GJCSR
Global Journal of Contemporary Social Research
Faculty of Social Sciences, Imo State University, Owerri, Nigeria • imsufoss.com
Vol. 1 • No. 1
November 2026
pp. 43–54

RESEARCH ARTICLE OPEN ACCESS DOUBLE-BLIND PEER REVIEWED

Between Transparency and Tipping Off: Security Communication, Operational Secrecy and National Security in Nigeria

Emmanuel Ogueri Ibekwe[1, *]

[1] *Department of Political Science, Faculty of Social Sciences, Imo State University, Owerri, Nigeria*
* **Correspondence:** emmanuelibekwe@yahoo.com
DOI: https://doi.org/10.68442/gjcsr/2026/v1i1.005

RECEIVED	REVISED	ACCEPTED	PUBLISHED
29 September 2026	26 October 2026	28 October 2026	2 November 2026

ABSTRACT

Nigeria faces overlapping threats from jihadist insurgency, armed banditry, kidnapping for ransom and communal violence. Security agencies and political leaders respond partly through the mass media, announcing deployments, operations, the relocation of commanders and new initiatives. Such communication can reassure citizens and support accountability, but it may also give armed groups useful warning. This article examines how security information is publicly disclosed in Nigeria and assesses what this means for intelligence, operational effectiveness and national security. Using qualitative documentary analysis of official statements, press briefings, media reports, legal instruments and recent scholarship, mainly from 2024 to 2026, it identifies five disclosure patterns: pre-announced operations and named targets; the publication of force locations and capabilities; unauthorised social media posts by personnel; media publication of classified material; and leakage through informant networks surrounding security meetings. The analysis draws on operations security theory, the mosaic effect, democratic accountability and strategic communication. It suggests that the problem lies less in communication as such than in its timing, level of detail and coordination. Announcements that reveal where, when and how forces will act appear most likely to help adversaries anticipate operations and relocate. Silence, however, carries its own costs, including misinformation, weak public trust and reduced human intelligence. The article therefore proposes a tiered security communication framework that separates strategic intent and results, which should be shared, from operational detail, which should be withheld or delayed, supported by media liaison protocols, social media discipline and independent oversight. It concludes that transparency and operational secrecy can be reconciled if Nigerian authorities explain purpose and report results openly while protecting method.

KEYWORDS Security Communication • Operational Security • Intelligence • National Security • Media • Security Agencies • Nigeria • Banditry • Counter-Terrorism

HOW TO CITE THIS ARTICLE • APA 7
Ibekwe, E. O. (2026). Between transparency and tipping off: Security communication, operational secrecy and national security in Nigeria. *Global Journal of Contemporary Social Research, 1*(1), 43–54. https://doi.org/10.68442/gjcsr/2026/v1i1.005

Licence: © 2026 The Author(s). Published by the Faculty of Social Sciences, Imo State University, Owerri, Nigeria. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International Licence (CC BY 4.0), which permits use, distribution and reproduction in any medium, provided the original authors and source are credited.

1. INTRODUCTION

In January 2026, a brigade commander in north-central Nigeria told journalists that the army had set up new forward operating bases at Patigi and Ilemona, with further patrol bases at Babasango, Gada and Daban Lema, and that it would tighten its grip on bandit hideouts across Kwara, Oyo and Niger States ("Banditry: We'll Deepen Offensive," 2026). The statement was meant to reassure communities living under the threat of armed groups. It also placed the positions of troops on the public record in an area where bandits move quickly and keep their own sources of information. Announcements of this kind are routine in Nigeria. They raise a question that the national security debate has seldom examined in a systematic way: at what point does telling the public about security operations begin to help the people those operations are meant to stop?

The question matters because the threat environment remains severe. The Global Terrorism Index 2026 recorded 750 terrorism deaths in Nigeria in 2025, a rise of 46 per cent on the previous year and the largest national increase in the index (Institute for Economics & Peace [IEP], 2026). Researchers cited by the Africa Defense Forum (2026) counted 599 banditry incidents and 2,742 casualties in 2025, nearly double the previous year. Between July 2025 and June 2026, an SBM Intelligence study recorded 1,713 kidnapping incidents in which 7,825 people were abducted and 1,142 killed, with ransom payments estimated at ₦7.78 billion ("Nigeria's Kidnap Crisis," 2026). In November 2025, the President declared a nationwide security emergency and ordered the recruitment of 20,000 additional police officers (State House, 2025).

Public communication is part of the state's response. Defence and police spokespersons hold regular briefings, ministers and governors announce new measures, and service chiefs speak during operational visits. This communication does useful work. It reassures frightened citizens, shows that government is acting and allows the press and Parliament to hold security institutions to account. Yet senior officers have themselves warned of its risks. In July 2026, the Director of Defence Media Operations told defence correspondents that some information could not be released immediately because of operational security, and that premature disclosure could have serious consequences ("DHQ Worries," 2026). Days later, the Chief of Army Staff described the unauthorised posting of troop movements, sensitive locations and operational information on social media as a serious breach of military regulations (Federal Ministry of Information and National Orientation [FMINO], 2026).

This article examines the practice of publicly announcing security initiatives in Nigeria and assesses its implications for intelligence gathering, operational effectiveness and national security. It addresses three questions. What kinds of security information are publicly disclosed, and through which channels? How might such disclosures help criminal and terrorist groups to anticipate, evade or adapt to state action? How can the legitimate public interest in security information be reconciled with the need to protect operations and intelligence? The article argues that the main problem lies not in communication itself but in poorly judged timing, excessive detail and weak coordination. Its contribution is a typology of disclosure risks drawn from recent Nigerian cases and a tiered framework for security communication that separates what the public needs to know from what adversaries want to learn. The article first clarifies its key concepts, reviews related literature and sets out its theoretical perspectives, then describes its method and the Nigerian context, presents five patterns of disclosure, discusses the costs of both disclosure and secrecy, and closes with the proposed framework.

2. CONCEPTUAL CLARIFICATION

Security Communication

Security communication refers here to the deliberate release of information by security institutions and political authorities about threats, policies, operations and outcomes, through press briefings, statements, interviews, official websites and social media. It overlaps with strategic communication, which Rice and Innes (2025) describe, in the counter-terrorism field, as campaigns designed to signal trust and to deter threats. In practice, security communication in Nigeria also includes less formal channels: remarks by governors at security council meetings, comments by commanders during visits, and the personal social media accounts of serving personnel. Some of this communication is planned; much of it is not.

Operational Secrecy and Operations Security

Operational secrecy is the protection of information whose disclosure would damage an ongoing or planned security activity. The most developed doctrine on this subject is operations security (OPSEC). The United States Department of Defense (2020) defines OPSEC as a process of identifying critical information, analysing which

friendly actions adversaries can observe, determining the indicators that adversaries might obtain and piece together to derive critical information in time to use it, and then selecting countermeasures. Two ideas in this definition are central to the present article. The first is critical information: facts about intentions, capabilities and activities that an adversary needs in order to act effectively. The second is indicators: observable details, often harmless in isolation, from which critical information can be inferred. A press statement naming the location of a new patrol base is an indicator of this kind.

National Security

National security is understood here as the protection of the state, its institutions and its population from organised violence and other serious threats. In Nigeria, this has increasingly meant protecting citizens in rural areas where the state's presence is thin. A recent study of Sokoto State found that armed groups in some areas had appointed administrators and were taxing residents, in effect replacing state authority (Okunola & Ayodele, 2026). Under such conditions, the protection of security operations and the protection of communities are closely linked.

3. REVIEW OF RELATED LITERATURE

Scholarship on media and political violence has long recognised that publicity cuts both ways. Armed groups seek attention, while states seek to shape the information environment in their favour. Recent work adds that the information content of open reporting is greater than is often assumed. Lampe et al. (2025), analysing more than two million newspaper articles on over 42,000 attacks, found that the content of media coverage was related to the interval before an organisation's next attack and to whether that attack would be novel. If open reporting carries enough signal to help analysts forecast terrorist behaviour, it is reasonable to assume that it can also help armed groups anticipate state behaviour. Makridis et al. (2024), in a study of cyber conflict, show a related point from the other direction: where operations are secret and complex, media coverage relies on partial sources and can feed public misperception.

Research on Nigeria has approached the issue mainly through press freedom and journalist safety. Jatula (2025) documents the political and legal pressures on the press between 2015 and 2023, and Pate and Jibril (2025), drawing on interviews with journalists in the north-east, show that reporters face physical and psychological attacks from insurgents, the military and communities. A second strand examines intelligence. Ohazulike and Okafor (2026) argue that inter-agency rivalry, limited technology, corruption and weak community trust have undermined intelligence gathering, and that without credible engagement with communities the flow of grassroots intelligence is constrained. A third strand concerns the wider security response. Madueke (2025) links the weakness of the police response to banditry to problems of size, funding and structure, while Okunola and Ayodele (2026) attribute the failure of successive interventions in Sokoto partly to coordination deficits and corruption.

Studies of counter-terrorism communication in established democracies offer further guidance. Clubb et al. (2025) show that the type of transparency, not its quantity, determines whether it builds trust. Rice and Innes (2025) show how trust is designed into, and contested within, public campaigns. Schrijver (2026) shows that disclosure can itself be an instrument of intelligence strategy when it is deliberate and controlled.

What is missing is a sustained analysis of how routine official announcements, rather than leaks or journalism alone, affect operational security in an African conflict setting. Nigerian debate tends to frame the problem as one of irresponsible media. The literature on intelligence, meanwhile, pays little attention to what officials themselves say in public. This article addresses that gap by examining disclosure across all its channels, official and unofficial, and by asking how the need for openness might be reconciled with the need to protect operations.

4. THEORETICAL FRAMEWORK

The article draws on four related perspectives. Each explains a different side of the tension between openness and secrecy.

Operations Security and the Mosaic Effect

OPSEC theory assumes that adversaries collect information continuously and that they gain most from details that are specific, timely and relevant to their own decisions (Department of Defense, 2020). The mosaic

theory, developed in the context of United States freedom of information law, adds that individually harmless items may be combined to reveal sensitive patterns (Pozen, 2005). Pozen also warned that the same reasoning can be stretched to justify withholding almost anything, since nearly any fact might form part of some mosaic. This caution is important for Nigeria, where security claims have at times been used against journalists. Neal (2026) identifies a related "visibility dilemma" in the protection of critical infrastructure: making hidden locations public can improve safety while also helping those who would attack them. Security communication faces the same dilemma. Information that reassures a village may also guide an attacker.

Democratic Accountability and the Right to Know

A second perspective begins from the public's right to information. Section 22 of the Constitution of the Federal Republic of Nigeria 1999 charges the mass media with upholding the responsibility and accountability of government to the people, and the Freedom of Information Act 2011 establishes a right of access to information held by public institutions. The Act permits refusal where disclosure "may be injurious to the conduct of international affairs and the defence of the Federal Republic of Nigeria" (Freedom of Information Act, 2011, s. 11(1)), but it also provides that such refusal shall not apply where the public interest in disclosure outweighs the injury (s. 11(2)). Secrecy has well-known democratic costs. In a historical study of French nuclear policy, Fraise (2025) shows how secrecy regimes excluded actors from decision-making, distorted the information available to citizens and allowed officials to escape democratic control. Jatula (2025) finds that the Nigerian press between 2015 and 2023 worked in a contested space shaped by illiberal regulation, state interference and self-censorship. From this perspective, calls for operational secrecy must be tested against the risk that they shield error or abuse.

Strategic Communication and Signalling

A third perspective treats communication as an instrument of security policy. Schelling (1966) argued that coercion depends on communicating resolve, so that what a state says about its intentions can shape an adversary's choices. Public announcements can therefore deter, reassure allies and mobilise citizens. Recent work shows that disclosure can also be used offensively. Schrijver (2026) describes how Ukraine's military intelligence directorate has used a public Telegram channel to project legitimacy, target the adversary through selective disclosure and enlist the public as contributors. The form of transparency matters too. In two survey experiments in the United Kingdom, Clubb et al. (2025) found that providing more procedural information about a prevention programme reduced public support for it, whereas explaining the rationale behind decisions increased acceptance and trust. Rice and Innes (2025) similarly argue that public trust in counter-terrorism messaging is not simply present or absent but is actively shaped by how campaigns are designed and received. These findings suggest that effective communication depends less on volume than on explaining purpose.

Adversary Learning and Adaptation

The fourth perspective concerns the adversary. Armed groups are not passive targets. Lubrano (2024) models strategic innovation in terrorist organisations as a process of evaluation, formulation, adoption and implementation, in which leaders assess the environment and change course. Nigerian bandit groups appear well suited to rapid adjustment. Community testimony gathered by the United Nations Institute for Disarmament Research describes them as highly mobile, forest-based units that carry out quick-strike attacks on motorcycles (Kleffmann & Ramachandran, 2024). For groups of this kind, advance knowledge of where and when security forces will act has immediate value, because relocation is cheap and fast.

Taken together, these perspectives suggest that the security value of a disclosure to an adversary depends on three factors: how specific it is about place, time and method; how timely it is relative to the planned action; and how easily the adversary can act on it. Strategic statements of intent score low on all three. Announcements that name a target, a location and a timeframe before an operation score high. This logic structures the analysis that follows.

5. METHODOLOGY

The study uses a qualitative design based on documentary analysis, which offers a systematic way of examining official documents, media texts and institutional records (Bowen, 2009). The material comprises official statements from the State House, the Defence Headquarters, the Nigerian Army and the Ministry of Defence; reports in national newspapers and news platforms; legal instruments; reports by international organisations and research bodies; and peer-reviewed scholarship. Most sources date from August 2024 to September 2026, a period

that includes the relocation of defence leaders to Sokoto, the declaration of a national security emergency and foreign air strikes in north-west Nigeria. An earlier episode, the 2019 military raid on the Daily Trust newspaper, is included as a reference case because it remains the clearest public confrontation over the publication of operational information.

Episodes were selected purposively where security information was publicly disclosed or where officials publicly discussed the risks of disclosure. Each was coded by type of information (intent, policy, results, location, capability, timing, sources), level of detail (strategic, operational or tactical), timing relative to action (before, during or after) and channel (official briefing, political statement, media publication, personnel social media or informal leakage). Themes were then developed through iterative comparison, following the general logic of thematic analysis (Braun & Clarke, 2006).

The design has clear limits. Public sources cannot show whether a particular disclosure caused a particular failure, since classified operational records are not available and adversaries rarely explain their decisions. Official accounts may also be self-serving: officers have an interest in blaming the media for setbacks. The analysis therefore identifies plausible risk pathways and recurring patterns rather than proven causal effects, and it treats claims by all parties with caution.

6. THE NIGERIAN CONTEXT

The Threat Environment

Nigeria's security challenges are geographically dispersed and organisationally varied. In the north-east, Boko Haram factions and the Islamic State West Africa Province continue their insurgency. In the north-west and parts of the north-central zone, bandit groups engage in kidnapping, cattle rustling and attacks on villages. Human Rights Watch (2026) reports that 2,938 people were kidnapped in the north-west between July 2024 and June 2025, more than 60 per cent of reported incidents nationwide, with 1,203 in Zamfara State alone. In Sokoto, the emergence of the Lakurawa group has been interpreted as a sign of convergence between criminal profiteering and jihadist insurgency (Okunola & Ayodele, 2026). The capacity of the police to respond remains limited by size, funding, conditions of service and operational structure (Madueke, 2025), and the broader security situation has been described as fragile (Madueke, 2026).

The Legal and Media Setting

Security communication takes place within a mixed legal setting. The Constitution guarantees freedom of expression (s. 39) but allows laws that are reasonably justifiable in the interest of defence, public safety and public order (s. 45). The Official Secrets Act 1962 criminalises the unauthorised transmission of classified matter. The Freedom of Information Act 2011 establishes a right of access, qualified by exemptions for defence and law enforcement. The Cybercrimes (Prohibition, Prevention, etc.) Act, amended in 2024, has been used against journalists. Reporters Without Borders (2024) counted at least eight journalists prosecuted under the cybercrime law in the months after the amendment and argued that its Section 24 retained vague wording that allowed misuse. Nigeria ranked 112th of 180 countries in the 2026 World Press Freedom Index, an improvement of ten places but still within the "difficult" category ("Nigeria Ranked 112th," 2026). Journalists who report from conflict zones face threats from insurgents, the military and communities alike (Pate & Jibril, 2025). These conditions matter for the argument that follows. Any call for greater operational secrecy in Nigeria must take place against a background of real pressure on the press.

7. PATTERNS OF SECURITY DISCLOSURE IN NIGERIA

The analysis identified five recurring patterns through which security information reaches the public and potentially adversaries. They are summarised in Table 1 and discussed below.

Table 1. *Patterns of Security Disclosure in Nigeria and Their Possible Value to Adversaries*

Pattern	Illustrative case	Information revealed	Possible adversary use
Pre-announced operations and named targets	Relocation of defence leadership to Sokoto to pursue named bandit networks (2024); public foreign threats before strikes (2025)	Target, theatre and intensification of effort	Relocation, dispersal, preparation of defences
Publication of force locations and capabilities	Naming of new forward operating and patrol bases in Kwara and Niger States (2026); media tours of weapons	Positions, coverage gaps, equipment	Mapping of security presence; avoidance of patrolled areas
Unauthorised posts by personnel	Army warning on posts showing troop movements and locations (2026)	Movements, locations, morale	Tracking of units; propaganda
Media publication of classified material	Daily Trust report on planned operations and the 2019 raid; 2026 appeal to verify before publication	Plans, timing, intelligence	Anticipation of operations
Leakage through informants and meetings	Outcome of a Katsina security meeting reportedly relayed to a bandit within minutes (2026)	Decisions, timing, participants	Evasion; targeting of informants

Note. Cases are drawn from the sources cited in the text. Inclusion in the table does not imply that a disclosure caused a specific operational failure.

Pre-Announced Operations and Named Targets

The first pattern involves public announcements of forthcoming operations, often naming both the theatre and the target. In September 2024, the Federal Government ordered the Minister of State for Defence and the service chiefs to relocate to Sokoto State to intensify operations against bandits, with particular reference to networks led by Bello Turji (The ICIR, 2024). The Minister declared that time was up for the bandits and that increased operations would weaken all their bases (The ICIR, 2024). The move was widely reported. Seven months later, the Defence Headquarters was still promising to "fix an appointment" for Turji "with his maker" (Aleke, 2025). Public sources cannot show that the announcement itself allowed Turji to evade capture, and it would be wrong to claim so. What the episode does show is that the leadership publicly named the target, the theatre and the intensification of effort before results were achieved, giving a highly mobile adversary time to adjust.

Foreign actors have added a new dimension to this pattern. In November 2025, the United States President publicly threatened military action in Nigeria (Warner, 2025). When strikes on Islamic State-linked camps in Sokoto were carried out on 25 December 2025, they were announced by the President on social media and by United States Africa Command, while the United States defence secretary posted that there was "more to come" (Palmer & Oppel, 2025). Shortly afterwards, the Defence Headquarters reported that it had observed terrorist factions relocating to some communities in response to military pressure ("U.S. Strikes," 2026). Dispersal under pressure is an expected response to air strikes and should not be attributed to announcements alone. Still, weeks of public threats followed by public promises of further action told armed groups, in broad terms, what to expect.

Publication of Force Locations and Capabilities

The second pattern involves the disclosure of force dispositions and capabilities. The January 2026 statement on new forward operating bases and patrol bases in Kwara and Niger States, cited at the start of this article, named five specific locations along with the operations under way in the area ("Banditry: We'll Deepen Offensive," 2026). Individually, such details may seem harmless, since local residents can see a new base. Combined with other reporting, however, they help an adversary map where security forces are present and, by implication, where they are not. This is the mosaic effect in practice (Pozen, 2005).

Displays of capability raise a similar concern. Samuel Aruwan, a former commissioner for internal security in Kaduna State, has argued that military simulations, battle inoculation exercises and tours showcasing weapons sometimes dominate media coverage, although they should remain outside the public domain. In his view, the media space should be filled with successes against the enemy rather than displays of combat readiness or details

that may aid the adversary (Aruwan, 2026). The distinction he draws, between reporting results and advertising capabilities, is central to the framework proposed later in this article.

Unauthorised Disclosure by Personnel on Social Media

The third pattern arises from the personal use of social media by serving personnel. In July 2026, the Chief of Army Staff warned that posting operational information, military activities, troop movements, sensitive locations and other classified material would attract disciplinary measures including dismissal, because such posts compromise operational security and weaken discipline (FMINO, 2026). Commentary on the issue has noted that social media is both "a torchlight and a tripwire" for the armed forces (Okogba, 2026). It exposes alleged abuse and corruption, as in cases where personnel used TikTok to make complaints against superiors, but it also risks revealing troop movements, locations and equipment to adversaries (Okogba, 2026). This tension is important. A policy that treated all personnel posts as security breaches would silence legitimate grievances; a policy that ignored them would leave a steady stream of indicators in public view.

Media Publication of Classified Material

The fourth pattern concerns the publication of classified or sensitive material by the press. The best-known case is the military raid on the Daily Trust in January 2019, after the newspaper reported details of planned operations against Boko Haram. The army argued that the disclosure of classified information breached Sections 1 and 2 of the Official Secrets Act and could have warned the insurgents; after public criticism and presidential intervention, the troops withdrew from the newspaper's premises ("Nigeria Army Explains," 2019). The episode showed both the operational concern and the danger of a heavy-handed response.

More recent exchanges have taken a less confrontational form. In July 2026, the Director of Defence Information asked defence correspondents to verify any classified information with the appropriate authorities before publication, warning that disclosure could benefit terrorist groups ("DHQ Charges Media," 2026). At a separate meeting, the Director of Defence Media Operations told the correspondents that the press was "not our enemy" but a partner, while noting that some information could not be released immediately for reasons of operational security ("DHQ Worries," 2026). This language of partnership suggests a possible basis for agreed protocols, although it also carries the risk that "partnership" becomes a polite name for control.

Leakage Through Informant Networks and Security Meetings

The fifth pattern is the least visible and perhaps the most damaging. Much sensitive information does not reach adversaries through the media at all but through people. The Governor of Katsina State has complained that within five minutes of the end of a high-level security meeting, a notorious bandit had already been briefed on its outcome; he pointed to collaborators within communities rather than to the security forces (Aruwan, 2026). The abduction of schoolgirls in Maga, Kebbi State, in November 2025 raised related questions. The state governor said that troops deployed at the school had withdrawn shortly before the attack and asked who had authorised the withdrawal, and the Defence Headquarters opened an investigation ("Defence Headquarters Probes," 2025). The findings of that inquiry are not public, and no conclusion about leakage should be drawn from it. The case nonetheless shows how much depends on who knows where security forces are, and when.

This pattern carries an important lesson for the wider argument. Public debate in Nigeria often blames the press for security leaks. The evidence reviewed here suggests that official announcements, personnel behaviour and informal networks around security meetings may present equal or greater risks. A communication policy aimed only at journalists would miss much of the problem.

8. DISCUSSION: THE COSTS OF DISCLOSURE AND THE COSTS OF SILENCE

The five patterns point to a common mechanism. Disclosures that are specific about place, time and method, and that are made before or during an operation, give mobile adversaries the chance to anticipate state action, relocate, disperse or prepare. The theoretical model outlined earlier predicts this, and the concerns expressed by senior officers are consistent with it (FMINO, 2026; "DHQ Worries," 2026). Nigerian bandit groups, described as mobile and forest-based (Kleffmann & Ramachandran, 2024), are well placed to act on such information. It would be a mistake, however, to conclude that the answer is simply more secrecy. Secrecy has costs of its own, and in Nigeria at least four stand out.

First, silence creates a vacuum that others fill. The Defence Headquarters has expressed concern about hostile propaganda and about false narratives spread on social media ("DHQ Worries," 2026). Where official information is scarce or late, rumour, recycled videos and propaganda by armed groups can shape public perception more quickly than the state. Second, secrecy can erode the trust on which intelligence depends. A recent Nigerian study found that weak community trust constrains the flow of human intelligence, which is especially important in asymmetric conflict (Ohazulike & Okafor, 2026). Communities that feel ignored or misled are less likely to report what they see.

Third, secrecy can shield abuse and error. Human Rights Watch (2026) reports that a military air strike on Tungar Kara village in Zamfara State in January 2025 killed at least 20 people, including members of a community protection group, and it notes persistent gaps in accountability. The Kebbi case shows how public questioning by an elected governor can prompt an investigation ("Defence Headquarters Probes," 2025). Without disclosure and scrutiny, such cases might never be examined. Fourth, the language of security can be used against legitimate journalism. The prosecution of journalists under the cybercrime law (Reporters Without Borders, 2024) and the 2019 raid on the Daily Trust ("Nigeria Army Explains," 2019) show that claims of national security are not always made in good faith. Pozen's (2005) warning that mosaic reasoning can justify almost any withholding applies with force here.

The tension is therefore real, but it is narrower than it first appears. The research on transparency suggests that the public gains most from explanations of purpose and rationale, not from procedural detail (Clubb et al., 2025). Adversaries, by contrast, gain most from procedural and tactical detail: where forces are, when they will move and how they operate. These are largely different categories of information. The declaration of a national security emergency in November 2025 illustrates the point. It announced policy measures, including the recruitment of additional police officers, the deployment of trained forest guards and the redeployment of police withdrawn from protecting prominent individuals, without disclosing locations or timelines (State House, 2025). That kind of statement communicates resolve, in Schelling's (1966) sense, without handing adversaries a plan.

A fair assessment should also recognise that advance announcement is sometimes deliberate. Where the aim is to push armed groups out of an area, to encourage surrender or to warn civilians, signalling in advance may be rational, and it fits the logic of coercion described by Schelling (1966). The difficulty is that displacement tends to move violence rather than end it. In January 2026, the Defence Headquarters itself reported measures to stop fleeing terrorists from migrating into and infiltrating communities elsewhere ("U.S. Strikes," 2026). Advance signalling may therefore be justified in particular cases, but it should be a considered choice made at the planning stage, not the unplanned result of a press conference.

Two features of the Nigerian setting sharpen this problem. The first is the number of voices. Federal ministers, state governors, service chiefs, theatre and brigade commanders, police commands and community security outfits all speak publicly about operations, often without a shared view of what should be protected. The coordination deficits identified in Sokoto (Okunola & Ayodele, 2026) appear to extend to communication. When many actors speak, the combined picture available to an adversary may be far more detailed than any single statement suggests, which is precisely the risk described by mosaic theory (Pozen, 2005). The second feature is speed. Statements are now shared on social media within minutes, and the Katsina example suggests that information from closed meetings can travel just as fast (Aruwan, 2026). The window between an announcement and the moment when an adversary can act on it has narrowed sharply.

Time is the other key variable. Operational information loses value to adversaries once an operation is complete. Results can therefore be reported fully after the event without the risks attached to advance notice, provided that sources, methods and continuing operations are protected. Much of the risk identified in this study arises from reversing this sequence: announcing intentions and deployments in detail at the start, and reporting outcomes vaguely or not at all.

9. TOWARDS A STRATEGIC FRAMEWORK FOR SECURITY COMMUNICATION

Building on this analysis, the article proposes a tiered security communication framework. It sorts information into four tiers according to its value to the public and its likely value to adversaries, and it attaches a default handling rule to each (Table 2).

Table 2. *A Tiered Framework for Security Communication in Nigeria*

Tier	Type of information	Default handling	Purpose
1. Open	Policy, strategic intent, legal changes, resources committed, public safety advice, aggregate results	Release proactively and regularly	Reassurance, deterrence, accountability
2. Delayed	Results of specific operations, rescues, arrests, names of completed operations	Release after completion and once personnel and victims are safe	Accountability and trust without advance warning
3. Generalised	Unit locations, force levels, equipment and capabilities	Release only at state or theatre level, without specific sites	Visibility of effort without mapping the force
4. Protected	Future timing and targets, troop movements, sources and methods, informant identities, surveillance capabilities	Withhold from public; brief oversight bodies in closed session	Operational effectiveness and protection of sources

Note. Handling rules are defaults. The public interest test in Section 11(2) of the Freedom of Information Act 2011 should apply where withholding would conceal wrongdoing.

The framework would need institutional support to work. Six measures follow from the analysis.

First, each major operation should have a written list of critical information, prepared at the planning stage, that identifies what must not be disclosed and by whom. This reflects standard OPSEC practice (Department of Defense, 2020) and gives spokespersons a clear reference point. Second, security communication should be coordinated through a single centre, linking the Defence Headquarters, the police, the intelligence services and the Office of the National Security Adviser, so that ministers, governors and commanders do not make conflicting or overly detailed statements. Political office holders make many of the most detailed announcements and should receive basic OPSEC training.

Third, the partnership between the Defence Headquarters and defence correspondents could be formalised in a written protocol. Such a protocol might provide for verification before publication, short embargoes on operational details, and timely release of results, together with an explicit guarantee that journalists will not face prosecution or raids for reporting matters of public interest. Fourth, the social media policy for personnel should combine clear OPSEC rules with confidential channels for complaints, so that discipline does not become a means of silencing whistle-blowers (Okogba, 2026).

Fifth, secrecy should be matched by oversight. Defence and security committees of the National Assembly could receive classified briefings in closed session, and the public interest override in Section 11(2) of the Freedom of Information Act should be applied in good faith. Withholding operational detail from the public is easier to justify when elected representatives can examine it. Sixth, access to security meetings should follow the principle of need-to-know. The Katsina experience suggests that broad attendance at security meetings, however well intended for community engagement, can itself become a channel of leakage (Aruwan, 2026). Engagement with communities remains essential, but it can focus on sharing results and gathering information rather than discussing plans.

Finally, legal reform would strengthen the framework's legitimacy. Narrowing the vague wording in Section 24 of the cybercrime law, as critics have urged (Reporters Without Borders, 2024), would reduce the risk that security claims are used to punish legitimate reporting. A framework that protects operations while leaving journalists exposed to arbitrary prosecution would lose public trust and, with it, much of its value.

10. CONCLUSION

This article has examined the public disclosure of security information in Nigeria and its implications for intelligence, operational effectiveness and national security. The evidence reviewed suggests that the risks do not arise from communication as such. They arise from specific disclosures, made at the wrong time and in too much detail: naming targets and theatres before operations begin, publicising the locations of bases and the details of capabilities, careless posts by personnel, the publication of classified plans, and informal leakage around security meetings. For mobile armed groups, such information has immediate value.

The analysis also shows that silence is not a safe alternative. Excessive secrecy leaves space for hostile propaganda, weakens the trust on which human intelligence depends, shields abuses and can be turned against the press. The task, then, is to decide what to disclose, when and how. The tiered framework proposed here offers one way of doing so. It asks Nigerian authorities to explain purpose and report results openly, to delay or generalise operational detail, and to protect sources, methods and plans, while giving Parliament and the courts the means to check that secrecy is not abused. Future research could test these propositions more directly, for instance through interviews with security officials and journalists, or through systematic comparison of announcements with subsequent patterns of violence. What already seems clear is that in a conflict against adversaries who listen closely, the state should speak openly about why it acts and what it has achieved, and speak far less about where and how it will act next.

DECLARATIONS

Funding

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Conflict of Interest

The author(s) declare no conflict of interest.

Data Availability Statement

No new data were created or analysed in this study. All documentary sources are cited in the reference list.

REFERENCES

Africa Defense Forum. (2026, July). *Nigeria's banditry crisis worsens*. https://adf-magazine.com/2026/07/nigerias-banditry-crisis-worsens/

Aleke, L. (2025, April 4). Your days are numbered, military tells notorious bandit leader, Bello Turji. *ThisDay*. https://www.thisdaylive.com/2025/04/04/your-days-are-numbered-military-tells-notorious-bandit-leader-bello-turji/

Aruwan, S. (2026, May 20). Inside the informant networks undermining Nigeria's anti-banditry campaign. *Premium Times*. https://www.premiumtimesng.com/opinion/881202-inside-the-informant-networks-undermining-nigerias-anti-banditry-campaign-by-samuel-aruwan.html

Banditry: We'll deepen offensive in Kwara, Oyo, Niger – Army commander. (2026, January 11). *Daily Trust*. https://allafrica.com/stories/202601130335.html

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Clubb, G., Davies, G., & Kobayashi, Y. (2025). Transparent communication in counter-terrorism policy: Does transparency increase public support and trust in terrorism prevention programmes? *Terrorism and Political Violence, 37*(4), 531–549. https://doi.org/10.1080/09546553.2024.2322489

Constitution of the Federal Republic of Nigeria 1999 (as amended).

Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024 (Nigeria).

Defence Headquarters probes sudden withdrawal of soldiers before Kebbi school abduction. (2025, November 29). *Sahara Reporters*. https://saharareporters.com/2025/11/29/defence-headquarters-probes-sudden-withdrawal-soldiers-kebbi-school-abduction

Department of Defense. (2020). *DoD Directive 5205.02E: DoD operations security (OPSEC) program* (Incorporating Change 2). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520502e.pdf

DHQ charges media against publishing classified military information. (2026, July). *Sonic Realtime*. https://www.sonicrealtime.ng/2026/07/dhq-charges-media-against-publishing.html

DHQ worries over hostile propaganda, declares social media fuels misinformation. (2026, July 2). *ThisDay*. https://www.thisdaylive.com/2026/07/02/dhq-worries-over-hostile-propaganda-declares-social-media-fuels-misinformation/

Federal Ministry of Information and National Orientation. (2026, July). *COAS warns soldiers against social media misuse, seeks greater South-East recruitment as Otti commends military expansion*. https://fmino.gov.ng/coas-warns-soldiers-against-social-media-misuse-seeks-greater-south-east-recruitment-as-otti-commends-military-expansion/

Fraise, T. (2025). Nuclearization and de-democratization: Security, secrecy, and the French pursuit of nuclear weapons (1945–1974). *European Journal of International Relations, 31*(1), 203–226. https://doi.org/10.1177/13540661241301648

Freedom of Information Act 2011 (Nigeria).

Human Rights Watch. (2026). *World report 2026: Nigeria*. https://www.hrw.org/world-report/2026/country-chapters/nigeria

Institute for Economics & Peace. (2026). *Global Terrorism Index 2026: Measuring the impact of terrorism*. https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf

Jatula, V. (2025). Revisiting press freedom in Nigeria: The Buhari years (2015–2023). *Journal of Central and Eastern European African Studies, 5*(2), 173–195. https://doi.org/10.12700/jceeas.2025.5.2.375

Kleffmann, J., & Ramachandran, S. (2024). *Banditry violence in Nigeria's North West: Insights from affected communities*. United Nations Institute for Disarmament Research. https://doi.org/10.37559/meac/24/05

Lampe, H., Herschinger, E., Nitzl, C., & Willems, J. (2025). Predicting novel terrorism: Media coverage as early-warning system of novelty in terror attacks. *Terrorism and Political Violence, 37*(5), 610–631. https://doi.org/10.1080/09546553.2024.2345729

Lubrano, M. (2024). Choosing what (not) to do next: A preliminary theoretical framework on strategic innovation in terrorist organizations. *Dynamics of Asymmetric Conflict, 17*(1), 1–22. https://doi.org/10.1080/17467586.2023.2280929

Madueke, O. (2025). Why the Nigeria police struggles to tackle banditry in Nigeria. *The Round Table, 114*(4), 436–450. https://doi.org/10.1080/00358533.2025.2518321

Madueke, O. (2026). Why should we worry about Nigeria's fragile security? *The Political Quarterly, 97*(1), 108–117. https://doi.org/10.1111/1467-923X.70010

Makridis, C., Maschmeyer, L., & Smeets, M. (2024). If it bleeps it leads? Media coverage on cyber conflict and misperception. *Journal of Peace Research, 61*(1), 72–86. https://doi.org/10.1177/00223433231220264

Neal, A. W. (2026). After Nord Stream: Four security dilemmas in critical maritime infrastructure protection. *International Affairs, 102*(1), 207–225. https://doi.org/10.1093/ia/iiaf229

Nigeria army explains media raid over classified info publication. (2019, January 7). *Africanews*. https://www.africanews.com/2019/01/07/nigeria-army-explains-media-raid-over-classified-info-publication/

Nigeria ranked 112th in 2026 press freedom index, up 10 places but still in "difficult category". (2026, April 30). *TheCable*. https://www.thecable.ng/nigeria-ranked-112th-in-2026-press-freedom-index-up-10-places-but-still-in-difficult-category/

Nigeria's kidnap crisis: 7,825 abducted, ₦7.78bn ransom paid in one year. (2026, August 28). *The Guardian* (Nigeria). https://guardian.ng/news/nigerias-kidnap-crisis-7825-abducted-%E2%82%A67-78bn-ransom-paid-in-one-year/

Official Secrets Act 1962 (Nigeria).

Ohazulike, G. A., & Okafor, Q. N. (2026). Roles and effectiveness of intelligence gathering in the maintenance of security in Nigeria. *Global South Social Sciences Digest, 3*(1), 37–51. https://www.nigerianjournalsonline.org/index.php/GSSSD/article/download/4300/4028/7780

Okogba, E. (2026, August 26). Armed forces personnel and social media exposure. *Vanguard*. https://www.vanguardngr.com/2026/08/armed-forces-personnel-and-social-media-exposure/

Okunola, R., & Ayodele, A. (2026). Sovereignty under siege: State response, fragility and the political ecology of banditry in Sokoto, Nigeria. *Small Wars & Insurgencies, 37*(7), 1700–1737. https://doi.org/10.1080/09592318.2026.2661937

Palmer, A., & Oppel, E. (2025, December 26). *Why did the United States conduct strikes in Nigeria?* Center for Strategic and International Studies. https://www.csis.org/analysis/why-did-united-states-conduct-strikes-nigeria

Pate, U. A., & Jibril, A. (2025). Insurgency in northeast Nigeria: Are journalists safe to report? *Journalism, 26*(6), 1288–1306. https://doi.org/10.1177/14648849241245203

Pozen, D. E. (2005). The mosaic theory, national security, and the Freedom of Information Act. *Yale Law Journal, 115*(3), 628–679.

Reporters Without Borders. (2024, September 9). *Nigeria: At least eight journalists prosecuted under cybercrime law despite new amendment*. https://rsf.org/en/nigeria-least-eight-journalists-prosecuted-under-cybercrime-law-despite-new-amendment

Rice, C., & Innes, M. (2025). Counter-terrorism strategic communication campaigns and the generative nature of trust. *International Journal of Strategic Communication, 19*(5), 624–650. https://doi.org/10.1080/1553118X.2025.2501558

Schelling, T. C. (1966). *Arms and influence*. Yale University Press.

Schrijver, P. (2026). Ukrainian intelligence's use of Telegram in wartime. *International Journal of Intelligence and CounterIntelligence, 39*(4), 981–1007. https://doi.org/10.1080/08850607.2025.2522222

State House. (2025, November 26). *President Tinubu declares a security emergency, orders army, police to recruit more personnel*. https://statehouse.gov.ng/president-tinubu-declares-a-security-emergency-orders-army-police-to-recruit-more-personnel/

The ICIR. (2024, September 1). *FG orders Matawalle, military chiefs to relocate to Sokoto to combat insecurity*. https://www.icirnigeria.org/fg-orders-matawalle-military-chiefs-to-relocate-to-sokoto-to-combat-insecurity/

U.S. strikes: Defence Headquarters moves against fleeing terrorists. (2026, January 3). *Leadership*. https://allafrica.com/stories/202601030125.html

Warner, L. A. (2025, November 14). The political theater behind Trump's "guns-a-blazing" Nigeria threat. *Just Security*. https://www.justsecurity.org/124725/trump-nigeria-military-threat/