Global Journal of History of International Relations & Diplomacy (GJOHIRD)
An International Journal Domiciled in the Department of History & Diplomatic Studies, Adeyemi Federal University of Education, Ondo, Ondo State, Nigeria.
Vol.1, No.1, Feb. 2026.

DIGITAL MILITIAS AND THE WEAPONIZATION OF SOCIAL MEDIA: IMPLICATIONS FOR NATIONAL SECURITY IN WEST AFRICA AND BEYOND

Usman, Ismaila Ajibola
Nigerian Army College Of Education, Ilorin
Email:
Tel:08030488305

And

S. O. Aghalino(Prof.)
Department of History And International Studies
University of Ilorin, Ilorin
Email :samlino@unilorin.edu.ng.
Tel:08039435843
Department of History And International Studies
University of Ilorin, Ilorin

Abstract
The rise of digital militias such as non-state actors exploiting social media for ideological propagation, recruitment and coordinated disruption of nation states has created a new layer of insecurity in West Africa and beyond. This study investigated how extremist groups, separatist movements and cyber-activists strategically use platforms such as Facebook, WhatsApp and X (formerly Twitter) to shape public opinion, spread misinformation and weaken state authority. Deploying qualitative research methodology, the study combined case studies from Nigeria, Ghana and Cameroon with primary data drawn from interviews involving military intelligence officers, civil society representatives and social media analysts. Findings revealed that digital mobilization allows hostile actors to bypass traditional surveillance systems, creating hybrid warfare dynamics that blur the boundaries between physical and virtual conflict. The study concluded that strengthening digital intelligence capabilities through a 'Digital Threat Intelligence Fusion' (DTIF) framework that is focused on early warning, inter-agency collaboration and cybersecurity integration would enhance counterinsurgency operations and regional stability. This research thus contributes to understanding the intersection of digital communication, hybrid warfare and national security in West Africa and beyond.

Keywords: *Traditional security systems, banditry, Nigeria, community policing, and national security architecture.*

Introduction

In recent years, the security landscape of West Africa has experienced a fundamental shift, driven by the convergence of digital technology, socio-political fragmentation and asymmetric conflict. Social media, once celebrated as a tool for democratic engagement and civic mobilization has transformed into a contested terrain for digital insurgency and hybrid warfare. Central to this development is the rise of digital militias, loosely organized, ideologically motivated online actors, including bots, influencers and diaspora sympathizers. These actors employ social media platforms to propagate disinformation, radicalize followers, erode public trust and incite violence. Unlike traditional armed groups, digital militias operate largely in the shadows of cyberspace. Their weapons are hashtags, livestreams, deepfakes, memes and encrypted communication channels. These actors exploit algorithmic

amplification and anonymity to coordinate online campaigns that often translate into offline unrest. In a region where state surveillance capacity, digital infrastructure and regulatory frameworks are still evolving, such phenomena present unprecedented threats to national stability.

In Nigeria, for instance, separatist groups like the Indigenous People of Biafra (IPOB) and jihadist factions such as Boko Haram have leveraged digital tools to expand their reach, influence public perception and mobilize support. In Ghana, though less impacted by violent militancy, early warning signs such as digitally mediated hate speech and misinformation highlight the urgent need for preventive frameworks. Cameroon's Anglophone conflict similarly reveals the strategic use of digital platforms by diaspora activists and local armed movements to escalate hostilities.

This study examines how digital militias weaponize social media to challenge sovereign authority and undermine national cohesion. It focuses on three country case studies of Nigeria, Ghana and Cameroon, using a comparative lens to uncover patterns in narrative construction, radicalization and digital mobilization. The paper argues that the convergence of youth disenfranchisement, identity politics and unregulated online spaces has created fertile ground for digital militancy in West Africa and beyond.

Conceptual Framework

Digital militias are informal, non-state cyber actors or loosely coordinated online networks that exploit digital technologies, primarily social media platforms, to propagate ideology, disseminate disinformation, mobilize support, incite violence and undermine state authority. Unlike conventional militias, these actors operate predominantly in the information domain rather than physical battlefields. Their tools include viral hashtags, manipulated images, deepfakes, fake news, anonymous troll accounts, bot networks and algorithmic distortion. Digital militias often align along political, religious, ethnic, or ideological lines. Some are affiliated with offline armed movements, such as the Indigenous People of Biafra (IPOB), Boko Haram and Ambazonian separatists in Cameroon, while others operate autonomously, using events such as the #EndSARS protests as a springboard for digitally mediated agitation. The operational behaviour of digital militias displays several distinctive features such as:

Decentralization: These actors lack formal hierarchies and coordination is often organic, fluid and enabled through encrypted messaging apps such as Telegram or Signal.

Anonymity: Digital militants frequently use pseudonymous handles and virtual private networks (VPNs) to evade identification and surveillance.

Rapid Mobilization: A single viral image or video, real or doctored, can incite protests, generate panic, or inspire global online solidarity in minutes.

Hybrid Tactics: Their methods combine disinformation, psychological operations, cyberbullying, and real-world calls to action, blurring the line between activism and subversion.

Low Barrier to Entry: There is no need for formal enlistment, arms training, or hierarchical loyalty. All that is required is ideological motivation and internet access.

Hybrid Warfare and Information Operations

Hybrid warfare represents the fusion of military, cyber, informational and economic tactics employed to achieve strategic objectives through ambiguity and indirect confrontation rather than open armed conflict. Information operations (IOPs), a key component of hybrid warfare, involve the use of communication tools to deceive adversaries, shape public perception and influence decision-making. Digital militias serve as the front-line agents of these IOPs.

In the West African context, hybrid strategies are increasingly evident. In Nigeria, both jihadist and separatist groups deploy edited videos and fake news to manipulate narratives about military

excesses, erode public trust and provoke hostility toward the state. In Cameroon, social media has been weaponized to deepen the Anglophone-Francophone divide, reinforcing ethnic polarization and resistance against central authority. These are not isolated digital expressions but deliberate interventions aimed at psychological destabilization.

The Cyber-Conflict Theory

This study is anchored in Cyber-Conflict Theory, which posits that cyberspace constitutes a new domain of geopolitical and social conflict, where state and non-state actors can wage war, disrupt institutions and reshape public consciousness without traditional warfare. The theory highlights a significant power asymmetry where even poorly resourced actors can project disruptive influence through digital means. Applying this lens to the activities of digital militias reveals the inadequacy of traditional, state-centric models of national security. States must adapt to a reality where sovereignty is contested not just by guns and borders but by tweets and memes. Therefore, national defence must now encompass cybersecurity, content monitoring, narrative control and digital literacy as strategic imperatives.

Social Media As A Tool for Weaponised Narratives

Social media platforms such as Facebook, WhatsApp, Twitter (now X), Telegram and TikTok have become strategic battlegrounds for digital militias. These platforms offer low-cost, high-reach avenues for disseminating disinformation, rallying support and orchestrating online-to-offline transitions in protest or violence. In Nigeria, during the #EndSAR's protests of 2020, digital actors used hashtags, livestreams and influencer accounts to mobilize mass participation and shape international perceptions of state brutality. Similarly, IPOB-affiliated accounts have shared selectively edited videos of military operations to inflame ethnic sentiments and discredit the Nigerian Army. In Cameroon, WhatsApp groups serve as virtual command centres for Anglophone separatists, who use audio messages and viral images to coordinate attacks and amplify their cause. Digital militias utilize several key tactics which include:

Hashtag Hijacking: Redirecting trending topics to insert political messaging.
Meme Warfare: Using humorous or symbolic images to reinforce ideological positions.
Doctored Media: Editing videos or images to mislead viewers or evoke emotional reactions.
Deepfake Content: Employing AI-generated fake videos to manipulate perceptions of leaders or institutions.
Swarm Reporting: Coordinated mass reporting to take down opposition content or silence dissenting voices.
These tactics are strategically deployed to build ideological communities, attract global attention and trigger social unrest.

Recruitment, Radicalization and Mobilization

Social media has emerged as both a recruitment ground and radicalization incubator. Boko Haram and the Islamic State West Africa Province (ISWAP) have used encrypted platforms like Telegram to share propaganda videos, recruit fighters, and issue ideological decrees. These messages often appeal to youth disillusioned with socio-economic marginalization, state corruption, and ethnic grievances. Unlike traditional radicalization processes, digital pathways are accelerated. A single viral video or emotionally charged narrative can push a vulnerable individual from passive observer to active supporter or combatant. These platforms foster echo chambers where dissenting voices are drowned and ideological reinforcement is algorithmically enhanced. Evidence from interviews with military intelligence personnel in Borno and North West Nigeria suggests that several young insurgents were first exposed to extremist ideology through social media before being contacted in person. Similarly, in Ghana, authorities have intercepted attempts by diaspora-linked groups to radicalize local youth through YouTube sermons and Twitter threads.

Social media algorithms favour content that triggers engagement, particularly anger, outrage and fear. Digital militias exploit this by crafting

emotionally resonant narratives that go viral quickly. This form of cognitive warfare seeks not just to inform or misinform but to alter how people think and what they believe. Digital militias hijack the national discourse by embedding false narratives into trending topics and discussions. For instance, during the #Lekki Massacre incident in Nigeria, conflicting accounts, videos and hashtags created a cloud of uncertainty, eroding trust in both government and mainstream media. This cognitive fog serves the strategic purpose of delegitimizing state authority and cultivating suspicion among citizens. The line between truth and propaganda becomes increasingly blurred, complicating national cohesion and crisis response.

The Digital Arms of IPOB and Boko Haram in Nigeria

In Nigeria, two major digital militia networks have emerged prominently: the Indigenous People of Biafra (IPOB) and Boko Haram (including ISWAP). While differing in ideology and geography, both have demonstrated mastery in the use of digital tools to shape perceptions, recruit sympathizers, and undermine state narratives. IPOB, through its media wing "Radio Biafra," broadcasts inflammatory content on YouTube, Facebook, and X, appealing to Igbo nationalism while vilifying the Nigerian state. They often circulate unverified videos allegedly showing military brutality against civilians, which stoke ethnic resentment and fuel secessionist fervour. During the 2021 Southeast security crisis, IPOB-aligned social media accounts actively spread misinformation to discredit the Army's internal security operations and to portray the group as victims of ethnic cleansing.

Boko Haram, by contrast, uses social media less for public engagement and more for strategic messaging to potential recruits and enemies. The group's encrypted Telegram channels and occasional video releases on jihadist forums serve to announce attacks, demonstrate capability, and inspire global jihadist sympathy. These videos are often accompanied by chants, Arabic invocations and ideological rhetoric meant to reinforce their theological legitimacy and military prowess. Both groups have demonstrated the ability to coordinate online narratives that echo in mainstream media, thereby magnifying their influence and reach.

Digital Warfare in The Anglophone Crisis in Cameroon

In Cameroon, the Anglophone Crisis has witnessed a steady digitization of separatist agitation. Ambazonian activists, primarily based in the diaspora, have turned platforms such as WhatsApp, Facebook and Telegram into tools of insurgent coordination. Leaders in exile conduct weekly live streams, issue virtual commands and use digital platforms to shame or pressure residents perceived to be collaborating with the central government. Ambazonian fighters frequently release footage of confrontations with the Cameroonian military, using captions to frame the conflict as genocide or ethnic persecution. These videos, often lacking context or authenticity, evoke emotional reactions from sympathizers and international observers. They have successfully shifted the discourse on global platforms, casting the Cameroonian state as repressive while legitimizing insurgent actions. Moreover, online campaigns such as #FreeAmbazonia and #StopCameroonGenocide have trended repeatedly, often accompanied by fabricated casualty statistics and AI-generated images. The psychological impact of this sustained digital campaign is evident in the growing mistrust between Anglophone civilians and government security forces.

A Case of Preventive Digital Monitoring in Ghana

Ghana has not faced armed insurgency on the scale of Nigeria or Cameroon, the country however presents a unique case of proactive digital threat management. Intelligence services in Ghana have developed early-warning systems focused on monitoring extremist discourse in online spaces. Between 2020 and 2023, the Ministry of National Security intercepted online radicalization attempts targeting northern youth via YouTube and Islamic Facebook groups. The government has partnered with civil society organizations to conduct digital literacy workshops, emphasizing the dangers of online disinformation and radical recruitment. In addition, Ghanaian cyber units regularly monitor cross-border ideological spill overs, especially from northern Burkina Faso and Mali which are

regions with high jihadist activity. While not immune to digital militancy, Ghana demonstrates how digital threat awareness and inter-agency collaboration can serve as a model for pre-emptive action in cyberspace.

Challenges to National Security Architecture: The weaponization of social media by digital militias presents significant and multidimensional challenges to the national security architecture across West Africa and beyond. Traditional defence and intelligence models, built around physical borders and kinetic threats, are increasingly ineffective against the decentralized, fast-paced and transnational nature of online insurgency. The rise of digital militias groups that use social media platforms to mobilize support, spread disinformation and incite violence has exposed glaring gaps in West African security systems. These challenges are structural, legal, technological and societal in nature and they collectively inhibit the region's capacity to pre-empt and respond to cyber-enabled security threats.

Surveillance Limitations and Technological Gaps: One of the most pressing issues is the limited surveillance capacity and technological shortfall confronting most West African nations. National intelligence agencies are often ill-equipped to track, analyse and respond to the activities of digital militias in real time. The region lacks comprehensive cyber forensic laboratories, digital intelligence infrastructures and skilled personnel trained in cybersecurity and data analytics. Moreover, digital insurgents continually migrate between open platforms such as Facebook, X and TikTok and encrypted messaging apps like Telegram, Signal as well as WhatsApp. This tactical fluidity makes it difficult for national security agencies to maintain sustained monitoring. For instance, Boko Haram and the IPOB are known to utilize encrypted channels to coordinate propaganda, fundraising and recruitment, effectively evading state surveillance mechanisms.

In Nigeria, the absence of a unified and centralized digital monitoring platform has resulted in fragmented intelligence collection and delayed responses to online threats. Agencies operate in silos, without an integrated threat fusion system, leading to redundancy, inefficient resource utilization and gaps in national situational awareness.

Legal and Policy Deficiencies: Although several West African countries, including Cameroon, have enacted cybercrime laws, many of these frameworks remain outdated and inadequate for confronting today's rapidly evolving digital threats. In Nigeria, the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 recently amended in 2024, still prioritizes economic and financial crimes while offering limited guidance on emerging concerns such as algorithmic radicalisation, bot-driven disinformation, and foreign digital interference. Despite the amendment's expanded penalties and reporting obligations, it falls short of addressing the complex dynamics of online extremism and digital militancy. This legal gap enables extremist actors and cyber-propagandists to exploit social media platforms with minimal accountability. Furthermore, government attempts to tighten online regulation often spark public resistance, particularly when such measures are viewed as infringements on freedom of expression. The 2021 suspension of Twitter (now X) in Nigeria, for instance, provoked both domestic and international criticism, underscoring the fragile balance between safeguarding national security and protecting civil liberties. These unresolved legal and political tensions continue to impede the creation of a coherent and credible digital security framework across the region.

Misinformation, Public Distrust and Civil Unrest: Digital militias exploit public discontent and existing grievances to sow distrust in state institutions. Through the dissemination of manipulated images, deepfake videos and emotionally charged falsehoods, they incite unrest and delegitimize state authority. Viral videos of alleged military or police brutality, even when unverified or doctored, rapidly circulate on social media, inflaming tensions and leading to spontaneous protests or violent confrontations. The #EndSARS protests in Nigeria provide a vivid example. During the demonstrations, misinformation spread widely, some of it intentionally curated by hostile digital actors, leading to retaliatory attacks on police stations and

government assets. The government's response, which included violent crackdowns and digital blackouts, further eroded public trust and handed a narrative advantage to digital insurgents.

Cross-Border Propaganda and Foreign Interference: Another emerging challenge is the role of diaspora networks in fuelling digital militancy. Many separatist or insurgent movements have active online support bases among West Africans and Cameroonians living abroad. These diaspora actors often possess greater access to technology, media platforms and funding, allowing them to influence narratives back home with considerable impact. In Cameroon, for example, Anglophone separatist messages are often drafted and disseminated by activists based in the United Kingdom and the United States. These messages, amplified through targeted social media campaigns, shape local perceptions, erode confidence in government responses, and attract international attention and sympathy to their cause. This transnational propaganda complicates domestic stabilization efforts and requires coordinated diplomatic and intelligence responses.

Towards A Digital Threat Intelligence Fusion (DTIF) Framework

Given the limitations of current approaches, states in West Africa and beyond must adopt a more coordinated, data-driven and anticipatory strategy to counter digital militancy. The proposed DTIF framework offers a holistic model that integrates military and civilian efforts, leverages emerging technologies and promotes regional cooperation. DTIF is designed to move beyond reactive security policies and instead emphasize real-time intelligence, narrative control and proactive disruption of digital militant networks.

Integrated Cyber Command Centres (ICCCs): These centres would serve as the operational hub for digital threat monitoring. Jointly managed by civilian and military actors, ICCCs would collect, analyse and act on intelligence sourced from telecom providers, internet service companies, and social media platforms. Nigeria's existing Defence Cyber Command can be upgraded to serve this role, provided it is given sufficient legal backing and technical capacity.

AI-Driven Threat Detection Systems: Artificial intelligence and machine learning tools can greatly enhance early warning capabilities. These systems can flag coordinated disinformation campaigns, hate speech spikes, or bot activity by analysing massive datasets in real-time. Platforms such as Graphika and Google's Jigsaw have demonstrated the feasibility of AI-supported threat detection in fragile and polarized environments.

Strategic Communication and Counter-Narrative Units: Controlling the narrative space is as critical as physical security. DTIF proposes dedicated units focused on countering disinformation and promoting accurate, pro-national narratives. These units would partner with local influencers, religious leaders, educators and journalists to build credibility and engagement. Effective storytelling and rapid rebuttal of fake news can deny digital militias the public sympathy they often exploit.

Community-Based Digital Literacy Initiatives

Empowering citizens to recognize and resist disinformation is a grassroots solution to a digital problem. Integrating media literacy into school curricula, youth programs and community outreach can reduce the susceptibility of vulnerable populations to digital manipulation. Programs like Ghana's CyberSafe Community and Nigeria's pilot initiatives under the Nigeria Security and Civil Defence Corps (NSCDC) should be expanded nationally to build a digitally resilient society.

Regional Cybersecurity Collaboration Platforms

Since digital militias often operate across national borders, regional responses are essential. ECOWAS should lead in establishing a Regional Digital Threat Observatory to facilitate data sharing, real-time intelligence exchange and coordinated response strategies. A formal DTIF charter could also include mutual cybersecurity assistance protocols, technical training programs and sanctions against content hosts or financiers of digital insurgency.

Implementation Considerations

To make DTIF operational, several foundational elements must be addressed which include legislative safeguards essential to define the scope of digital militancy, protect civil liberties and standardize data-sharing agreements. Platform

accountability must also be enforced by compelling social media companies to set up in-country content moderation teams and comply with national security protocols. Moreover, adequate funding is critical. National budgets must allocate sustained resources for DTIF infrastructure, capacity-building and software development. Finally, there must be a strong military-education interface, where digital threat studies are embedded in the curricula of defence academies and military colleges. Officers should be trained in social media analytics, cognitive warfare and digital influence operations.

The threat posed by digital militias in West Africa and beyond is evolving rapidly, outpacing traditional national security mechanisms. If left unchecked, their activities could undermine governance, deepen civil unrest, and destabilize entire states. The DTIF framework, built on coordination, technology and trust, provides a blueprint for proactive, integrated digital defence. In this digital age, safeguarding national security will depend not only on the strength of arms bought, but on the agility of minds and the resilience of societies online.

Conclusion and Policy Recommendatios

The proliferation of digital militias and their strategic weaponization of social media represent a new and complex threat to national security in West Africa and beyond. These actors are not confined to traditional battlegrounds but operate within the intangible yet highly influential domain of cyberspace. Their operations are rooted in the manipulation of digital platforms, exploitation of algorithmic systems, mobilization of diasporic networks and the leveraging of existing political or ideological grievances. Through these means, they distort public discourse, incite communal violence and systematically delegitimize state institutions.

The experiences of Nigeria, Cameroon and Ghana reveal that digital militancy has evolved beyond fringe cyber-activism into a central security challenge. From the #EndSARS movement hijacked by external agitators in Nigeria, to secessionist campaigns in Cameroon that rely heavily on diaspora-led digital propaganda and the rise of political misinformation networks in Ghana, the region is witnessing a convergence of online insurgency with offline consequences. This convergence demands a shift in the way West African states understand, respond to and anticipate national security threats. Addressing this threat requires more than isolated crackdowns or reactive policies. It calls for a comprehensive, forward-looking strategy that aligns technology, governance and civil engagement. The Digital Threat Intelligence Fusion (DTIF) framework, as proposed, offers a viable response. This model prioritizes anticipation over reaction, emphasizing the need for proactive intelligence gathering and predictive analysis. It encourages coordination across security, civil and tech domains, recognizing that digital threats cut across multiple sectors and cannot be contained by security agencies alone. It also promotes digital literacy as a countermeasure to manipulation, favouring education and awareness over censorship and suppression.

For the DTIF framework to succeed, certain policy actions are necessary. Primarily, every country in the sub-region must institutionalize dedicated National Digital Threat Units with clear mandates, operational independence and legal authority to liaise with both international tech companies and domestic security actors. These units should serve as nerve centres for monitoring, analysing and responding to digital threats. Also, the region's legislative instruments must be revisited. Outdated cybercrime laws should be revised to specifically criminalize online incitement, disinformation campaigns driven by bots, and the non-cooperation of social media platforms with national security protocols. Without a solid legal framework, enforcement remains inconsistent and ineffective. Furthermore, there must be deliberate efforts to foster civil-military synergy in the digital domain. By working with tech innovators, researchers and civil society groups, the armed forces can support the development of robust early-warning systems, machine learning-based threat detection tools and culturally relevant counter-narratives. Additionally, a sustained investment in digital literacy is indispensable. Education systems and community outreach programs must incorporate media literacy to empower citizens particularly in vulnerable, conflict-prone areas, to critically engage with online content and resist manipulation.

Lastly, regional cooperation is essential.

ECOWAS must therefore lead the way by establishing a Regional Digital Threat Observatory to facilitate real-time intelligence sharing and innovation exchange among member states. In today's digital era, a viral tweet can destabilize a region faster than a battalion. The security future of West Africa and beyond will be defined not only by the capacity to deploy troops but also by the ability to deploy knowledge, digital foresight and collaborative intelligence.

Bibliography

Adebajo, M. 2022. "Cyber-Radicalization and Counterterrorism Strategy in North-East Nigeria." *African Security Review* 31, no. 2: 123–139.

Adebayo, J., and Y. Karam. 2023. "Foreign Disinformation Networks and Hybrid Warfare in West Africa: Emerging Trends and National Response Strategies." *Defence & Security Journal of Africa* 11, no. 1: 22–41.

Agbakwuru, T., and C. Mbah. 2021. "Cybersecurity Policy Coordination in Nigeria: Inter-Agency Rivalry and Institutional Fragmentation." *African Security Review* 30, no. 4: 342–358.

Akonor, K. 2023. "The WhatsApp War: Communication and Separatist Mobilization in Cameroon's Anglophone Crisis." *Conflict Studies Quarterly* 44: 88–105.

Benkler, Yochai, Robert Faris, and Hal Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford: Oxford University Press.

Carlucci, P., and A. Mumford. 2020. "Hybrid Warfare: The Continuation of Ambiguity by Other Means." *European Journal of International Security* 5, nos. 3–4: 315–333. https://doi.org/10.1017/eis.2020.2.

Chifu, I. 2019. *Hybrid Threats: Understanding and Responding to the Changing Nature of Conflict.* Helsinki: European Centre of Excellence for Countering Hybrid Threats.

Chiluwa, I., and P. O. Adebayo. 2021. "Online Discursive Aggression and the Legitimation of Separatist Agitation in Nigeria." *Journal of Language and Politics* 20, no. 3: 379–402.

Czosseck, C., and K. Geers. 2009. *The Virtual Battlefield: Perspectives on Cyber Warfare.* Amsterdam: IOS Press.

Dunn Cavelty, M. 2013. "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber - Security Discourse." *International Studies Review* 15, no. 1: 105–122.

Kpodo, T., and Y. Nyarko. 2022. "Digital Surveillance and Preventive Counterterrorism in Ghana." *Ghana Journal of Security and Intelligence* 3, no. 1: 45–60.

Makinde, F., and B. Olatunji. 2021. "Hashtag Revolutions and Digital Resistance: The EndSARS Protest in Nigeria."*Media, War & Conflict* 14, no. 3: 265–283.

Mensah, I., and K. Boateng. 2023. "Diaspora Influence on Youth Radicalization in Ghana's Digital Space." *West African Journal of Security Studies* 5, no. 1: 59–77.

National Assembly of the Federal Republic of Nigeria. 2024. *Cybercrimes (Prohibition, Prevention,etc.)(Amendment) Act, 2024.* Abuja: Federal Government Printer. https://naltf.gov.ng/nigerias-cybercrime-reform/.

Ndangam, L. 2021. "Diasporic Media Activism and the Framing of the Anglophone Conflict in Cameroon." *African Journalism Studies* 42, no. 1: 54–71.

Ndukwe, I. 2022. "Rethinking Nigeria's Cyber Defence Posture: Lessons for the Armed Forces." *Nigerian Defence Policy Review* 4, no. 1: 67–83.

Nwanze, U. 2022. "Weaponizing Social Media in Nigeria's Security Discourse: A Case Study of IPOB and the 2021 Eastern Unrest." *African Conflict Review* 8, no. 2: 101–118.

Oloruntoba, S., and T. Ajayi. 2022. "Contested Narratives and Trust Deficit: The Lekki Toll Gate Incident in Nigerian Media." *African Journal of Media Studies* 10, no. 1: 45–62.

Onuoha, F. C., and G. E. Ezirim. 2020. "Terrorism and Encrypted Communication: Boko Haram's Adaptation Strategies." *Studies in Conflict & Terrorism* 43, no. 4: 311–330.

Umaru, M., and M. Hassan. 2023. "Countering Disinformation through Strategic Narratives: Nigerian Approachesand Gaps." *African Media Studies Quarterly* 6, no. 2: 112–132.