electoral choices, including diminished trust in institutions and post-election instability.

Igwebuike and Chimuanya (2021) illustrate the circulation of political fake news within Nigeria's 2019 electoral context. Their analysis supports the view that digital manipulation should be addressed not only as a media issue but also as a governance concern. Therefore, democratic stability requires an information environment in which citizens can distinguish legitimate political discourse from deliberate deception.

Information Sovereignty and Foreign Influence

The global scope of new media introduces the potential for foreign influence on domestic security discussions. Digital platforms operate internationally, enabling actors outside Nigeria to create, amplify, or manipulate narratives concerning Nigerian politics and national security. This scenario challenges traditional notions of information sovereignty, which are based on territorial control, as external actors can influence domestic attitudes without physical presence. Foreign influence operations may exploit existing societal divisions, including political, ethnic, or institutional distrust, potentially amplifying existing conflicts rather than solely creating new ones. Consequently, national security institutions require the capacity to identify coordinated transnational influence campaigns. This must be done without misrepresenting legitimate international criticism or diaspora engagement as foreign interference.

The distinction between cybersecurity and information security is becoming increasingly ambiguous. While traditional cybersecurity focuses on protecting systems and data from unauthorized access, digital propaganda targets public perceptions. However, these threats can be combined into a single threat type. For instance, hacked documents can be released selectively and presented misleadingly, or a cyberattack on a government entity might be accompanied by propaganda exaggerating the severity of institutional breakdowns. Similarly, fabricated claims of cyberattacks can generate public anxiety and fear among the public. The contemporary national security landscape necessitates a broader understanding of information security that encompasses both technological infrastructure and the integrity of public discourses.

The widespread dissemination of digital propaganda erodes trust in journalism. When fabricated content mimics journalistic formats, it becomes difficult for audiences to differentiate between professional reporting and false information. This challenge is compounded by the prevalent use of screenshots, imitation news sites, and altered headlines, which can make false claims appear to originate from established sources. The increasing sophistication of generative artificial intelligence is likely to exacerbate authenticity issues. Therefore, professional media organizations must implement robust authentication practices, transparent correction mechanisms, and public education initiatives focused on official digital channels.

Generative AI substantially expands the capacity for digital propaganda. The creation of realistic synthetic media, such as videos, photographs, and audio recordings, previously required specialized technical skills. Current tools have lowered both the cost and required expertise. Malicious actors can now generate substantial volumes of persuasive content, translate them into various Nigerian languages, and distribute them across numerous platforms. This creates an imbalance between content generation and verification, as false content can be produced rapidly, while its authentication may necessitate specialized forensic analysis. The national security challenge therefore shifts from identifying individual instances of falsehoods to building systemic resilience against large-scale synthetic communication.

While digital propaganda presents genuine national security concerns, there is also a risk of over-securitization. Governments may categorize a wide array of critical communications as security threats, potentially justifying stringent restrictions by framing public criticism as detrimental to national security. This risk is particularly pertinent in Nigeria, given the historical context of state attempts to define legitimate national security discourse and the documented imbalance between state authority and media freedom in this domain. Responses to digital propaganda must therefore avoid equating disagreement with disinformation or criticism with insecurity. A democratic national security framework should differentiate between legitimate criticism, unintentional inaccuracies, deliberate disinformation, incitement to violence, and operationally harmful communication. Failing to maintain these distinctions could undermine the democratic institutions that national security aims to protect.

The evolving information environment requires regulatory adaptation. Existing regulations were largely designed for communication systems in which identifiable organizations controlled content production. Digital communication complicates this model because information can be produced anonymously, distributed internationally, and replicated almost instantaneously. Effective regulation necessitates collaboration among government entities, technology companies, civil society, journalists, and researchers. However, regulatory legitimacy relies on transparency and proportionality. Measures implemented to counter digital propaganda must be clearly defined, subject to legal oversight, and consistent with constitutional protections of expression. Broad or vague prohibitions on "false information" risk creating a chilling effect on journalism and political discourse. The appropriate regulatory objective should focus on mitigating demonstrable harm rather than enforcing singular viewpoints.

Implications for Strategic Communication

The evolving information landscape necessitates that Nigerian security organizations re-evaluate communication strategies as a component of operational readiness. Strategic communication units should continuously monitor emerging narratives, identify information deficits, and promptly address significant instances of misinformation.

However, communication must prioritize accuracy over speed. While state-sponsored propaganda might yield short-term benefits, it can ultimately undermine the credibility essential for effective security messaging to be successful. Consequently, the most effective countermeasure to adversarial propaganda is not necessarily a direct retaliatory campaign. Instead, credible, timely, and verifiable information often serves as a more effective response.

Implications for Media and Digital Literacy

Citizens constitute the ultimate safeguard against various forms of digital manipulation. Technology platforms cannot eliminate all misleading content, and government agencies can not preemptively verify every claim before public dissemination. Therefore, individuals require the skills to assess information sources, recognize manipulative tactics, and confirm the veracity of information prior to sharing. Wardle and Derakhshan (2017) highlight the intricate nature of contemporary information disorder, underscoring the limitations of simplistic approaches to addressing "fake news." Consequently, digital literacy must encompass more than the identification of demonstrably fabricated content. Citizens should acquire proficiency in source verification, understanding visual manipulation techniques, recognizing algorithmic recommendations, discerning emotional appeals, and practicing restraint in information redistribution until its authenticity is confirmed.

Therefore, educational institutions, professional bodies, media organizations, and civil society groups should integrate digital and media literacy training into comprehensive civic education programs.

Implications for National Security Policy

The overarching implication of the reconceptualized national security discourse is the imperative for Nigeria's security framework to broaden its understanding of threats and resilience. While military strength, intelligence capabilities, and effective policing remain crucial, they are insufficient on their own to adequately counter digitally mediated insecurity.

Therefore, the national security policy should incorporate:

1. Information integrity

2. Strategic communication

3. Digital forensics

4. Open-source intelligence

5. Counter-disinformation capabilities

6. Public trust

7. Media literacy

8. Platform accountability

9. Protection of legitimate democratic communication

The objective should not be the establishment of absolute informational control, which is neither feasible nor desirable within a democratic society. Instead, the aim should be the cultivation of an information-resilient populace capable of resisting manipulation while preserving societal pluralism. This objective represents a significant consequence of the reconfiguration examined herein. In a digitally interconnected society, national security must extend beyond the safeguarding of physical territory against hostile actors. The integrity of the

information environment, credibility of institutions, and the populace's capacity to differentiate evidence from manipulation are increasingly fundamental to the nation's overall security.

Conclusion and Recommendations

Conclusion

The proliferation of new media has fundamentally reshaped Nigeria's communication landscape, altering the production, circulation, and interpretation of national security discourse. Previously centered on government institutions, security agencies, and traditional mass media, national security communication now operates in a decentralized and increasingly contested digital information environment. Social media platforms, online news outlets, citizen journalists, influencers, political figures, activists, insurgent groups, and the general public have all become active participants in defining security threats, identifying responsible parties, and evaluating government responses.

This study argues that this transformation signifies more than a mere technological shift in communication channels; it represents a reconfiguration of communicative power. The authority to construct national security realities is becoming distributed among various actors with differing interests, motivations, and credibility levels. Consequently, security incidents in Nigeria are no longer solely interpreted through official statements or professional journalism. Instead, they are subjected to immediate digital interpretation, contestation, amplification, and, at times, deliberate manipulation.

The rise of digital propaganda is central to this shift in the political landscape. Contemporary propaganda leverages the interactive, instantaneous, and algorithmically mediated nature of new media to shape public perception. Computational techniques, coordinated networks, emotional framing, selective information dissemination, decontextualized audiovisual materials, and artificial amplification can enhance the visibility of specific narratives. International scholarship has identified digital platforms as crucial infrastructures for contemporary information disorder and political manipulation (Wardle & Derakhshan, 2017; Woolley & Howard, 2018). Wardle and Derakhshan's framework is particularly pertinent as it distinguishes between misinformation, disinformation, and malinformation, demonstrating that harmful communication involves not only fabricated information but also the strategic deployment of authentic information.

Within the Nigerian context, the relationship between new media and security is particularly intricate. Digital platforms can bolster national security communications by enabling security institutions to directly engage with citizens. For instance, Uwalaka and Nwala (2022) found that the Nigerian military used social media to publicize its activities in Northern Nigeria, deter insurgents, demoralize adversaries, and foster public trust. Their study, which analyzed 10,750 social media posts, comments, and tweets, indicates that digital communication has become a significant aspect of contemporary conflict communication in Nigeria.

Conversely, digital communication can undermine security when institutional communication proves ineffective. Uwalaka's (2023) examination of the Nigerian Defence Academy terrorist attack revealed that the Nigerian military's limited social-media response and reliance on silence failed to establish an effective counter-narrative amidst the ensuing online controversy. This study, which analyzed 8,210 Facebook posts and comments, showed that digital silence permitted criticism, suspicion, and alternative interpretations to dominate online discussions. This reinforces the paper's argument that security institutions cannot afford to view communication solely as a supplementary public relations function; strategic communication is now an integral component of contemporary security capabilities.

The Nigerian situation is further complicated by the interplay of digital propaganda and existing political, ethnic, religious, and regional divisions. Misleading information becomes especially dangerous when it frames individual criminal acts as collective ethnic aggression, political disagreements as existential conflicts, or security operations as the systematic persecution of specific communities. In such scenarios, digital propaganda can escalate existing grievances into more heightened hostility.

Therefore, the primary danger lies not merely in the dissemination of inaccurate information but in its potential impact on social relations. Information disorder can erode institutional credibility, intensify political polarization, deepen ethno-religious suspicion, undermine confidence in electoral processes, complicate security operations, and diminish citizens' willingness to accept credible governmental information. Wardle and Derakhshan (2017) similarly highlight that contemporary disinformation campaigns can exploit existing societal tensions, contributing to mistrust and confusion.

However, responding to digital propaganda solely through governmental control presents another significant security and democratic challenge. National security cannot legitimately serve as an overarching justification for suppressing criticism, journalism, activism, or political dissent. The conceptual framework underpinning this paper similarly underscores the risks associated with the state acquiring excessive authority to define national security and expecting uncritical acceptance of these definitions from the media and citizens.

Consequently, the solution to digital propaganda should not involve establishing a government monopoly over national security narratives. Democratic societies inherently accommodate competing interpretations of public events. Instead, the objective should be to enhance the integrity and resilience of the national information environment, enabling citizens to access credible information, allowing institutions to respond swiftly to deceptive narratives, and making it increasingly difficult for malicious actors to exploit information gaps in the system.

This study posits that national security in contemporary Nigeria must be reconceptualized beyond territorial integrity, military capacity, and physical protection. It increasingly involves information integrity, institutional credibility, communication resilience, and citizens' ability to discern credible evidence from manipulation. Security in the era of digitally networked communication is partly a contest over information, meaning, and public trust.

Nigeria cannot entirely eradicate misinformation, disinformation, or propaganda, nor can it realistically revert to an information environment in which traditional gatekeepers dictate all public knowledge about security. What is attainable is the development of institutional and societal resilience capable of mitigating the influence of harmful information without compromising the democratic communication freedoms expanded by new media.

This paper's central assertion is that new media have reconfigured Nigeria's national security discourse from a predominantly state-traditional media relationship into a networked, participatory, and contested communication environment in which narrative power is dispersed among institutions, citizens, political

actors, technological platforms, and strategic propagandists. The appropriate response is not absolute information control but rather the cultivation of credible institutions, professional journalism, strategic communication, digital literacy, technological preparedness and proportionate democratic regulation.

Ultimately, national security in the digital age depends not only on the state's capacity to physically defend its territory and citizens but also on society's ability to maintain sufficient informational integrity for citizens to differentiate genuine threats from manipulated narratives and make informed judgments on matters crucial to the nation's survival.

Recommendations

Given the aforementioned conclusions, the following recommendations are proposed to enhance Nigeria's national security in the context of the new media:

1. Strengthen Institutional Communication Capabilities

Security institutions should prioritize the development of robust, agile, and responsive communication strategies. This includes investing in professional communication personnel, training them in digital engagement and crisis communication, and establishing clear protocols for the rapid dissemination of accurate information. Direct engagement through social media platforms, as demonstrated by the Nigerian military's successful efforts in deterring insurgents and building trust, should be strategically employed and consistently evaluated for effectiveness.

2. Promote digital literacy and critical thinking:

A comprehensive national digital literacy program is essential. This program should equip citizens with the skills to critically evaluate online information, identify propaganda techniques, understand the mechanisms of information disorder, and verify the sources of information. Partnerships between government agencies, educational institutions, civil society organizations, and technology companies can facilitate the development and dissemination of educational resources across diverse populations.

3. Fostering Collaboration Between State and Non-State Actors:

Building resilience against information disorders requires a multi-stakeholder approach. This involves establishing formal and informal channels for collaboration among government security agencies, traditional media, online news platforms, fact-checking organizations, academia, and civil society groups. Such collaboration can facilitate early warning systems for emerging threats, coordinated responses to disinformation campaigns, and the development of shared frameworks for understanding and addressing information challenges in the future.

4. Develop Proportionate and Targeted Regulatory Frameworks:

Regulatory frameworks addressing harmful online content should be developed while avoiding blanket censorship. These regulations must be proportionate, transparent, and aligned with democratic principles and

human rights. Focus should be placed on combating coordinated inauthentic behavior, foreign interference, and the amplification of illegal and dangerous content rather than restricting legitimate expression or criticism. International best practices for platform accountability and content moderation must be considered.

5. Enhance technological preparedness:

Security agencies and government bodies must enhance their understanding and application of technologies relevant to the digital information environment. This includes investing in tools to monitor online discourse, detect disinformation campaigns (including the use of AI-generated content), and understand the algorithmic processes that shape information visibility. Capacity building in cybersecurity and digital forensics is crucial for countering state-sponsored or sophisticated disinformation operations.

6. Reconceptualizing National Security Communication

National security communication must be integrated into the broader national security strategy and recognized not as a peripheral public relations activity but as a core capability. This involves understanding communication as a battlefield where narratives are contested and where maintaining public trust and institutional credibility is as vital as physical defense. Continuous research and analysis of the evolving information environment are necessary to adapt strategies effectively to the changing environment.

7. Support professional journalism and fact-checking:

A vibrant and independent press is a critical bulwark against the spread of disinformation. Efforts should be made to support professional journalism, ensure media freedom, and encourage the growth of credible and reliable fact-checking initiatives. This can involve funding mechanisms, training opportunities, and fostering an environment in which journalists can operate safely and effectively.

By implementing these recommendations, Nigeria can work towards building a more resilient information environment, strengthening its national security, and preserving the democratic benefits of new media technologies.

Recommendations

Based on the conceptual issues discussed in this study, the following recommendations are proposed.

1. National Security Policy Should Explicitly Integrate Information Integrity

Nigeria’s national security framework should explicitly recognize information integrity as a critical component of national security. National security should not be narrowly defined by military capabilities, intelligence, territorial integrity, or policing. A society's capacity to resist deliberate disinformation, computational propaganda, and coordinated manipulation must be integrated into contemporary security planning. This does not imply that ordinary disagreements are classified as security threats. Instead, national security institutions should develop measurable capabilities to identify coordinated information operations

that demonstrably possess the potential to incite violence, disrupt institutions, or cause significant social instability.

2. Strategic Communication Should Be Established as a Core Security Capability

Government ministries, military, police, and other security agencies should institutionalize professional strategic communication within their operational planning processes. Evidence from Uwalaka and Nwala (2022) suggests that social media already plays vital roles in Nigerian military conflict communication, including public engagement and trust-building. Uwalaka's (2023) findings regarding the NDA attack also highlight the risks associated with inadequate communication during digitally visible crises. Consequently, security institutions should establish dedicated communication units with the capacity to: (a) promptly acknowledge significant security incidents; (b) provide regular, verified updates; (c) correct demonstrably false information; (d) respond to emerging rumors; (e) coordinate communication among relevant agencies; and (f) transparently communicate uncertainty when complete information is unavailable. Strategic communication must remain evidence-based, as institutional propaganda, while potentially offering short-term reputational advantages, ultimately erodes public confidence.

3. Government Should Prevent Information Vacuums During Security Crises

Delayed communication provides fertile ground for rumors and digital propaganda to establish dominant interpretations of events. Therefore, security institutions should implement protocols for releasing preliminary verified information while investigations are ongoing. It is preferable to inform citizens that certain facts are still under investigation rather than maintain complete silence, which allows speculative narratives to dominate the digital space.

4. Nigeria Should Establish a Coordinated National Counter-Disinformation Framework

A national counter-disinformation framework should convene relevant security agencies, professional media organizations, technology experts, fact-checking organizations, academics, and civil society institutions to work together. The framework should prioritize the identification of coordinated manipulative activities over the policing of political opinions. Its functions could include (a) detection of coordinated influence operations, (b) rapid verification of viral security claims, (c) authentication of official communications, (d) identification of impersonated government accounts, (e) analysis of organized bot networks, (f) monitoring of malicious synthetic media, and (g) public communication regarding verified information. Such a mechanism must operate transparently and be subject to constitutional and judicial oversight.

5. Digital and Media Literacy Should Be Treated as a Component of National Security Resilience

Nigeria should integrate media and digital literacy into formal education and broader public communication initiatives to achieve this. Citizens should be equipped with the skills to (a) identify credible sources, (b) recognize manipulated headlines, (c) distinguish commentary from evidence, (d) verify photographs and videos, (e) recognize emotionally manipulative content, (f) understand misinformation and disinformation, (g) identify impersonated accounts, and (h) refrain from forwarding unverified security information. Wardle and Derakhshan (2017) argue that addressing information disorder requires concerted efforts from governments, educators, civil society, technology companies, and media institutions. Therefore, universities, secondary schools, journalism training institutions, and civic organizations should incorporate digital verification training into their curricula and public programs.

6. Professional Journalism Should Emphasize Verification-Based Reporting

The increasing volume of citizen-generated information underscores, rather than diminishes, the importance of professional journalism. Nigerian media organizations should invest in the following: (a) dedicated fact-checking desks, (b) digital verification tools, (c) open-source investigation techniques, (d) specialized national security reporting, (e) transparent correction procedures, and (f) enhanced communication with audiences

regarding the verification process. In the digital age, the comparative advantage of professional journalism should lie in credibility, context, and verification, not merely speed.

7. Media Organizations Should Avoid Amplifying Unverified Security Claims

Traditional media organizations must exercise caution when incorporating viral social media content into news reports. The existence of a trending claim does not necessarily validate its accuracy or reliability. Journalists should verify the origin, date, location, and context of photographs, videos, and security claims before they are published. Media organizations should also avoid sensationalizing security incidents in headlines for audience engagement if such framing generates unnecessary panic or collective blame.

8. Government Regulation Should Be Rights-Sensitive and Proportionate

Regulatory responses to digital propaganda must respect constitutional protections for freedom of expression and legitimate journalism. Legal provisions addressing harmful digital communication should clearly differentiate among (a) legitimate political criticism, (b) satire, (c) inaccurate but good-faith communication, (d) misinformation, (e) deliberate disinformation, (f) incitement to violence, (g) terrorist propaganda, and (h) communication that directly compromises security operations. Ambiguous laws that criminalize vaguely defined "false information" risk encouraging censorship and suppressing legitimate democratic discourse. Regulatory interventions should therefore adhere to the principles of legality, necessity, proportionality, and judicial accountability.

9. Technology Platforms Should Assume Greater Responsibility

Digital platforms are not neutral intermediaries, as their recommendation systems influence information visibility. Technology companies operating in Nigeria should strengthen mechanisms for (a) identifying coordinated inauthentic behavior; (b) reducing the amplification of demonstrably harmful disinformation; (c) detecting impersonated government accounts; (d) labeling manipulated media; (e) providing researchers with appropriate transparency data; (f) responding rapidly during security emergencies; and (g) improving moderation capacity in Nigerian languages. Platform accountability should be pursued through transparent means rather than opaque governmental pressure.

10. Nigeria Should Develop AI and Deepfake Detection Capacity

The increasing availability of generative artificial intelligence necessitates urgent preparedness. Government agencies, universities, media organizations, and technology institutions should invest in digital forensic capabilities for detecting synthetic images, cloned voices, and manipulated videos. A rapid-response authentication system should also be established for high-risk situations involving apparent statements by (a) the President or senior government officials; (b) military commanders; (c) religious leaders; (d) electoral officials; and (e) other influential public figures. Official government communications should increasingly incorporate digital authentication mechanisms to mitigate impersonation.

11. Security Institutions Should Improve Open-Source Intelligence Capability

Social-media platforms contain substantial amounts of potentially valuable information related to emergencies, terrorist activities, criminal incidents, and public perceptions. Security institutions should develop specialized open-source intelligence capabilities while adhering to privacy and legal safeguards. Personnel should be trained to distinguish organic citizen communication from coordinated manipulation and to verify information prior to its operational use.

12. Political Actors Should Be Held Accountable for Organized Digital Disinformation

Political parties and candidates should adopt enforceable codes of conduct to prevent the production or financing of disinformation campaigns. Electoral institutions, civil society, and professional organizations should collaborate to identify coordinated manipulations during elections. Political competition should not be used to legitimize communication that can incite ethnic, religious, or regional hostility.

13. Greater Attention Should Be Paid to Local Languages

A significant portion of research and counter-disinformation efforts disproportionately focuses on English-language communication. However, substantial political, religious, and security discourse occurs in Hausa, Yoruba, Igbo, Nigerian Pidgin, and other Nigerian languages. Propaganda and misinformation disseminated in indigenous languages may evade automated moderation and elite fact-checking institutions. Therefore, digital literacy programs, platform moderation, and research initiatives must become linguistically inclusive.

14. Security Communication Should Prioritize Public Trust

Security institutions should recognize that public trust is not cultivated solely in emergencies. Consistent accuracy, transparency, accountability, and willingness to acknowledge errors are essential for maintaining credibility. Citizens are more likely to accept emergency communications from institutions that they regard as trustworthy. Consequently, public trust should be viewed as an integral component of the long-term national security infrastructure.

15. Interagency Communication Should Be Improved

Contradictory statements from different government agencies can inadvertently create conditions conducive to propaganda. Nigeria should establish clearer communication and coordination protocols during major national security incidents to prevent relevant institutions from disseminating inconsistent information. This does not necessitate suppressing institutional autonomy; rather, it requires agreed-upon procedures for verification and public communication to be implemented.

16. Fact-Checking Organizations Should Receive Greater Institutional Support

Independent fact-checking organizations play an increasingly vital role in digital information. Collaboration among universities, media organizations, technology companies, and fact-checking institutions should be encouraged. However, their independence must be protected to prevent fact-checking from becoming an extension of government propaganda or serving partisan interests.

17. Universities Should Expand Research on Digital Propaganda and Security

Nigerian communication, media, and security scholars should deepen interdisciplinary research into (a) computational propaganda; (b) algorithmic amplification; (c) political bots; (d) AI-generated disinformation; (e) extremist digital communication; (f) online ethno-religious narratives; (g) security communication; (h) digital political mobilization; and (i) public resilience against information manipulation. The rapid evolution of technology means that research findings can quickly become outdated, necessitating continuous empirical investigation.

18. A Multi-Stakeholder National Information Resilience Strategy Should Be Developed

Ultimately, no single institution can independently manage the challenges posed by digital propaganda. Nigeria requires a national information resilience strategy involving the government, security institutions, traditional media, technology platforms, academia, civil society, educators, and citizens. The objective should neither be censorship nor governmental control of national narratives. Instead, it should foster an information

environment in which (a) credible information is readily accessible; (b) deceptive communication is rapidly challenged; (c) citizens possess verification skills; (d) institutions communicate transparently; (e) platforms are held accountable; (f) professional journalism remains sustainable; and (g) constitutional freedoms are protected. This approach recognizes that the most effective defense against propaganda is not absolute information control but a society whose citizens and institutions are sufficiently resilient to recognize, interrogate, and resist manipulation. The future of Nigerian national security will, in part, depend on the quality of its information environment. A society inundated by propaganda, distrust, and competing fabricated realities becomes difficult to govern and vulnerable to manipulation. Conversely, a society characterized by credible institutions, informed citizens, responsible journalism, and resilient digital systems possesses a stronger foundation for national cohesion and security. New media need not become adversaries of national security. When properly governed and responsibly utilized, they can enhance early warning systems, public accountability, citizen participation, and institutional communication. The challenge for Nigeria lies in ensuring that the democratization of communication does not simultaneously lead to the democratization of manipulation.

References

1. Arnaudo, D. (2018). Brazil: Political bot intervention during pivotal events. In P. N. Howard & S. C. Woolley (Eds.), *Computational propaganda: Political parties, politicians, and political manipulation on social media* (pp. 128–152). Oxford University Press. https://doi.org/10.1093/oso/9780190931407.003.0007

2. DiResta, R., & Goldstein, J. A. (2025). Full-spectrum propaganda in the social media era. *Security Studies, 34*(4), 714–750. https://doi.org/10.1080/09636412.2025.2563254

3. Howard, P. N., Lin, F., & Tuzov, V. (2023). Computational propaganda: Concepts, methods, and challenges. *Communication and the Public, 8*(2), 47–53. https://doi.org/10.1177/20570473231185996

4. Igwebuike, E. E., & Chimuanya, L. (2021). Legitimating falsehood in social media: A discourse analysis of political fake news. *Discourse & Communication, 15*(1), 42–58. https://doi.org/10.1177/1750481320961659

5. Lawal, J. M. (2025). Public awareness of the implications of AI and social media proliferation of disinformation on public safety and Nigeria's national security. *African Journal of Stability and Development, 17*(1), 785–803. https://doi.org/10.53982/ajsd.2025.1701.41-j

6. Mustafa, H., Luczak-Roesch, M., & Johnstone, D. (2025). Conceptualizing the evolving nature of computational propaganda: A systematic literature review. *Annals of the International Communication Association, 49*(1), 45–60. https://doi.org/10.1093/anncom/wlaf001

7. Ogbodo, J. N., Orji-Egwu, A. O., Njoku, E. O., & Ngwu, O. L. (2026). Dynamics and contours of online disinformation based on perspectives from Nigerian internet users. *Discover Global Society, 4*, Article 54. https://doi.org/10.1007/s44282-026-00392-9

8. Sule, S. Y., & Ridwanullah, A. O. (2023). The evolution of strategic communication: Practices and reflections in Nigeria. *Public Relations Review, 49*(2), Article 102323. https://doi.org/10.1016/j.pubrev.2023.102323

9. Uwalaka, T. (2023). Nigerian military strategic use of social media during online firestorms: An appraisal of the NDA terrorist attack. *Journal of Communication Inquiry*. Advance online publication. https://doi.org/10.1177/01968599231151727

10. Uwalaka, T., & Nwala, B. (2022). Military social media use and conflict communication in Nigeria. *The Nigerian Journal of Communication, 18*(2), 58–73.

11. Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

12. Wardle, C., & Derakhshan, H. (2017). *Information disorder: Towards an interdisciplinary framework for research and policy making*. Council of Europe.

13. Wellington, N., Adetola, A. S., & Agbiti-Douglas, O. E. (2026). Implications of social media on national security: An overview of social media data on security issues in Nigeria. *Journal of Communication and Media Research, 18*(1, Special Issue 4), 111–119. https://doi.org/10.67107/jcmr.2026.649

14. Woolley, S. C., & Howard, P. N. (Eds.). (2018). *Computational propaganda: Political parties, politicians and political manipulation on social media*. Oxford University Press. https://doi.org/10.1093/oso/9780190931407.001.0001