

EMERGING TRENDS IN WARFARE AND THEIR IMPLICATIONS FOR NIGERIA'S NATIONAL SECURITY ARCHITECTURE

By

AVM Emmanuel Ogbonnaya Chukwu PhD

Directing Staff, National Defence College

Abuja

chukwueo2000@yahoo.com

Abstract

The rapid evolution of global conflict dynamics in the twenty-first century has reshaped the character, conduct, and complexity of warfare, compelling states to rethink and recalibrate their security frameworks. This article examines the emerging trends in contemporary warfare, ranging from cyber conflict/information manipulation, autonomous/unmanned systems and hybrid warfare, and analyzes their implications for Nigeria's national security architecture. Drawing on recent security developments within and beyond Nigeria, the study interrogates how these trends expose structural vulnerabilities in the country's defence, intelligence, and law enforcement institutions. It further assesses the adequacy of Nigeria's current security strategies in anticipating, preventing, and responding to evolving threats, especially in the context of porous borders, asymmetric conflicts, and socio-political fragilities. The article argues that Nigeria's national security framework must transition from a predominantly conventional, reactive model to a technologically enabled, intelligence-driven, and multi-dimensional system. It concludes by proposing policies for strengthening national resilience, enhancing inter-agency cooperation, deepening regional security partnerships, and modernizing defence capabilities to effectively confront the realities of modern warfare.

Introduction

The nature of warfare in the 21st century has significantly changed. Traditional battles between armies on defined battlefields are being replaced by more complex threats that are dynamic, decentralized, and often difficult to detect using conventional military approaches. These modern threats span physical, digital, and psychological domains. Cyber-attacks, drone warfare, hybrid tactics, and proxy conflicts now define the landscape of war. Both state and non-state actors use advanced technologies, misinformation, and irregular strategies to undermine national and regional security systems.¹ These developments represent emerging trends in warfare, as they are shaped by rapid technological advancements, increased involvement of non-state actors, and a shift toward non-kinetic forms of conflict. These emerging forms of warfare are difficult to detect, prevent, and counter, which makes them a serious threat to national security. In this context, national security refers to a country's capacity to safeguard its people, territory, and vital institutions from both internal and external threats.

In Ukraine, the ongoing war with Russia demonstrates how cyber warfare, drone strikes, and information manipulation have become central to military operations.² The war, which began in 2014 and escalated in 2022, has seen the extensive use of drones for reconnaissance and targeted strikes, cyber-attacks on critical infrastructure, and disinformation campaigns, all of which have severely disrupted government functions, weakened public morale, and exposed vulnerabilities in national defense systems.³ On the flipside, the United States (US) and China are increasing investments in artificial intelligence (AI), space-based defense, and electromagnetic warfare to gain technological superiority and global strategic advantage.⁴ Much of the raw materials required for these technologies, such as rare earth minerals, lithium, and cobalt are sourced from African countries, making the continent a vital resource base in their competition.⁵

While Africa remains a strategic battleground for foreign influence, particularly in the ongoing competition between global powers through economic agreements, military alliances, and covert operations,⁶ it is simultaneously exposed to a range of emerging threats that complicate its security landscape. Transnational terrorism, organized crime, human and organ trafficking, and the activities of foreign mercenaries have increasingly blurred the boundaries between war and peace, as well as between military and civilian life, creating a complex and volatile environment that undermines both national and regional security.⁷ In Mali, for instance, jihadist insurgencies have overwhelmed the national military, forcing reliance on costly private military contractors such as the Wagner Group reportedly at a cost of around US \$120 million annually, thereby weakening state authority and eroding public confidence.⁸ In Libya, over a decade of conflict has inflicted severe economic damage, with terrorism alone costing the country about US \$500 million annually, while the broader war has reduced economic potential by an estimated US \$174 billion.⁹ These financial and security challenges have spilled across borders, fueling arms proliferation, triggering mass displacement, and enabling the spread of violent extremist networks throughout the Sahel and North African regions

Nigeria, like many African countries, is being affected by these new trends in warfare. The country is facing multiple security threats that range from terrorism and banditry to cybercrime and maritime insecurity. These threats are evolving rapidly, making it difficult for existing security institutions to keep pace. While the Nigerian state has focused much of its resources on counterinsurgency operations against Boko Haram and ISWAP, other areas such as cyber defense, drone surveillance, and civil-military coordination seem to remain weak or underdeveloped.¹⁰ It is important to state that Nigeria's national security architecture is largely structured around traditional threats and territorial defense. It includes the Armed Forces of Nigeria (AFN), the Nigeria Police Force (NPF), the Department of State Services (DSS), and other paramilitary agencies. However, the emergence of non-traditional threats demands a shift in orientation and capability. Nigeria is still grappling with setting up a central cybersecurity command that can coordinate responses to digital threats. Aside that, the AFN is yet to integrate AI, data analytics, or autonomous systems into their operational strategies. Importantly, hybrid threats require interagency

collaboration, which the security agencies lack because they most often operate in silos. In view of the foregoing, this paper seeks to examine how these emerging trends in warfare are impacting Nigeria's national security architecture. The paper will evaluate the readiness of Nigeria's security institutions to respond to modern threats and explores opportunities for reform and innovation.

Conceptual clarification and Theoretical Framework

Understanding the dynamics of modern conflict and security management in Nigeria requires a clear conceptual grounding. Key concepts central to this study include emerging warfare, national security architecture, and hybrid warfare. Each of these terms captures critical dimensions of contemporary threats and the corresponding responses that states are developing or must develop in the face of evolving challenges.

Conceptual Clarification

Emerging Warfare

Emerging warfare refers to novel forms of conflict shaped by technological innovation, shifting geopolitical dynamics, and evolving strategies by both state and non-state actors. Kaspersen defines emerging warfare as "the transformation of the character of war through advancements in science and technology, resulting in new methods of attack, such as cyber warfare, autonomous weapon systems, and artificial intelligence-driven operations."¹¹ Similarly, Singer and Brooking describe it as "the use of unconventional tools and platforms that blur the traditional boundaries between combatants and civilians, peace and war, and physical and virtual domains."¹² For the purpose of this study, Kaspersen's definition is adopted because it underscores the role of technological disruptions, which are central to understanding Nigeria's contemporary security environment. This focus allows the research to examine how innovations such as drone surveillance, AI-powered analytics, and cyberattacks are reshaping conflict dynamics and national security responses.

National Security Architecture

National security architecture encompasses the organizational, legal, institutional, and operational arrangements a state employs to safeguard its sovereignty, citizens, and strategic interests. Ogbonnaya and Ehugbo define it as "the framework of institutions, strategies, and operations designed to defend a nation from both internal and external threats."¹³ Alemika, however, offers a broader perspective, describing it as "a country's integrated system of actors, processes, and instruments designed to anticipate, manage, and neutralize threats to its national interests."¹⁴ This study adopts Alemika's definition as it captures the anticipatory and integrative dimensions critical to national security management in fragile and complex environments such as Nigeria. In particular, it aligns with the need for a multi-agency, adaptive security framework capable of responding to asymmetric threats and hybrid tactics.

Hybrid Warfare

Hybrid warfare is a military and political strategy that combines conventional and unconventional methods, often implemented by both state and non-state actors, to achieve strategic objectives without triggering full-scale war. Hoffman defines it as “a military strategy that employs political warfare and blends conventional warfare, irregular warfare, cyber warfare, and influence operations.”¹⁵ Murray and Mansoor offer a complementary view, characterizing it as “a multi-modal form of conflict in which the adversary uses a mix of kinetic and non-kinetic tools, including propaganda, proxy forces, economic pressure, and disinformation, to undermine state authority.”¹⁶ This study adopts Hoffman’s definition as it clearly articulates the strategic blending of diverse conflict tools that resonate with Nigeria’s current security challenges. The country faces simultaneous threats from insurgents, transnational actors, and digital misinformation campaigns, all of which fall within the spectrum of hybrid conflict.

Nexus among the Concepts

Emerging warfare offers the technological and strategic innovations that serve as enablers for hybrid conflict. Hybrid warfare, in turn, places unique demands on a nation’s security architecture, testing its ability to respond to non-linear, multi-dimensional threats. In Nigeria, the increasing deployment of drones, cyber capabilities, and disinformation tactics by both insurgent groups and foreign actors reveals the gaps in its current security framework and underscores the need for a comprehensive and adaptive national security architecture. The interplay of these concepts highlights the urgency for Nigeria to recalibrate its defence policies and invest in technologies that can counter asymmetric threats. Without such strategic alignment, the country risks further erosion of state authority, territorial integrity, and public trust.

Theoretical Framework

Three theoretical lenses have been considered in this paper. They are Realism, Asymmetric Conflict Theory, and Security Sector Reform (SSR). Realism posits that international relations are driven by the pursuit of power and the anarchic nature of the international system. States, as rational actors, act primarily to secure their survival and maximize their influence.¹⁷ Realism helps explain the behavior of powerful states such as the United States and China as they invest in emerging technologies and project power through proxies and technological superiority. Asymmetric Conflict Theory focuses on conflicts where belligerents have significantly unequal military capabilities, leading the weaker actor to adopt unconventional or irregular methods of warfare. This theory is particularly useful in explaining the strategies employed by insurgent groups in Nigeria and elsewhere who resort to cyberattacks, guerrilla tactics, or disinformation in response to the conventional superiority of the state.¹⁸

SSR is both a conceptual and practical framework aimed at transforming the institutions responsible for security such as the military, police, and intelligence

services so they become more effective, accountable, and aligned with democratic norms and rule of law.¹⁹ SSR is particularly relevant in fragile states facing internal conflicts, systemic corruption, and institutional weaknesses. While all three theoretical frameworks offer valuable insights, this study adopts Asymmetric Conflict Theory due to its analytical power in understanding the strategic behavior of weaker actors in technologically complex and uneven battlefields. Originating from the work of military strategists and political scientists, the theory gained prominence through the writings of Arreguín-Toft²⁰ who examined how weaker actors often prevail in conflicts by avoiding the strengths of their opponents and exploiting vulnerabilities through irregular methods.

This theory has been applied in the analysis of insurgencies in Afghanistan, Iraq, and Somalia, and is equally applicable to the Nigerian context, where insurgent groups like Boko Haram and ISWAP adopt asymmetric strategies ranging from suicide bombings to cyber propaganda to challenge the state. Its strength lies in its capacity to explain how technologically or militarily inferior actors can remain resilient or even succeed in prolonged conflict. However, a key limitation of the theory is its insufficient attention to the structural and institutional reforms needed to address root causes of insecurity, an area where SSR becomes complementary. Additionally, it is essential to integrate this theoretical framework with complementary frameworks that address its blind spots particularly by incorporating human security and governance perspectives to ensure a more holistic response to Nigeria's complex security threats.

Overview of Nigeria's National Security Architecture

Nigeria's national security architecture comprises a complex web of institutions, legal frameworks, and strategic actors mandated to protect the state's sovereignty, territorial integrity, and citizens. This architecture is structured around key security institutions including the AFN, the NPF, DSS, the Nigeria Security and Civil Defence Corps (NSCDC), and other paramilitary bodies. At the apex of the security hierarchy is the National Security Council (NSC), chaired by the President and including service chiefs, the National Security Adviser (NSA), the Minister of Defence, and other high-ranking officials. The Office of the National Security Adviser (ONSA) plays a central role in coordinating inter-agency collaboration, intelligence fusion, and policy direction across Nigeria's security landscape.

The AFN consist of the Nigeria Army (NA), Nigeria Navy (NN), and Nigeria Air Force (NAF), with the NA being the largest and most actively engaged in internal security operations across the six geopolitical zones. As of 2023, Nigeria's active military personnel numbered approximately 223,000, while the paramilitary police force had a workforce of over 370,000 officers.²¹ The DSS, which evolved from the National Security Organization (NSO), handles counterintelligence and domestic surveillance. Alongside these, the NSCDC focuses on protecting critical national infrastructure and supporting internal security during civil disturbances.

The legal foundation of Nigeria's national security framework is enshrined in several core documents. The Constitution of the Federal Republic of Nigeria 1999 is the supreme legal reference, particularly Section 14(2)(b), which states that "the security and welfare of the people shall be the primary purpose of government."²² Complementary legislation includes the Armed Forces Act (2004), the Nigeria Police Act (2020), the National Security Agencies Act (1986), and the Terrorism (Prevention and Prohibition) Act (2022). These legal instruments provide the statutory mandates for the establishment, powers, and operational scope of the various agencies within the national security system. Institutionally, Nigeria's security framework is often criticized for fragmentation, lack of coordination, and over-reliance on kinetic responses. Despite the existence of multi-agency platforms such as the Joint Task Forces (e.g., Operation Hadin Kai in the Northeast), interoperability challenges persist. Intelligence sharing remains weak, and bureaucratic competition undermines operational synergy. For instance, while the Defence Intelligence Agency (DIA), DSS, and National Intelligence Agency (NIA) have overlapping mandates, they often function in silos, thereby limiting the nation's early warning and strategic threat analysis capabilities.²³

Nigeria's national security objectives are anchored in four core imperatives: maintaining internal stability, defending against external aggression, safeguarding critical infrastructure, and ensuring the protection of lives and property. These objectives are pursued through a broad spectrum of stakeholders, including the executive arm of government, the armed forces (Army, Navy, Air Force), the Nigeria Police Force, the Department of State Services (DSS), the Nigeria Security and Civil Defence Corps (NSCDC), and other paramilitary agencies. State and local governments, traditional institutions, civil society organizations, and increasingly, non-state actors such as private security firms and community-based vigilante groups also play key roles. Due to overstretched federal security forces, NSAs and localized security outfits have emerged as vital components of Nigeria's fragmented security landscape. These include the Amotekun Corps in the Southwest, Civilian Joint Task Force (CJTF) in the Northeast, Ebube Agu in the Southeast, Yan Sakai vigilantes in the Northwest, Hisbah religious police in parts of the North, and Benue Livestock Guards in the Middle Belt. While many of these groups fill critical security vacuums, some operate outside formal regulatory frameworks, undermining national security by engaging in extrajudicial actions, ethnic profiling, or clashing with federal forces.

Nigeria continues to face multidimensional security threats that are evolving in scale, tactics, and geography. According to SBM Intelligence,²⁴ more than 10,000 people were killed and over 3,000 abducted in violent incidents across the country in 2023 alone. Terrorism by Boko Haram and ISWAP persists in the Northeast, while the Northwest battles escalating banditry and mass kidnappings. The Middle Belt remains plagued by deadly farmer-herder conflicts, and the Southeast is increasingly affected by separatist violence and targeted attacks. Simultaneously, piracy and illegal oil bunkering challenge security in the Niger Delta and Gulf of Guinea. These threats are compounded by porous borders, corruption, youth unemployment, arms proliferation, and a weak criminal justice system.

To respond, the Federal Government has instituted several policy frameworks, including the National Counter-Terrorism Strategy (NACTEST) and the revised National Security Strategy.²⁵ While these frameworks demonstrate an awareness of Nigeria's evolving threat environment, implementation has often lagged behind policy intent. Moreover, the country's national security apparatus remains heavily centralized, reactive, and structurally unprepared for emerging forms of warfare that rely on cyber tools, drone surveillance, digital propaganda, and hybrid operations—characteristics of the evolving global security ecosystem. From a theoretical perspective, the Asymmetric Conflict Theory is particularly useful in understanding Nigeria's complex security landscape. Asymmetric threats—posed by insurgents, vigilantes, and transnational criminal networks—challenge the conventional military doctrines that Nigeria's security sector was designed around. This theory explains why traditional force-on-force strategies are insufficient in combating adversaries who blend into civilian populations, use low-cost technologies, and operate without defined borders or formal structures. The hybrid tactics employed by such actors further test the effectiveness of Nigeria's centralized command structure and reactive posture.

Mapping Emerging Trends in Warfare

Contemporary conflicts are increasingly shaped by technological advancements and unconventional tactics that transcend traditional battlefield confrontations. One of the most significant trends is cyberwarfare and information operations, which have become essential tools for both state and NSAs. Cyberattacks target critical infrastructure, disrupt governance, and erode public trust. In Nigeria, the National Information Technology Development Agency (NITDA) reported a 70% increase in cyberattacks targeting government institutions and financial platforms between 2020 and 2023, particularly during electoral cycles and periods of civil unrest.²⁶ In 2023 alone, the Nigerian Communications Commission (NCC) warned of over 13 million malware attacks within the country, most originating from phishing and ransomware targeting public and private databases.²⁷ Moreover, the spread of misinformation and hate speech on social media platforms especially during elections and crisis periods continues to deepen political and ethnic divisions, undermining democratic stability.

The rise of drones and autonomous weapon systems has also transformed the landscape of armed conflict. These tools, previously exclusive to advanced militaries, are now accessible to insurgents, militias, and even criminal gangs. In Nigeria's Northeast, Boko Haram and ISWAP have reportedly deployed commercial drones for reconnaissance and battlefield coordination.²⁸ On the government side, the Nigerian Air Force has increased its use of Unmanned Aerial Vehicles (UAVs) for surveillance and targeted strikes, though limited infrastructure and technical capacity hinder sustained operations. Globally, the use of Turkish Bayraktar drones in Libya and Azerbaijan, and U.S. drone operations in the Middle East, illustrate the strategic advantage that unmanned systems confer in asymmetric conflicts.

AI and surveillance technologies are increasingly being leveraged to manage internal threats and maintain public order. AI-powered facial recognition and predictive policing algorithms have been deployed in countries like China, India, and South Africa, raising both efficacy and ethical concerns. In Nigeria, surveillance initiatives such as the Smart City project in Lagos and Abuja's Safe City infrastructure seek to harness AI and CCTV technologies to monitor urban crime and civil disturbances. However, data privacy, poor inter-agency coordination, and underdeveloped AI governance frameworks limit their effectiveness. As these tools become more entrenched, they introduce new vulnerabilities, including algorithmic bias and misuse by authoritarian elements within the state.

Hybrid and proxy warfare represent another dimension of modern conflict, blending conventional combat with irregular tactics such as disinformation, economic sabotage, and the use of mercenaries. Nigeria's security environment increasingly reflects this reality. The activities of foreign actors—ranging from arms smuggling by transnational cartels to ideological and material support for separatist groups—suggest elements of proxy engagement. For instance, reports indicate that ISWAP maintains logistical ties with international jihadist networks in the Sahel, while secessionist groups in the Southeast have benefited from financial and media support from diasporic sources.²⁹ These complex affiliations challenge traditional security responses and highlight the need for adaptive strategies.

The persistence of insurgency and non-state armed groups in Nigeria further illustrates the evolving face of warfare. Groups such as Boko Haram, ISWAP, and bandit networks in the Northwest operate with increasing sophistication—often mimicking state functions in territories they control, such as taxation, judicial rulings, and social service delivery. According to SBM Intelligence, more than 3,000 communities in the North have been displaced by armed groups, with over 2.5 million internally displaced persons (IDPs) as of late 2023.³⁰ The Nigerian state's inability to monopolize the use of force across its territory affirms Asymmetric Conflict Theory's relevance: where non-state actors use unconventional methods to exhaust a superior but rigid state apparatus.

Comparative insights from global case studies reinforce the magnitude of these emerging threats. In Ukraine, hybrid tactics—ranging from cyberattacks on power grids to drone surveillance and propaganda warfare—have defined Russia's strategy since 2014.³¹ In Ethiopia's Tigray conflict, both government forces and rebels used drones for airstrikes, while internet blackouts and information control shaped public perception. In Myanmar, the military junta's deployment of facial recognition and surveillance software, supported by Chinese firms, has enabled mass crackdowns on dissenters. These cases emphasize how warfare is no longer limited to battlefields but is embedded in digital spaces, civil governance, and psychological domains.

For Nigeria, these global and domestic trends reveal deep vulnerabilities in its national security architecture. Realism underscores the centrality of state power and sovereignty, but these must now be expressed through technological adaptability

and intelligence superiority. Asymmetric Conflict Theory helps explain the endurance of insurgent groups exploiting state weaknesses, while Security Sector Reform (SSR) provides a lens for institutional transformation. Together, they suggest that Nigeria must recalibrate its security posture—investing in cyber defense, drone capabilities, AI governance, and intelligence-led policing—to address the complex challenges of 21st-century warfare.

Manifestation of Emerging Warfare Trends in Nigeria

Emerging trends in warfare have increasingly shaped Nigeria's security landscape, with violent non-state actors adapting their methods in response to technological advancements and gaps within the national security architecture. Groups such as Boko Haram and its splinter faction, the Islamic State West Africa Province (ISWAP), have evolved from traditional guerrilla-style ambushes into more sophisticated asymmetric warfare strategies. These groups now exhibit increased tactical precision, using hit-and-run attacks, vehicle-borne improvised explosive devices (VBIEDs), and coordinated raids on military formations and soft targets. ISWAP, in particular, has adopted a quasi-governance structure in parts of the Lake Chad Basin, leveraging local grievances and religious ideology to maintain control and legitimacy among some populations.

A notable shift has been the reported use of drones and rudimentary surveillance technologies by NSAs. While these drones are not as technologically advanced as those used by formal militaries, their deployment for reconnaissance purposes in conflict zones such as Borno, Yobe, and Katsina suggests a rising sophistication among insurgent and bandit groups.³² These tools allow for the monitoring of troop movement and the identification of soft targets, further eroding the state's tactical advantage. Digital radicalization and online recruitment have become central to extremist strategies in Nigeria. Boko Haram and ISWAP exploit social media platforms, encrypted messaging apps, and locally adapted propaganda materials to indoctrinate and recruit young Nigerians, particularly those in underserved or marginalised communities. According to a 2023 report by the Tony Blair Institute, digital platforms were found to contribute to the recruitment of at least 18% of new Boko Haram recruits in northeastern Nigeria, reflecting a worrying trend of cyber-enabled extremism.

Foreign influence and proxy dynamics have also been observed in Nigeria's security environment, especially within the broader Sahel and Lake Chad Basin regions. International jihadist networks such as ISIS and Al-Qaeda have provided ideological and logistical support to local franchises like ISWAP and Jama'at Nasr al-Islam wal Muslimin (JNIM). The porous borders shared with Niger, Chad, and Cameroon enable the flow of fighters, weapons, and intelligence, turning Nigeria into a frontline state in a much larger transnational conflict. Moreover, competition among global powers for strategic influence in the Sahel often leads to conflicting interests, which can undermine cohesive security responses in the region. Threats to critical national infrastructure have also become more frequent and calculated.

Attacks on oil pipelines, power installations, and telecommunications towers—particularly in the Niger Delta, Northcentral, and Northwestern zones—are not only economically damaging but also strategically disabling. In July 2023, coordinated attacks on power infrastructure in Kaduna and Abuja led to a loss of over 400 megawatts from the national grid.³³ Such actions reflect the growing adoption of hybrid warfare tactics by criminal and terror groups, blending sabotage with conventional attacks to maximize state destabilization.

These manifestations underscore the increasing complexity of Nigeria's security challenges, with traditional law enforcement and military strategies proving insufficient. They also align with the theoretical underpinnings of asymmetric conflict theory, which explains how weaker actors leverage unconventional methods to exploit the vulnerabilities of a stronger adversary. As these actors adopt a mix of digital, kinetic, and psychological tools, Nigeria must urgently reform its security architecture to include anticipatory and technologically advanced measures capable of preempting and neutralizing emerging threats.

Implications for Nigeria's National Security

The emergence of new trends in modern warfare has profound implications for Nigeria's national security, affecting military operations, policy development, institutional coherence, and societal stability. These challenges require a comprehensive reassessment of Nigeria's security doctrine and capacity to respond to both traditional and non-traditional threats. At the operational level, the Nigerian military is increasingly confronted with enemies that exploit asymmetric tactics, cyber vulnerabilities, and emerging technologies to outmaneuver conventional forces. Guerrilla warfare by insurgent groups, coupled with attacks on logistical routes and forward operating bases, has stretched the operational bandwidth of the armed forces. The Nigerian Army, for instance, continues to contend with ambushes and improvised explosive devices (IEDs), which have led to significant casualties and resource attrition. According to a 2024-Armed Conflict Location & Event Data Project (ACLED) report, over 500 security personnel were lost in asymmetric engagements across the North East and North West zones within a span of 12 months. Intelligence gathering has also been complicated by the increased use of encrypted communications by non-state actors, reducing the efficacy of traditional surveillance and interception tools.

In the policy domain, the rapid evolution of threats has exposed major legislative and regulatory gaps. Nigeria's cybercrime law, last amended in 2015, is outdated and lacks provisions for emerging domains such as cyberwarfare, artificial intelligence-enabled crimes, and deepfake propaganda. There is also a lack of clear legal definitions and frameworks for drone usage by non-state actors, making it difficult to prosecute violations or preempt illicit deployments. Furthermore, the absence of a national doctrine on hybrid warfare or comprehensive counter-terrorism strategy leaves the country vulnerable to multi-dimensional attacks. Policy inertia has also contributed to delayed budgetary responses, undercutting the capacity of critical

security agencies to adapt swiftly to dynamic threat landscapes. The institutional consequences are equally severe. Nigeria's security institutions, including the military, intelligence community, and civil defence corps, face coordination and interoperability issues. Inter-agency rivalry and siloed intelligence remain significant barriers to unified action. The Defence Intelligence Agency (DIA), Department of State Services (DSS), and Nigerian Police Force often operate in parallel rather than in synergy, creating intelligence lapses that non-state actors exploit. This institutional fragmentation undermines threat analysis and response efficiency. Moreover, overstretched human and material resources have placed enormous strain on personnel morale and operational sustainability.

On the societal front, the human cost of emerging warfare has been devastating. Civilian populations have borne the brunt of insurgent violence, targeted attacks, and infrastructural sabotage. The Internal Displacement Monitoring Centre (IDMC) estimated in early 2024 that over 3.2 million Nigerians remain internally displaced due to conflict-related violence, especially in Borno, Zamfara, and Benue states. Civilian casualties from both insurgent attacks and security operations—especially airstrikes and counterinsurgency missions—have eroded public trust in the government and its security institutions. The prevalence of digital radicalization, especially among unemployed youth, also signals a deeper societal vulnerability rooted in economic exclusion and poor digital literacy.

The erosion of trust between citizens and the state further complicates national cohesion and weakens the state's ability to mobilize communities against extremism. This mistrust was evident in the 2023 EndSARS aftershock protests in some southern states, where perceptions of state repression and surveillance stirred resistance to government-led security initiatives. As Nigeria becomes increasingly urbanized and digitized, the state's failure to anticipate and respond to evolving security risks may exacerbate governance deficits and deepen insecurity.

Nigeria's Response Strategy: Gains and Gaps

Nigeria's response to its evolving national security threats has been multi-pronged, involving both kinetic and non-kinetic measures. While there have been notable gains in terms of strategic partnerships, technological upgrades, and tactical innovations, significant gaps remain in doctrine development, institutional coordination, cyber capacity, and sustainable funding. The effectiveness of Nigeria's security strategy, therefore, lies in its ability to build on existing successes while urgently addressing systemic deficiencies.

Kinetic and Non-Kinetic Countermeasures

On the kinetic front, Nigeria has continued to rely heavily on military force to suppress insurgent groups such as Boko Haram and the Islamic State West Africa Province (ISWAP). Operations like Lafiya Dole, Hadarin Daji, and Whirl Stroke have led to the neutralization of numerous combatants and the recapture of territories in the North East and North Central regions.³⁴ However, overreliance on kinetic

operations have also resulted in collateral damage, displacement of civilians, and a growing perception of state violence, particularly in urban and peri-urban conflict zones.³⁵

Non-kinetic responses have included deradicalization programs, such as the Operation Safe Corridor initiative, which provides rehabilitation and reintegration for surrendered militants. Civil society organizations and international donors have supported soft approaches including counter-narrative messaging and youth empowerment programs. Nevertheless, these efforts are often underfunded and poorly coordinated, limiting their long-term impact.³⁶

Cybersecurity Framework and Military Modernization

Recognizing the cyber dimension of contemporary warfare, Nigeria launched a National Cybersecurity Policy and Strategy (NCPS) in 2021, anchored by the Office of the National Security Adviser (ONSA). The framework aims to improve resilience across critical infrastructure, enhance digital forensics, and build cyber awareness in both public and private sectors. Furthermore, the Nigerian military has embarked on modest modernization efforts, including the acquisition of Unmanned Aerial Vehicles (UAVs), enhanced communication systems, and armored personnel carriers from international partners.³⁷

However, the implementation of cybersecurity protocols remains weak due to skill shortages, outdated infrastructure, and poor coordination among agencies. Most military cyber units lack the technical depth and real-time response capability to handle complex threats, including ransomware, disinformation campaigns, and drone-based surveillance.³⁸ Moreover, the civilian cyberspace remains largely unregulated, making it fertile ground for digital radicalization.

Civil-Military Cooperation and Inter-Agency Coordination

Civil-military cooperation has improved through initiatives like the Civilian Joint Task Force (CJTF), which has assisted in local intelligence gathering and community engagement, especially in the North East. The establishment of multi-agency coordination centers has also sought to streamline operations between the Nigerian Army, Nigeria Police Force, Department of State Services (DSS), and Nigeria Security and Civil Defence Corps (NSCDC).

Nonetheless, these efforts are often undermined by inter-agency rivalry, overlapping mandates, and lack of interoperability. Information silos persist, particularly in the area of intelligence sharing, which diminishes the effectiveness of coordinated responses to complex threats.³⁹ There is also the persistent challenge of militarization of internal security, which erodes public trust and stifles community-based policing.

Strategic Partnerships

Nigeria has leveraged regional and international partnerships to strengthen its national security architecture. Through the Multinational Joint Task Force (MNJTF), Nigeria collaborates with Chad, Cameroon, and Niger in the fight against terrorism in the Lake Chad Basin. At the continental level, Nigeria aligns with African Union (AU) frameworks such as the African Standby Force and AU Early Warning System.

Bilateral cooperation with the United States, United Kingdom, and European Union has resulted in technical training, intelligence sharing, and arms procurement. For instance, the delivery of Super Tucano aircraft from the US has significantly enhanced airstrike capabilities against insurgent camps.⁴⁰ However, such partnerships often come with restrictions on end-use, human rights compliance, and conditionalities that slow down tactical responses. There is also a dependence risk, where Nigeria's security trajectory is tied too closely to the priorities and politics of external actors.⁴¹

Conclusion and Recommendations

Conclusion

This study establishes that Nigeria's national security architecture is under significant strain due to the evolving nature of warfare characterized by hybrid threats, cyberwarfare, and the growing influence of non-state actors. The traditional, heavily centralized security apparatus, while structured across military, intelligence, paramilitary, and law enforcement institutions, remains largely reactive and lacks the anticipatory posture required to confront asymmetric and technologically-driven threats. Community-based security actors such as Amotekun, Ebube Agu, and the CJTF play critical roles in local security responses, but their activities sometimes undermine the broader national security agenda due to lack of regulation, interoperability, and occasional abuse of power. While Nigeria has made some progress in modernizing its security sector—evident in frameworks like the National Cybersecurity Policy and Strategy^{42a} and platforms like the Defence Industries Corporation of Nigeria (DICON)—operational fragmentation, underfunding, poor civil-military trust, and weak cyber laws remain key bottlenecks. Emerging trends such as the use of drones by insurgents, digital radicalization, and proxy conflicts in the Sahel reflect a broader global trend where developing nations like Nigeria are vulnerable due to limited resilience in digital defense, outdated doctrines, and lack of comprehensive counter-hybrid warfare strategies.

Nigeria's security challenges are no longer solely conventional; they now exist within a complex ecosystem of hybrid warfare and asymmetric threats, amplified by technological disruption, regional instability, and institutional weaknesses. The inadequacy of current structures to adapt to these emerging realities jeopardizes national cohesion, development, and territorial integrity. While policy strides have been made, including inter-agency cooperation and regional security collaboration,

much more is required to transform Nigeria's security architecture into a proactive, tech-enabled, intelligence-driven system that can manage 21st-century security risks. A rethinking of doctrine, investment in technological capabilities, and the institutionalization of accountability and trust are now imperative.

Recommendations

The following are recommended:

- a. The FGN should adopt a national hybrid warfare strategy that integrates military, intelligence, cyber, and diplomatic tools to combat multidimensional threats.
- b. The FGN should revise the National Security Strategy to prioritize emerging technologies, cyber defence, and artificial intelligence as core components.
- c. The AFN should establish a central command for inter-agency coordination with legal backing to ensure intelligence and operational interoperability.
- d. The NPF should regulate and harmonize community vigilante groups under a national framework to prevent abuse and enhance synergy with formal security forces.
- e. The ONSA should invest in advanced training and simulation technologies for security forces to prepare them for cyber, drone, and hybrid warfare scenarios.
- f. The FGN should expand cybersecurity capacity by increasing budget allocation, human capital development, and establishing Cyber Fusion Centres across zones.

Endnotes

1. M. Kaldor, *New and old wars: Organized violence in a global era* (3rd ed.). Polity Press, 2012.
2. M. Galeotti, *Putin's wars: From Chechnya to Ukraine*. Bloomsbury Publishing, 2023.
3. Council on Foreign Relations, *Russia's war in Ukraine: Timeline and facts*. <https://www.cfr.org/timeline/russias-war-ukraine>, 2023.
4. E.B. Kania, & J. Costello, *AI, China, and the future of warfare*. Center for a New American Security. <https://www.cnas.org/publications/reports/ai-china-and-the-future-of-warfare>, 2020.

5. S. Lezhnev, and A. Mukpo, Cobalt and conflict: How Congolese resources fuel global tech. The Enough Project. <https://enoughproject.org/reports/cobalt-and-conflict>, 2020.
6. P. Fabricius, Africa's emerging role in global power competition. Institute for Security Studies. <https://issafrica.org/iss-today/africas-emerging-role-in-global-power-competition>, 2022.
7. E. Munyi, and A. Adeoye, Africa in the new global order: Peace, security and development. Palgrave Macmillan, (2022).
8. W. Nasr, How the Wagner Group is aggravating the jihadi threat in the Sahel. CTC Sentinel, 15(11). <https://ctc.westpoint.edu/how-the-wagner-group-is-aggravating-the-jihadi-threat-in-the-sahel>, 2022.; The Washington Post. (2025, March 11). Russia's Wagner mercenaries are leading a campaign of terror in Mali. The Washington Post. <https://www.washingtonpost.com/world/2025/03/11/russia-wagner-mali-mercenaries-putin>, 2025.
9. Economic and Social Commission for Western Asia (ESCWA). (2020, December 2). Cost of conflict in Libya exceeds US \$576 billion [Press release]. United Nations ESCWA. <https://www.unescwa.org/news/cost-conflict-libya-exceeds-576-billion-escwa-study-finds>, 2020.
10. F. C. Onuoha, "The rise of non-state security actors in Nigeria", African Security Review, 29(3), 2020, 305–322.
11. A. T. Kaspersen, "Emerging technologies and the future of conflict", World Economic Forum, 2020.
12. P. W. Singer, and E. T. Brooking, LikeWar: The weaponization of social media, Houghton Mifflin Harcourt, 2018.
13. U. M. Ogbonnaya and U. C. Ehugbo, "The national security architecture in Nigeria: Challenges and prospects", African Journal of Security Studies, 10(2), 2022, 45–62.
14. E. E. O. Alemika, Security challenges and national transformation, CLEEN Foundation, 2015.
15. F. Hoffman, Conflict in the 21st century: The rise of hybrid wars, Potomac Institute for Policy Studies, 2007.
16. W. Murray, and P. R. Mansoor (Eds.), Hybrid warfare: Fighting complex opponents from the ancient world to the present, Cambridge University

- Press, 2012.
17. H. J. Morgenthau, *Politics among nations: The struggle for power and peace*, Alfred A. Knopf, 1948.; K. N. Waltz, *Theory of international politics*, Addison-Wesley, 1979.
 18. I. Arreguín-Toft, "How the weak win wars: A theory of asymmetric conflict". *International Security*, 26(1), 2001, 93–128.
 19. OECD-DAC., "Handbook on security sector reform: Supporting security and justice", Organisation for Economic Co-operation and Development, 2007; A. Bryden, and H. Hänggi, "Reforming and reconstructing the security sector", Geneva Centre for the Democratic Control of Armed Forces (DCAF), 2005.
 20. I. Arreguín-Toft, "How the weak win wars: A theory of asymmetric conflict". *International Security*, 26(1), 2001, 93–128.
 21. *Global Firepower*, 2023; CLEEN Foundation, 2022.
 22. (CFRN 1999)
 23. (Adebajo, 2021)
 24. SBM Intelligence. (2023). *Annual Nigeria security report 2023*. <https://www.sbmintel.com/reports>
 25. *National Security Strategy (NSS)*. (2019). Office of the National Security Adviser, Nigeria.
 26. *National Information Technology Development Agency (NITDA), Nigeria's cybersecurity annual report*, 2023.
 27. NCC. (2023). *Cyber threat alert report*. Nigerian Communications Commission.
 28. International Crisis Group, *Winning the war on Boko Haram: Rebuilding Nigeria's Northeast*, 2023.
 29. UNODC, "Transnational organized crime in West Africa: Emerging threats", United Nations Office on Drugs and Crime, 2022.
 30. UNHCR, "Nigeria situation report" United Nations High Commissioner for Refugees, 2023.

31. M. Galeotti, *Putin's wars: From Chechnya to Ukraine*. Bloomsbury Publishing, 2023.
32. (Sahara Reporters, 2023)
33. NERC, 2023
34. International Crisis Group, *Winning the war on Boko Haram: Rebuilding Nigeria's Northeast*, 2023.
35. (Amnesty International, 2024)
36. F, C. Onuoha, "The rise of non-state security actors in Nigeria", *African Security Review*, 29(3), 2020, 305–322.
37. (Olonisakin & Oloruntoba, 2024)
38. (Eze, 2023)
39. (Aliyu & Eboh, 2023)
40. (US Department of Defense, 2022)
41. (Bøås, 2023)
42. *National Cybersecurity Policy and Strategy*, 2021.