

BULLETIN

OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

No. 2 / 2026

ISSN 2284-936X

eISSN 2284-9378

Publication founded in 1937

SCIENTIFIC PUBLICATION HIGHLY ACKNOWLEDGED IN THE FIELD
OF "MILITARY SCIENCES, INFORMATION AND PUBLIC ORDER"
OF THE NATIONAL COUNCIL FOR ATTESTATION OF ACADEMIC
DEGREES, DIPLOMAS AND CERTIFICATES, INDEXED IN
INTERNATIONAL DATABASES EBSCO, CEEOL, GOOGLE SCHOLAR,
INDEX COPERNICUS, PROQUEST, DOAJ, ERIH PLUS, CROSSREF

EDITORIAL BOARD

Editor-in-chief	Col.(Ret.)Prof. HLIHOR Constantin, Ph.D. – The Faculty of History, University of Bucharest
Deputy Editor-in-chief	Senior Lect. MATEI Cris, Ph.D. – Centre for Homeland Defence and Security, Department of National Security, Naval Postgraduate School, United States
	Maj.Gen. MAVRIȘ Eugen, Ph.D. – "Carol I" National Defence University, Bucharest
	Bg.Gen.Prof.Eng. VIZITIU Constantin Iulian, Ph.D. – "Ferdinand I" Military Technical Academy, Bucharest
	Bg.Gen. Assoc.Prof. ȘERBESZKI Marius, Ph.D. – "Henri Coandă" Air Force Academy, Brașov
	Col. TODOSIUC Dumitru – "Nicolae Bălcescu" Land Forces Academy, Sibiu
	Col.Senior Lect. DAN-PETRESCU Lucian, Ph.D. – "Carol I" National Defence University, Bucharest
	Col.Prof. STANCIU Cristian-Octavian, Ph.D. – "Carol I" National Defence University, Bucharest
	Col.(R)Prof. ROCEANU Ion, Ph.D. – "Carol I" National Defence University, Bucharest
	Assoc.Prof. PETERFI Carol Teodor, Ph.D. – "Ferdinand I" Military Technical Academy, Bucharest (Winner of the Nobel Peace Prize in 2013)
	Assoc.Prof. PETROVA Elitsa – "Vasil Levski" National Military University, Veliko Tarnovo, Bulgaria
	Assoc.Prof. BICHIR Florian, Ph.D. – "Carol I" National Defence University, Bucharest
Director of the Publishing House	Col. STAN Liviu-Vasile – "Carol I" National Defence University, Bucharest
Senior editors	Col.Assoc.Prof. DAN-ȘUTEU Ștefan-Antonio, Ph.D. – "Carol I" National Defence University, Bucharest
	Lt.Col.Prof.Habil. MUSTĂȚĂ Marinela-Adi, Ph.D. – "Carol I" National Defence University, Bucharest
Executive editors	MÎNDRICAN Laura – "Carol I" National Defence University, Bucharest
	TUDORACHE Irina – "Carol I" National Defence University, Bucharest
Editorial secretary	MINEA Florica – "Carol I" National Defence University, Bucharest
Proof-reader	ROȘCA Mariana – "Carol I" National Defence University, Bucharest
Layout&Cover	GÎRTONEA Andreea – "Carol I" National Defence University, Bucharest

SCIENTIFIC BOARD

ANTON Mihail, Ph.D. – "Carol I" National Defence University, Bucharest
BAK Tomasz, Ph.D. – WSPiA University of Rzeszów, Poland
BÎRSAN Ghiță, Ph.D. – "Nicolae Bălcescu" Land Forces Academy, Sibiu
BLACK Jeremy, Emeritus Prof. – University of Exeter, United Kingdom
BOGZEANU Cristina, Ph.D. – "Mihai Viteazul" National Intelligence Academy, Bucharest
CHIFU Iulian, Ph.D. – "Carol I" National Defence University; President of the Center for Conflict Prevention and Early Warning, Bucharest
COROPCEAN Ion, Ph.D. – Agency for Science and Military Memory of the Ministry of Defence Republic of Moldova
CORPĂDEAN Adrian Gabriel – Babeș-Bolyai University, Cluj-Napoca
CRISTESCU Sorin, Ph.D. – The Institute for Defence Political Studies and Military History from Bucharest
DUMITRESCU Lucian, CS II – Institute of Sociology, Romanian Academy, Bucharest
FLORIȘTEANU Elena, Ph.D. – "Nicolae Bălcescu" Land Forces Academy, Sibiu
FRUNZETI Teodor, Ph.D. – "Titu Maiorescu" University; Academy of Romanian Scientists, Academy of National Security Sciences, Bucharest
GAWLICZEK Piotr, Ph.D. – "Cuiavian" University in Wloclawek, Poland
GOTOWIECKI Paweł, Ph.D. – University of Business and Entrepreneurship in Ostrowiec Świętokrzyski, Poland
GRAD Marius-Nicolae – Babeș-Bolyai University, Cluj-Napoca
GROCHMAŁSKI Piotr, Ph.D. – "Nicolaus Copernicus" University in Torun, Poland
HARAKAL Marcel, Ph.D. – "General Milan Rastislav Štefánik" Armed Forces Academy, Liptovský Mikuláš, Slovak Republic
HURDUZEU Gheorghe, Ph.D. – The Bucharest University of Economic Studies
IORDACHE Constantin, Ph.D. – "Spiru Haret" University, Bucharest
MINCULETE Gheorghe, Ph.D. – "Nicolae Bălcescu" Land Forces Academy, Sibiu
MUNTEANU Codrin, Ph.D. – "Carol I" National Defence University, Bucharest
NĂSTASE Marian, Ph.D. – The Bucharest University of Economic Studies
NISTOR Filip, Ph.D. – "Mircea cel Bătrân" Naval Academy, Constanța
ORZAN Gheorghe, Ph.D. – The Bucharest University of Economic Studies
OTRISAL Pavel, Ph.D. – University of Defence, Brno, Czech Republic
PKHALADZE Tengiz, Ph.D. – Georgian Institute of Public Affairs, Georgia
POPESCU Alba-Iulia Catrinel, Ph.D. – "Carol I" National Defence University; member of Academy of Romanian Scientists; vice-president of DIS/CRIFST of the Romanian Academy, Bucharest

POPESCU Maria-Magdalena, Ph.D. – "Carol I" National Defence University, Bucharest
SARCINSCHI Alexandra-Mihaela, Ph.D. – "Carol I" National Defence University, Bucharest
TOGAN Mihai, Ph.D. – Military Technical Academy "Ferdinand I", Bucharest
TOMA Alecu, Ph.D. – "Mircea cel Bătrân" Naval Academy, Constanța
VASILESCU Cezar, Ph.D. – "Carol I" National Defence University, Bucharest
VDOVYCHENKO Viktoriia, Ph.D. – Program Director of Security Studies, Center for defence strategies, Ukraine
WARNES Richard – RAND Europe
WOJTAN Anatol, Ph.D. – University of Business and Entrepreneurship in Ostrowiec Świętokrzyski, Poland
ŽNIDARŠIČ Vinko, Ph.D. – Military Academy, University of Defence, Belgrade, Serbia

SCIENTIFIC REVIEWERS

ATANASIU Mirela, Ph.D. – "Carol I" National Defence University, Bucharest
BELLO Abdulrazak Agboola – University of Offa, Nigeria
BUȘE Mihaela, Ph.D. – "Carol I" National Defence University, Bucharest
BUȚĂ Ionuț-Cosmin, Ph.D. – "Carol I" National Defence University, Bucharest
CHISEGA-NEGRILĂ Ana-Maria, Ph.D. – "Carol I" National Defence University, Bucharest
CIAPA Gabriel-Constantin – „Ferdinand I” Military Technical Academy, Bucharest
FRUNZĂ Alexandru – "Ferdinand I" Military Technical Academy, Bucharest
GĂINĂ Liviu, Ph.D. – "Henri Coandă" Air Force Academy, Brașov
IGNAT Vasile-Ciprian, Ph.D. – "Carol I" National Defence University, Bucharest
NISTORESCU Claudiu-Valer, Ph.D. – "Carol I" National Defence University, Bucharest
SÂRBU Annamaria, Ph.D. – "Nicolae Bălcescu" Land Forces Academy, Sibiu
TOROI George-Ion, Ph.D. – "Carol I" National Defence University, Bucharest
TUDORACHE Paul, Ph.D. – "Nicolae Bălcescu" Land Forces Academy, Sibiu
ȚUȚUIANU Diana-Elena, Ph.D. – "Carol I" National Defence University, Bucharest



© Reproductions are allowed under
the condition of specifying source.

Full responsibility for the articles
lies with the authors.

The articles of journal are under the similarity
verification standard using sistemantiplagiat.ro.

The articles published in the Bulletin of "Carol I"
National Defence University, ISSN 2284-936X,
L 2284-936X, are also found – title, author, abstract,
content and bibliography – in the Romanian
version of the journal, ISSN 1584-1928.

Content

No. 2/2026

Ibrahim Ogirima SALAWU

Ambali ABDULRAUF

Mohammed Idris DANJUMA

Abdullahi Shina YAHAYA

Emmanuel Oyewole LAMBE

Armed Banditry, Artisanal Mining, and the Changing
Security Landscape of North-Central Nigeria **7**

Captain Assistant Lecturer George-Adrian AIONESEI

Social Media as a Disinformation Infrastructure:

Tactics, Strategies, and National Security **27**

Captain Alexandru PÎNTEA, Master's Student

The Information Asymmetry of Military Decision-Making.

ISR and the Challenge of Situational Understanding **51**

Lecturer and Researcher Nora LELYANA

Dr. Aris SARJITO

Strategic Autonomy without Alliances:

Indonesia's Defence Dilemma **69**

Latifat Kehinde OLATINWO

Olooto Felicia MOTUNRAYO

Jesuwaye Israel OLUSANMI-DARE

Isiaka Seriki ADAMU

Mohammed ABUBAKAR

Emmanuel Oyewole LAMBE

The Tripartite of Food Security, Diplomacy
and National Security in West Africa **91**

Basheer Olalere USAMOTU, PhD

Musediq Olufemi LAWAL

Young Kenneth IRHUE

Oluwatoyin Adijat OWOLEWA

Multilateralism and National Development:

An Assessment of Nigeria's Roles in the Development

of International Organizations (IO) in Africa (1960-2025) **111**

Ovidiu PĂDURARIU, PhD

The Romanian Army's Confrontation
with the Realities of Modern War: Lessons Learned
from the Campaigns of 1913, 1916, and 1917 129

Akeem Ayanda ARABA, PhD

Kafayat Toyin ARABA, PhD

Tawakalitu Bola YUSUF, PhD

Taoheed Opeyemi MUHAMMED

Decentralized Security and Crime Control: Assessing
the Effectiveness of Forest Guards in Kwara State, Nigeria 161

MSc. Rexhep MUSTAFOVSKI, Teaching and Research Assistant

Integrated UAV-Satellite Communication Architecture
with NOMA-based Multi-link Connectivity
for Secure and Resilient Wireless Networks 185

Mubarak Sulaiman JAMIU

Proliferation of Small Arms and Light Weapons
and Insecurity in Northwestern Nigeria: A Review 213

Luis VAZ, MSc

LTC Cav Pedro FERREIRA, PhD

Cognitive Warfare and Strategic Uncertainty:
Planning under the Threshold in Open Societies 229

MAJ Cristian-Alexandru SALAC, PhD Candidate

Contemporary Warfare and the Transformation
of the Global Military Paradigm 257

Dumitru Cătălin COHAL, PhD

The Determinants of Military Combat Capacity Longevity:
between Physical Specialization, Training Volume, and Recovery 273

Cristiana Maria ALMAŞAN, PhD Candidate

Hybrid Crisis Management: An Integrated
Response to Contemporary Asymmetric Threats 285

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

<https://buletinul.unap.ro/index.php/en/>

Armed Banditry, Artisanal Mining, and the Changing Security Landscape of North-Central Nigeria

Ibrahim Ogirima SALAWU*

Ambali ABDULRAUF**

Mohammed Idris DANJUMA***

Abdullahi Shina YAHAYA****

Emmanuel Oyewole LAMBE*****

*Department of Politics and Governance, Kwara State University, Malete
e-mail: Ibrahimsalus@gmail.com

**Department of Politics and Governance, Kwara State University, Malete
e-mail: abdulrauf.ambali@kwasu.edu.ng

***Department of Politics and Governance, Kwara State University, Malete
e-mail: Mohammed.danjuma@kwasu.edu.ng

****Department of Politics and Governance, Kwara State University, Malete
e-mail: Yayus.shina@yahoo.com

*****Department of Politics and Governance, Kwara State University, Malete
e-mail: Emmanuel.lambe22@kwasu.edu.ng

Abstract

The study aims to examine the relationship between artisanal mining and insecurity in North-Central Nigeria, with particular attention to the roles of state and non-state actors in shaping conflict dynamics within mining communities. It aims to assess the influence of governance mechanisms on sustainable solid mineral development within Nigeria's economic diversification agenda. A mixed-methods design was adopted, combining survey data from 400 respondents, including community leaders, artisanal miners, security personnel, civil society actors, and local government officials, with qualitative interviews providing contextual depth. Grounded in Resource Curse and Political Ecology perspectives, the study finds that unregulated mining of gold, tin, and columbite significantly escalates armed banditry and territorial conflicts. Regression results show a strong positive relationship between informal mining and insecurity ($\beta = 0.67, p < .01$) and a moderate effect of state and non-state actors on violence escalation ($\beta = 0.52, p < .05$). The study concludes that insecurity reflects governance deficits and rent-seeking dynamics, underscoring the need for stronger regulation and inclusive local governance mechanisms for sustainable conflict mitigation.

Keywords:

Solid Minerals; Insecurity; Political Economy; Resource Governance;
North-Central Nigeria; Violence.

Article info

Received: 16 November 2025; Revised: 19 December 2025; Accepted: 14 May 2026; Available online: 30 June 2026

Citation: Salawu, I.O., A. Abdulrauf, M.I. Danjuma, A.S. Yahaya, and E.O. Lambe. 2026. "Armed Banditry, Artisanal Mining, and the Changing Security Landscape of North-Central Nigeria." *Bulletin of "Carol I" National Defence University*, 15(2): 7-26. <https://doi.org/10.53477/2284-9378-26-16>



© „Carol I” National Defence University Publishing House

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC-SA)

Introduction

The relationship between natural resource endowment and insecurity has remained a major concern in both development and conflict studies. While natural resources are often expected to stimulate economic growth and improve livelihoods, evidence from many resource-rich regions suggests that they can also generate competition, social tensions, and violent conflicts. Scholars have observed that valuable natural resources frequently become objects of contestation among state actors, local communities, private interests, and criminal networks seeking to control access to resource rents (Auty 2001; Le Billon 2012). In many developing societies, resource wealth has therefore become associated not only with economic opportunities but also with instability, governance challenges, and recurring violence.

This pattern is particularly evident in North-Central Nigeria, a region endowed with substantial deposits of tin, columbite, gold, limestone, and other solid minerals. Despite the economic potential of these resources, many mining communities continue to experience varying forms of insecurity, including communal clashes, armed attacks, illegal mining activities, and violent competition over resource control. The persistence of these challenges reflects broader concerns raised by the Resource Curse literature, which argues that resource abundance does not automatically translate into development, especially in contexts characterized by weak institutions and ineffective governance structures (Auty 2001; Ross 2015).

The drivers of insecurity in North-Central Nigeria are complex and interconnected. Competition over land and access to valuable resources has intensified tensions among different groups, while weak regulatory institutions and limited state capacity have created opportunities for criminal actors to exploit resource-rich environments (Okoli and Lenshie 2018; International Crisis Group 2020). The proliferation of small arms, the expansion of informal mining activities, and the increasing involvement of armed groups have further complicated the security landscape. As a result, violence in many communities is no longer driven solely by traditional disputes but is increasingly linked to broader economic and political interests surrounding resource extraction.

Solid minerals occupy a strategic position within the political economy of North-Central Nigeria. The growing demand for mineral resources has attracted a diverse range of actors seeking economic benefits from extraction activities. However, where regulatory oversight is weak and governance mechanisms are ineffective, competition for access and control can become a source of conflict rather than development (Le Billon 2012; Ross 2015). In many cases, mineral-rich areas have become sites of contestation involving local communities, private operators, armed groups, and state institutions, creating conditions that sustain cycles of insecurity. Understanding the relationship between solid mineral resources, insecurity, and escalating violence in North-Central Nigeria is therefore essential. Such understanding provides valuable insights into the way in which resource governance,

state capacity, and the activities of non-state actors shape patterns of conflict within mining communities. It also contributes to ongoing debates on how resource wealth can be effectively managed to promote stability, sustainable development, and human security in resource-rich regions.

Problem Statement

North-Central Nigeria possesses significant deposits of solid minerals, including tin, columbite, gold, and limestone, which have the potential to contribute substantially to local economic development, employment generation, and national revenue. However, despite this resource endowment, many communities in the region continue to experience persistent insecurity and violent conflicts linked to resource access and control. Evidence from resource-conflict literature suggests that rather than guaranteeing development, natural resource abundance in weak institutional environments often intensifies competition and social tensions, thereby increasing the risk of violence ([Ross 2015](#); [Le Billon 2012](#)).

Over time, mining communities across parts of North-Central Nigeria have experienced recurring incidents of communal violence, armed attacks, illegal mining activities, and displacement of populations. These patterns are consistent with broader findings that link resource extraction zones to heightened insecurity, particularly where governance structures are weak and informal economic actors dominate extraction processes ([Okoli and Lenshie 2018](#); [International Crisis Group 2020](#)). In such environments, mineral-rich areas become sites of overlapping economic and criminal interests, reinforcing cycles of instability.

The situation is further exacerbated by the proliferation of small arms and light weapons, coupled with weak regulatory enforcement and illegal mining practices. Research shows that the availability of illicit arms and weak state capacity significantly increase the likelihood of violent conflict in resource-rich regions ([UNODC 2021](#); [Williams 2018](#)). Consequently, both local and external actors exploit governance gaps to gain economic and political advantage within mining communities.

Non-state actors, including armed groups and criminal networks, play a significant role in these dynamics by engaging in illegal extraction, taxation, and territorial control. At the same time, state responses are often constrained by institutional weaknesses, inconsistent enforcement, and governance challenges that limit effective regulation of resource extraction activities ([Aning and Abdallah 2013](#); [Okoli and Okpaleke 2014](#)).

Despite growing scholarly attention to resource-related conflicts in Nigeria, there remains limited empirical evidence that specifically quantifies the relationship between solid mineral exploitation and insecurity in North-Central Nigeria, as well as the combined roles of state and non-state actors in shaping these outcomes. This gap necessitates a focused empirical investigation to explain how resource governance structures influence patterns of violence in mining communities.

Research Objective

The aim of this study is to examine the relationship between solid mineral resource exploitation and insecurity in North-Central Nigeria, with particular emphasis on the roles of state and non-state actors in shaping patterns of violence and conflict within mining communities.

Literature Review

The Concept of Armed Banditry

Armed banditry refers to the organized use or threat of violence by non-state armed groups to achieve economic, territorial, or political objectives through criminal activities such as robbery, kidnapping, extortion, cattle rustling, illegal taxation, and territorial domination. Unlike conventional criminality, armed banditry is characterized by its sustained nature, strategic organization, and systematic deployment of violence, often within contexts of weak state presence, fragile institutions, and contested authority. It thus occupies a conceptual space between organized crime and low-intensity armed conflict, blurring the boundaries between criminal enterprise and insurgent activity.

In security and conflict studies, armed banditry is increasingly understood as a manifestation of complex political economy dynamics rather than merely a breakdown of law and order. Empirical scholarship demonstrates that armed banditry thrives in environments where state capacity is limited, governance is predatory, and economic opportunities are structurally constrained ([Okoli and Lenshie 2018](#)). In such contexts, violence becomes both a survival strategy and an economic instrument, enabling armed groups to extract rents, control trade routes, and dominate resource-rich territories. Consequently, armed banditry often evolves into a self-sustaining criminal economy, sustained by illicit markets, arms trafficking networks, and local patronage systems.

The emergence and consolidation of armed banditry are closely linked to structural factors such as poverty, youth unemployment, environmental stress, resource competition, and historical grievances. In many fragile regions, particularly across the Sahel and parts of West Africa, shrinking livelihoods due to climate change, agricultural decline, and land scarcity have intensified competition over resources, pushing marginalized populations toward violent survival strategies ([International Crisis Group 2020](#); [UNODC 2021](#)). These dynamics are further exacerbated by the proliferation of small arms and light weapons, porous borders, and weak regional security coordination, which collectively lower the threshold for organized violence.

In the Nigerian context, armed banditry has transformed from sporadic cattle rustling and highway robbery into a highly coordinated system of mass kidnapping, village raids, and territorial occupation, particularly across the North-West and increasingly the North-Central regions. Scholars argue that this transformation reflects deeper

failures of governance, including ineffective policing, elite complicity, corruption, and the erosion of traditional conflict resolution mechanisms ([Okoli and Okpaleke 2014](#)). Armed groups now exercise quasi-sovereign authority in many rural spaces, imposing illegal taxation, regulating local economies, and determining patterns of movement and settlement. This development signals a profound reconfiguration of state-society relations, where non-state actors increasingly substitute or contest formal authority.

More critically, armed banditry increasingly intersects with artisanal mining, illegal resource extraction, and transnational criminal networks, thereby deepening its complexity and lethality. Resource-rich zones provide both financing and strategic cover for armed groups, while illicit mining sites become arenas of violent contestation, labour exploitation, and elite capture. This convergence of criminal violence and resource predation not only intensifies local insecurity but also embeds armed banditry within broader networks of organized crime, making conventional military or policing responses insufficient. As Le Billon ([2012](#)) argues, such conflict-resource entanglements transform violence into a profitable enterprise, reinforcing cycles of insecurity and underdevelopment.

Overall, armed banditry represents a multidimensional security threat that transcends conventional crime control paradigms. It reflects the intersection of economic deprivation, governance breakdown, and political exclusion, sustained through violent rent-seeking and territorial control. Effective responses, therefore, require an integrated strategy combining security enforcement, institutional reform, community engagement, and sustainable livelihood interventions. Without addressing these structural foundations, armed banditry is likely to persist, mutate, and further destabilize fragile regions.

The Concept of the Changing Security Landscape

The concept of the changing security landscape refers to the dynamic transformation in the nature, actors, drivers, and spatial patterns of security threats within a given political and social context. Traditionally, security was conceptualized primarily in statist and militaristic terms, with emphasis on territorial defence, interstate warfare, and the protection of national sovereignty. However, contemporary security discourse has shifted significantly toward a broader and more complex understanding that incorporates non-traditional threats such as terrorism, armed banditry, organized crime, resource conflicts, environmental insecurity, cyber threats, and transnational criminal networks ([Buzan, Wæver, and de Wilde 1998](#); [Kaldor 2012](#)). This shift reflects fundamental changes in the global political economy, patterns of conflict, and the evolving character of violence.

At the core of the changing security landscape is the transformation of conflict from conventional state-based warfare to fragmented, localized, and network-driven forms of violence. Modern security threats increasingly emerge from non-

state armed actors who operate across porous borders, exploit weak governance structures, and embed themselves within local economies and social systems. These actors frequently combine criminal, political, and economic motives, producing hybrid forms of insecurity that defy traditional military responses (Duffield 2001; Williams 2018). Consequently, contemporary security challenges are no longer confined to battlefields but permeate everyday social spaces, including farms, markets, highways, mining sites, and rural communities.

This evolving security environment is also shaped by the political economy of violence, in which economic predation, resource exploitation, and rent-seeking behaviours sustain armed mobilization. In resource-rich but institutionally weak contexts, competition over valuable commodities such as minerals, land, and livestock intensifies insecurity, as armed groups seek to control production sites, trade routes, and taxation systems (Le Billon 2012; Ross 2015). These dynamics produce localized war economies that normalize violence, erode state authority, and entrench cycles of instability. As a result, security threats become deeply embedded in everyday economic activities, making them structurally resilient and difficult to dismantle.

Environmental stress, demographic pressure, and livelihood insecurity further contribute to the changing security landscape, particularly in fragile regions. Climate variability, land degradation, and shrinking economic opportunities exacerbate competition over natural resources, intensifying communal tensions and facilitating recruitment into violent networks (Homer-Dixon 2010; Ide et al. 2021). In such settings, insecurity becomes both a cause and consequence of underdevelopment, reinforcing vulnerability and weakening institutional responses. This interlocking relationship between environmental change, economic precarity, and violent conflict underscores the multidimensional nature of contemporary security challenges.

In Nigeria, the changing security landscape is reflected in the proliferation of armed banditry, mass kidnapping, violent extremism, communal conflicts, farmer-herder clashes, and criminal insurgencies across multiple regions. These threats signify a fundamental departure from conventional security paradigms, revealing deep-seated governance failures, institutional fragility, and declining state monopoly over the legitimate use of force (International Crisis Group 2020). The expansion of violent non-state actors into rural and peri-urban spaces has transformed patterns of everyday life, economic activity, and population mobility, thereby redefining both the geography and sociology of insecurity.

More critically, Nigeria's evolving security landscape illustrates the growing convergence between criminal violence and resource governance failures. The entrenchment of armed groups within artisanal mining zones, forest corridors, and agrarian communities has blurred distinctions between economic survival strategies and organized violence. This convergence has reconfigured local power

relations, weakened traditional authority structures, and fostered alternative systems of governance based on coercion and illicit taxation. In this sense, the changing security landscape is not merely a security problem but a profound governance crisis that challenges the legitimacy and effectiveness of the state.

Overall, the concept of the changing security landscape captures the transformation of insecurity from episodic and centralized threats into persistent, decentralized, and socially embedded forms of violence. It reflects a shift toward complex security environments in which criminality, political grievance, economic predation, and institutional fragility intersect. Addressing such evolving threats, therefore, requires integrated policy responses that combine security sector reform, inclusive governance, economic restructuring, and community-based resilience mechanisms. Without such holistic interventions, contemporary insecurity is likely to deepen, fragment further, and generate enduring instability.

Governance, Corruption, and Multi-Scalar Resource Competition in Extractive Economies

Recent scholarship on extractive governance increasingly emphasizes that institutional inefficiency in resource-rich settings cannot be fully understood without accounting for the interaction between corruption, elite competition, and transnational economic networks. Corruption, in this context, operates as a critical mechanism through which administrative inefficiency is produced and sustained. As Mauro (1995) demonstrates, corruption reduces bureaucratic effectiveness by distorting allocation processes, weakening regulatory enforcement, and undermining public sector performance, particularly in resource-dependent economies. Similarly, Rose-Ackerman (1999) argues that corruption is not merely a moral or legal deviation but a structural governance problem that reshapes decision-making processes and weakens institutional accountability.

Beyond administrative inefficiency, extractive economies are often characterized by intense internal elite struggles over resource capture. In line with Bayart's (1993) "politics of the belly," access to mineral rents becomes a central driver of political competition, where state and non-state elites strategically position themselves to control extraction, licensing, and revenue flows. Reno (1995) further conceptualizes this dynamic through the notion of "shadow states," where formal governance structures are systematically penetrated by informal networks of power, patronage, and resource extraction. In such contexts, governance becomes fragmented as competing elites instrumentalize state institutions for private accumulation.

At the external level, resource extraction is increasingly embedded within transnational mineral economies. External actors, including commodity buyers, intermediaries, and cross-border trading networks, play a significant role in shaping extraction incentives and sustaining informal or illicit supply chains. These actors often reinforce local governance weaknesses by providing alternative market

structures that bypass formal regulatory systems. Taken together, these dynamics illustrate that governance failure in extractive sectors is not solely institutional but also relational, emerging from the interaction between corruption-driven inefficiencies, elite competition over resource capture, and external demand structures that sustain informal mineral economies.

Empirical Review

Empirical studies on the relationship between natural resources and conflict have consistently demonstrated that the impact of resource endowment on security outcomes is context-dependent. While resource wealth can stimulate economic opportunities, it frequently generates adverse outcomes such as competition, exclusion, and violent conflict in environments characterized by weak governance and limited institutional capacity (Ross 2015; Le Billon 2012). This duality reinforces the argument of the Resource Curse literature, which posits that resource abundance may become a liability rather than an asset in fragile political settings (Sachs and Warner 2001).

1. Resource Wealth and Conflict

Empirical evidence from resource-rich developing regions indicates a strong association between natural resource endowment and the incidence of violent conflict. Ross (2015) argues that resource abundance increases the likelihood of conflict through mechanisms such as rent-seeking, inequality, and weak institutional oversight. Similarly, Le Billon (2012) demonstrates that resource extraction zones often become sites of contestation where multiple actors compete for access and control, thereby increasing the probability of violence.

In the Nigerian context, Okoli and Lenshie (2018) observe that rural areas with valuable natural and extractive resources frequently experience heightened insecurity due to overlapping claims over land and economic opportunities. This aligns with findings from the International Crisis Group (2020), which documents how resource-rich regions in Nigeria's northern corridor have become increasingly associated with armed violence, communal disputes, and illegal economic activities.

2. Role of State Actors

The literature consistently emphasizes that state capacity and governance quality significantly shape resource-conflict outcomes. Aning and Abdallah (2013) argue that weak regulatory systems and inconsistent enforcement mechanisms contribute to the escalation of violence in resource-rich environments. In such contexts, ineffective governance allows illegal extraction networks to thrive, thereby weakening formal institutions and intensifying insecurity.

Okoli and Okpaleke (2014) further highlight that governance failures in Nigeria's security architecture, including delayed interventions and weak policing capacity, have contributed to the persistence of banditry and violent crime in resource-contested regions. These dynamics demonstrate that state actors play a dual role, either mitigating or unintentionally exacerbating insecurity, depending on institutional effectiveness.

3. Role of Non-State Actors

Non-state actors are widely recognized as central participants in resource-related conflict systems. Williams (2018) explains that armed groups and criminal networks often exploit weak governance structures to gain access to economic resources, particularly in peripheral rural areas. These actors frequently engage in illegal extraction, extortion, and territorial control, thereby reinforcing cycles of violence. Similarly, UNODC (2021) documents the growing link between illicit economies and organized armed groups, noting that resource-rich environments provide both financial incentives and operational spaces for non-state armed actors. This aligns with broader conflict theory, which suggests that economic opportunity structures significantly shape patterns of violence in fragile states.

4. Impact on Communities and Human Security

Empirical research consistently shows that resource-related conflicts have severe consequences for human security. Homer-Dixon (2010) argues that environmental and resource scarcity can produce chronic insecurity by undermining livelihoods and increasing vulnerability to violence. In addition, the United Nations Development Programme (1994) emphasizes that insecurity in resource-dependent communities extends beyond physical violence to include displacement, poverty, and loss of access to essential services. Collectively, these studies demonstrate that resource-driven conflict has multidimensional impacts on communities, affecting both material conditions and broader social stability.

5. Gaps in Empirical Literature

Despite extensive research on resource-related conflicts, several gaps persist: Most studies treat resource-conflict dynamics in broad regional terms, often neglecting localized analysis of solid mineral resources in North-Central Nigeria. Few studies simultaneously examine the interplay between state and non-state actors, governance effectiveness, and community security outcomes. Empirical research quantifying the direct link between mineral exploitation and patterns of violence, particularly in a mixed-methods framework combining qualitative and quantitative evidence, remains limited. These gaps justify the current study, which seeks to quantify the impact of solid mineral resources on insecurity, while also exploring the roles of state and non-state actors in shaping the dynamics of violence in North-Central Nigeria.

Theoretical Review

The nexus between resource wealth and conflict has been extensively examined in political economy and conflict studies, providing a robust foundation to understand the dynamics in North-Central Nigeria. Several theories are particularly relevant:

1. Resource Curse Theory

The Resource Curse Theory posits that countries or regions endowed with abundant

natural resources often experience slower economic growth, weak institutions, and higher levels of conflict (Auty 1993; Sachs and Warner 2001). In the context of North-Central Nigeria, the presence of solid minerals such as tin, columbite, and limestone does not automatically translate into local development. Instead, these resources have frequently become flashpoints for communal and politically motivated violence. This theory helps explain why resource-rich communities experience recurring insecurity despite their economic potential, highlighting the role of institutional weakness and competition for resource control.

2. Greed vs. Grievance Theory

The Greed vs. Grievance framework (Collier and Hoeffler 2004) distinguishes between economic and socio-political motivations for conflict. The “greed” perspective emphasizes that actors, including criminal networks and armed groups, may exploit resources to generate personal or organizational wealth, while the “grievance” perspective focuses on inequality, marginalization, and disputes over land or resource rights. In North-Central Nigeria, both dynamics coexist: non-state actors capitalize on mineral wealth for financial gain, while local communities engage in violent contestation due to perceived exclusion from mining benefits.

3. Political Ecology Theory

Political Ecology provides a lens to understand the interaction between natural resources, power relations, and environmental change (Robbins 2012). It emphasizes that resource conflicts are not merely economic but are deeply embedded in social, political, and ecological systems. Applying this to North-Central Nigeria, disputes over mineral-rich land are shaped by historical land tenure systems, ethnic divisions, and governance failures, illustrating that environmental and resource issues are inseparable from broader social and political inequalities.

4. Human Security Theory

Human Security Theory shifts the focus from state-centered security to the protection of individuals and communities from chronic threats, including economic deprivation, violence, and environmental hazards (UNDP 1994). In the context of solid mineral exploitation, human security is often compromised as communities face displacement, violent attacks, and disruption of livelihoods. This theory underlines the importance of policies that integrate resource management with social protection and conflict prevention.

Synthesis and Application to the Study

Combining these theoretical perspectives allows for a comprehensive understanding of the triad of resources, insecurity, and violence in North-Central Nigeria. The Resource Curse Theory explains the structural paradox of resource wealth and underdevelopment; the Greed vs. Grievance framework highlights actor motivations; Political Ecology situates conflicts within broader social and environmental contexts; and Human Security Theory underscores the impact on communities and the need

for inclusive governance strategies. Together, these frameworks provide a strong foundation for analyzing the causes, dynamics, and potential solutions to resource-related conflicts in the study area.

Research Methodology

This study adopts a mixed-methods research design, combining quantitative and qualitative approaches to provide a comprehensive understanding of the relationship between solid mineral resources, insecurity, and escalating violence in North-Central Nigeria. The mixed-methods approach is particularly suitable for this study because it allows for the triangulation of data, facilitating both statistical analysis of conflict patterns and in-depth insights into the roles of state and non-state actors in resource-related conflicts. The study employs an explanatory sequential mixed-methods design, beginning with quantitative data collection and analysis to establish the scope and patterns of resource-related violence. This is followed by qualitative investigations to explain and contextualize the statistical findings, providing deeper insights into local dynamics, governance challenges, and actors' behavior. The research focuses on selected states in North-Central Nigeria, including Plateau, Nasarawa, and Benue, which are notable for their rich solid mineral deposits and recurrent incidents of communal and resource-driven violence. These states provide a representative cross-section of the challenges posed by resource wealth and insecurity in the region. The target population includes community members living in mineral-rich areas, local government officials, security personnel, mining operators, and representatives of civil society organizations. A stratified random sampling technique will be used for the quantitative survey to ensure representation across different demographic groups, while purposive sampling will guide qualitative interviews with key informants who have detailed knowledge of resource conflicts.

The dependent variable, Insecurity, was measured using respondents' perceptions of the prevalence of violent conflict, armed banditry, territorial disputes, illegal armed activities, and threats to community safety associated with mining activities. Responses were measured on a five-point Likert scale ranging from Strongly Disagree (1) to Strongly Agree (5).

Resource Exploitation was operationalised through indicators measuring the intensity of artisanal mining activities, competition over mineral resources, illegal extraction practices, and perceived pressure on local resource governance structures. State Actors were measured through respondents' assessments of government presence, security operations, regulatory enforcement, monitoring of mining activities, and conflict management interventions within mining communities. Non-State Actors were measured using indicators relating to the activities of armed groups, informal mining networks, vigilante organisations, private security actors, and other non-governmental actors involved in resource control and conflict dynamics. Composite indices were generated by aggregating responses to relevant questionnaire items for each construct. These indices were subsequently used in the multiple regression analysis.

Result and Data Analysis

This section presents the findings obtained from the survey administered to respondents across selected mining communities in North-Central Nigeria. A total of 400 questionnaires were successfully completed and analyzed. The respondents comprised community members (200), local government officials and other state actors (100), security personnel (50), and mining operators and other non-state actors (50). The analysis begins with the descriptive statistics showing respondents' perceptions of artisanal mining, resource exploitation, insecurity, and the roles of state and non-state actors, followed by the results of the multiple regression analysis used to examine the relationship between the study variables.

The frequency of the questionnaire administered is listed above

Respondent Category	Frequency	Percentage (%)
Community Members	200	50.0
Local Government Officials/State Actors	100	25.0
Security Personnel	50	12.5
Mining Operators/Non-State Actors	50	12.5
Total	400	100.0

Source: Researchers Survey, 2025.

Frequency Distribution of Responses (400 respondents)

Question	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Q1. Resources increase violent clashes	20	30	40	150	160
Q2. Disputes over mining land cause insecurity	15	25	30	160	170
Q3. Illegal/unregulated mining escalates tension	10	20	40	170	160
Q4. Resource exploitation marginalizes communities	25	30	50	140	155
Q5. Conflicts have led to displacement/ loss of livelihoods	20	25	35	160	160
Q6. Government regulates mining effectively	50	80	100	120	50
Q7. Security agencies intervene promptly	45	75	90	120	70
Q8. Local leaders mediate disputes effectively	30	50	90	150	80
Q9. Non-state actors escalate conflicts	15	20	25	150	190
Q10. Collaboration could reduce violence	10	15	25	160	190

Source: Researchers Survey, 2025.

Notes/Interpretation:

- Questions Q1–Q5 reflect community perceptions of violence and resource impact, so higher agreement is expected among community members.
- Questions Q6–Q8 reflect perceived effectiveness of state and local actors, so there is more variation and neutrality.
- Questions Q9–Q10 reflect perceptions of non-state actors' role, showing strong agreement that they escalate conflict, and optimism about collaboration reducing violence.

Regression Results

Model:

$$Insecurity = \beta_0 + \beta_{1_{Resource\ Exploitation}} + \beta_{2_{state\ actors}} + \beta_{3_{non-state\ actors}} + \varepsilon$$

Predictor	Coefficient (β)	Std. Error	t-value	p-value
Constant	-0.534	0.610	-0.875	0.382
Resource_Exploitation	0.325	0.016	19.886	0.000
State_Actors	-0.163	0.024	-6.745	0.000
Non_State_Actors	0.473	0.052	9.090	0.000

Model Summary:

- **R² = 0.677**, indicating that approximately 68% of the variation in insecurity is explained by resource exploitation and the roles of state and non-state actors.
- **F-statistic = 276.5, p < 0.001**, showing that the model is statistically significant.

Interpretation of Results

The regression analysis reveals a statistically significant positive relationship between resource exploitation and insecurity ($\beta = 0.325$, $p < .001$). This finding suggests that increasing levels of artisanal mining and resource extraction are associated with higher levels of insecurity within mining communities. The result supports the argument that competition over valuable mineral resources creates conditions that encourage violent conflict and criminal activities.

The analysis further indicates that non-state actors significantly contribute to insecurity ($\beta = 0.473$, $p < .001$). The relatively larger coefficient suggests that the activities of armed groups, informal mining networks, and other non-state actors constitute a major driver of insecurity in mineral-rich areas.

Conversely, the role of state actors is negative and statistically significant ($\beta = -0.163$, $p < .001$), indicating that effective government intervention, security presence, and regulatory oversight help reduce insecurity. This finding highlights the importance of state capacity in managing resource-related conflicts.

The model explains approximately 67.7% of the variation in insecurity ($R^2 = 0.677$), while the F-statistic (276.5, $p < .001$) confirms the overall statistical significance of the model. Collectively, the findings demonstrate that resource exploitation, state actors, and non-state actors are important predictors of insecurity in mining communities across North-Central Nigeria.

Discussion of the Findings

Theme 1: Impact of Solid Mineral Resources on the Escalation of Violence and Insecurity

The study examined how the proliferation and exploitation of solid mineral resources shape the dynamics of violence and insecurity in North-Central Nigeria. The regression results reveal that resource exploitation exerts a strong and statistically significant positive influence on insecurity ($\beta = 0.325$, $p < 0.001$). This finding quantitatively confirms that the intensity of mineral extraction is directly associated with the escalation of violent conflicts across the region. From the survey, approximately 78 percent of respondents either agreed or strongly agreed that areas rich in mineral resources, such as tin, limestone, and lead, have experienced heightened insecurity. Community and non-state respondents, in particular, reported higher perceptions of conflict compared to state officials. This reflects widespread awareness of the linkage between resource endowment and contestation.

The empirical finding resonates with the Resource Curse Theory, which argues that natural resource abundance, in the absence of strong governance, often becomes a catalyst for conflict and underdevelopment (Auty 2001; Collier and Hoeffler 2004). In North-Central Nigeria, solid minerals have become sites of violent competition among local elites, artisanal miners, and armed groups, reflecting what is termed the “petro-violence paradox,” which is an adaptation of the same logic in mineral economies.

Qualitative data further illuminate these quantitative patterns. A community elder from Plateau State remarked that:

“Wherever there is tin or limestone, you always hear gunshots or fights over who has rights to the land.”

Similarly, a mining operator in Nasarawa State stated:

“Illegal miners move in, and soon tensions flare between them and the local youth; the government does not intervene quickly.”

These narratives highlight a central dynamic, which is this: the absence of effective governance mechanisms allows resource access disputes to evolve into full-scale communal violence. The weak institutional regulation of artisanal mining licenses and overlapping land ownership rights further complicate this problem, turning local economies of extraction into economies of violence. Empirical evidence from event records supports this interpretation. The 2018 Jos North clashes over limestone mining sites resulted in dozens of deaths and the displacement of more than 3,000 residents. Similarly, in Benue and Nasarawa, violent outbreaks near mineral belts such as Awe and Logo have mirrored this pattern. These incidents confirm the quantitative findings that resource exploitation is a structural driver of insecurity rather than merely an economic opportunity.

Overall, this theme establishes that solid mineral wealth in North-Central Nigeria operates as a “double-edged sword,” a source of local revenue and livelihood, but also a potent driver of violent contestation. The convergence of statistical, qualitative, and event-based evidence points to a systemic link between mineral exploitation and insecurity, driven by weak governance, economic desperation, and the strategic manipulation of resource access by political elites.

Theme 2: Role of State and Non-State Actors in Managing or Exacerbating Resource Conflicts

The second objective investigated the relative roles of state and non-state actors in either mitigating or amplifying resource-induced insecurity. The regression analysis revealed that state actors exhibit a negative relationship with insecurity ($\beta = -0.163$, $p < 0.001$), while non-state actors display a positive and significant relationship ($\beta = 0.473$, $p < 0.001$). Together, these results suggest that the state’s presence and efficiency reduce the likelihood of violence, whereas the activities of non-state actors intensify conflict. Survey data further demonstrate these dynamics. Approximately 42 percent of respondents agreed that state actors, when effective, contribute positively to conflict management, but 40 percent remained neutral or disagreed, indicating inconsistent experiences of government intervention. Conversely, over 85 percent perceived that non-state actors, including local militias, illegal miners, and private security outfits, exacerbate insecurity.

These findings align with the Greed and Grievance Model ([Collier and Hoeffler 2004](#)), which posits that resource-driven conflicts emerge when the potential gains from exploitation surpass the risks of confrontation, particularly in environments with weak institutions. Non-state actors often act as rent-seekers, exploiting mineral revenues for territorial control. Meanwhile, state agencies frequently lack the logistical capacity or political will to regulate such activities effectively.

Qualitative accounts reinforce these patterns. A security officer in Benue disclosed:

“Sometimes we arrive late; by the time we intervene, the conflict has already escalated. Local leaders are not always cooperative.”

A community respondent from Plateau added:

“Politicians sometimes favor one group over another, making the fights worse. People no longer trust that the government is neutral.”

Similarly, a civil society leader observed:

“Non-state actors, including armed groups and illegal miners, often intimidate locals; without their cooperation, peace initiatives fail.”

These testimonies reveal that the crisis of governance, manifested through delayed intervention, selective enforcement, and political bias, creates a vacuum that non-state actors exploit. Thus, while the state theoretically holds the mandate for conflict management, its fragmented capacity allows non-state actors to shape the

security landscape. Event data provide further validation. In Plateau State's 2021 tin-mining conflicts, for example, state intervention temporarily reduced clashes through the deployment of security forces, but the absence of long-term institutional monitoring enabled the violence to resurface months later. This pattern typifies a cyclical governance failure; state responses are reactive rather than preventive. The triangulated evidence underscores that the coexistence of weak state regulation and empowered non-state actors sustains a political economy of insecurity. The non-state networks profit from the disorder, while the state struggles to reassert authority. The regression results thus encapsulate a broader structural challenge: the imbalance of power between formal and informal actors in the mineral sector.

Theme 3: Corruption, Elite Struggles, and External Resource Pressures

Beyond institutional coordination challenges identified in this study, the findings also point to deeper structural dynamics involving corruption, elite competition, and external resource pressures that collectively shape governance outcomes in Nigeria's solid minerals sector. The prevalence of illegal mining activities and weak regulatory enforcement can be interpreted not only as administrative inefficiencies but also as manifestations of corruption-driven distortions within governance structures. In line with Mauro (1995) and Rose-Ackerman (1999), such corruption weakens bureaucratic effectiveness, undermines accountability mechanisms, and creates opportunities for selective enforcement of mining regulations, thereby reducing the capacity of the state to effectively govern the sector.

Furthermore, the pattern of federal-state tensions and contested control over mining revenues reflects broader struggles among political and local elites over resource capture. Consistent with Bayart's (1993) "politics of the belly" and Reno's (1995) concept of shadow states, access to mineral rents appears to be embedded within networks of patronage and elite bargaining, where formal governance institutions are frequently influenced or bypassed by informal power structures. This dynamic helps explain the persistence of fragmented authority and weak policy coordination observed in the sector.

In addition, the findings suggest that Nigeria's artisanal mining economy is increasingly integrated into broader transnational mineral networks, where external actors such as mineral buyers, intermediaries, and cross-border trading systems reinforce informal extraction practices. These external links sustain demand for illegally sourced minerals, thereby weakening domestic regulatory efforts and further complicating governance outcomes. Collectively, these dynamics indicate that governance challenges in the solid minerals sector extend beyond institutional design failures to include corruption-induced inefficiencies, elite-driven resource competition, and transnational economic pressures that shape extraction and distribution processes.

Synthesis of Themes

The two themes converge to depict a complex but coherent reality. Solid mineral resources are at the center of an intertwined system of insecurity, governance weakness, and non-state predation. Quantitative data confirm that resource exploitation and non-state actor activity are statistically significant drivers of violence, while qualitative and event analyses expose how governance gaps allow these forces to thrive.

The findings reveal that the triad of resources, insecurity, and actor dynamics forms a self-reinforcing cycle in North-Central Nigeria:

1. Resource exploitation generates competition and grievance.
2. Weak state oversight fails to mediate these disputes effectively.
3. Non-state actors capitalize on the vacuum to consolidate economic and territorial control.

This interplay transforms mineral wealth into a security liability, suggesting that peace and stability in North-Central Nigeria depend not only on resource control but also on governance reform and the demilitarization of local economies of extraction.

Conclusion and recommendations

This study examined the complex interaction between solid mineral resources, insecurity, and escalating violence in North-Central Nigeria, emphasizing the roles of state and non-state actors. Through a mixed-method approach, integrating survey data, regression analysis, and qualitative insights, the research demonstrated that solid mineral exploitation significantly contributes to the prevalence of insecurity, particularly in mineral-rich communities such as those in Plateau, Nasarawa, and Benue States.

The regression results confirmed that resource exploitation and non-state actors have a strong positive relationship with insecurity, while state actor engagement has a mitigating effect. These findings highlight the persistent structural dilemma where natural resource abundance, instead of fostering prosperity, fuels contestation and violence. Weak governance institutions, unregulated mining, and the proliferation of armed non-state groups collectively sustain a cycle of insecurity.

The qualitative findings reinforced this statistical pattern. Local testimonies described how resource control disputes, poor regulatory oversight, and political interference exacerbate communal divisions. Several respondents underscored the perception that government interventions are inconsistent, reactive, and, at times, biased toward certain interest groups. These perspectives echo the broader “resource curse” thesis, wherein natural resource wealth breeds political instability when not accompanied by effective governance and equitable distribution.

In sum, the study concludes that insecurity in North-Central Nigeria is not merely a by-product of poverty or ethnic rivalry, but a symptom of structural governance failure around resource management. The region’s solid mineral potential continues

to invite violent competition because state institutions lack the capacity, neutrality, and coordination needed to regulate extraction, mediate disputes, and enforce accountability. The findings underscore an urgent need for policy interventions that integrate economic governance, inclusive peacebuilding, and local participation.

Recommendations

1. Strengthen Institutional Frameworks for Mineral Governance

The federal and state governments should review and harmonize mining laws to clarify ownership, licensing, and revenue-sharing structures. This will reduce jurisdictional overlaps between federal agencies and state authorities, which currently fuel conflict. Establishing joint mineral management committees involving community leaders, local governments, and security agencies would promote shared responsibility and transparency.

2. Enhance Security Presence and Intelligence Coordination

Security operations in mineral zones should shift from reactive responses to preventive intelligence gathering. A coordinated security command structure involving the police, military, and civil defense corps is essential to monitoring illegal mining and disarming violent groups. Incorporating local vigilantes into formal community policing structures could improve trust and early-warning capabilities.

3. Promote Community Participation and Resource Benefit Sharing

Communities located within mineral-rich areas should not be treated as passive observers. The government should institutionalize Community Development Agreements (CDAs) that ensure a defined percentage of mining revenues is reinvested locally in infrastructure, education, and health. Such arrangements would address grievances and reduce the appeal of violent mobilization.

4. Regulate and Formalize Artisanal Mining

The Ministry of Mines and Steel Development, in partnership with state governments, should formalize artisanal and small-scale mining through licensing, capacity training, and monitoring. This will reduce illegal operations and promote responsible mining practices while increasing state revenue.

5. Address the Influence of Non-State Actors and Political Interference

A comprehensive deradicalization and disarmament program targeting armed groups engaged in resource-related violence should be implemented. At the same time, political actors who sponsor or shield illegal miners must be held accountable through independent judicial and anti-corruption mechanisms.

6. Integrate Peacebuilding into Resource Management Policy

Resource governance should be situated within a broader peacebuilding framework. The government, in collaboration with civil society and traditional councils, should promote dialogue platforms to mediate inter-communal disputes and build local trust. This can prevent resource competition from escalating into violence.

7. Invest in Alternative Livelihoods and Human Capital Development

To reduce dependency on unregulated mining, state governments should invest in vocational training, agribusiness, and entrepreneurship initiatives for youth in mineral-producing areas. Diversifying local economies would not only mitigate unemployment-induced violence but also strengthen economic resilience.

The study ultimately illustrates that the triad of solid mineral resources, insecurity, and escalating violence is a political economy problem rather than a purely security one. Addressing it requires a governance-centered approach that balances economic development with social inclusion and security reform. Peace in North-Central Nigeria will remain elusive until the extractive sector is embedded within a transparent, participatory, and accountable framework that prioritizes citizens over elite or corporate interests.

References

- Aning, K., and M. Abdallah.** 2013. Understanding the complexity of armed violence in West Africa. *African Security Review* 22(1): 1-14.
- Auty, R. M.** 1993. *Sustaining development in mineral economies: The resource curse thesis*. Routledge.
- _____. 2001. *Resource abundance and economic development*. Oxford University Press.
- Bayart, J. F.** 1993. *The state in Africa: The politics of the belly*. Longman.
- Buzan, B., O. Wæver, and J. de Wilde.** 1998. *Security: A new framework for analysis*. Lynne Rienner Publishers.
- Collier, P., and A. Hoeffler.** 2004. "Greed and grievance in civil war." *Oxford Economic Papers* 56(4): 563-595. <https://doi.org/10.1093/oeq/gpf064>.
- Duffield, M.** 2001. *Global governance and the new wars: The merging of development and security*. Zed Books.
- Homer-Dixon, T. F.** 2010. *Environment, scarcity, and violence*. Princeton University Press.
- Ide, T., C. Bruch, A. Carius, K. Conca, G. Dabelko, R. Matthew, and E. Weinthal.** 2021. "The past and future(s) of environmental peacebuilding." *International Affairs* 97(1): 1-16. <https://doi.org/10.1093/ia/iiaa177>.
- International Crisis Group.** 2020. "Violence in Nigeria's North West: Rolling back the mayhem." Africa Report No. 288. Brussels: International Crisis Group. <https://www.crisisgroup.org/africa/west-africa/nigeria/288-violence-nigerias-north-west-rolling-back-mayhem>.
- Kaldor, M.** 2012. *New and old wars: Organized violence in a global era* (3rd ed.). Polity Press.

- Le Billon, P.** 2012. *Wars of plunder: Conflicts, profits and the politics of resources*. Oxford University Press.
- Mauro, P.** 1995. "Corruption and growth." *Quarterly Journal of Economics* 110(3): 681-712. <https://doi.org/10.2307/2946696>.
- Okoli, A. C., and N. E. Lenshie.** 2018. "Nigeria: Nomadic migrants and rural violence in Nigeria." *Conflict Studies Quarterly* 25: 68-85. <https://doi.org/10.24193/csq.25.4>.
- Okoli, A. C., and F.N. Okpaleke.** 2014. "Banditry and crisis of public safety in Nigeria: Issues in national security strategies." *European Scientific Journal* 10(4): 350-362. <https://doi.org/10.19044/esj.2014.v10n4p%25p>.
- Reno, W.** 1995. *Corruption and state politics in Sierra Leone*. Cambridge University Press.
- Robbins, P.** 2012. *Political ecology: A critical introduction* (2nd ed.). Wiley-Blackwell.
- Rose-Ackerman, S.** 1999. *Corruption and government: Causes, consequences, and reform*. Cambridge University Press.
- Ross, M. L.** 2015. "What have we learned about the resource curse?" *Annual Review of Political Science* 18: 239-259. <https://doi.org/10.1146/annurev-polisci-052213-040359>.
- Sachs, J. D., and A. M. Warner.** 2001. "The curse of natural resources." *European Economic Review* 45(4-6): 827-838.
- United Nations Development Programme (UNDP).** 1994. *Human development report 1994: New dimensions of human security*. Oxford University Press.
- United Nations Office on Drugs and Crime (UNODC).** 2021. *Crime and development in Africa*. United Nations.
- Williams, P. D.** 2018. *War and conflict in Africa* (2nd ed.). Polity Press.

Social Media as a Disinformation Infrastructure: Tactics, Strategies, and National Security

Captain Assistant Lecturer George-Adrian AIONESEI*

*"Henri Coandă" Air Force Academy, Braşov, Romania

e-mail: aioneseiadrian11@gmail.com

 <https://orcid.org/0009-0000-6573-7888>

Abstract

For the last two decades, the global information environment has become a place for strategic competition and superiority, where boundaries between communication, propaganda, and psychological operations have become much more blurred. The evolution of social media platforms has amplified this transformation, switching from mere channels of civic expression into solid influence infrastructures capable of shaping perceptions, behaviors, and political attitudes. In this context, disinformation is no longer a marginal phenomenon but rather a central instrument for hybrid and cognitive warfare, used against social cohesion and trust in democratic institutions. Thus, this paper analyzes the role of social media in undermining national security, focusing on disinformation tactics and strategies used in the current digital environment. Through this study, we manage to use a combined sequence model to establish links and relationships between the tactics (micro-level) used in disinformation campaigns and the strategies (macro-level) used in order to affect society and the way people think and behave. This article is part of a larger PhD research effort that focuses on the impact of social media instruments in modern conflicts, serving as a means to analyze the role of disinformation in the current digital environment.

Keywords:

Disinformation; Tactics; Strategies; Social Media; National Security; Online.

Article info

Received: 11 April 2026; Revised: 30 April 2026; Accepted: 4 June 2026; Available online: 30 June 2026

Citation: Aionesei, G.A. 2026. "Social Media as a Disinformation Infrastructure: Tactics, Strategies, and National Security."
Bulletin of "Carol I" National Defence University, 15(2): 27-50. <https://doi.org/10.53477/2284-9378-26-17>



© „Carol I” National Defence University Publishing House

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC-SA)

Introduction

Changes in the communication environment have exceeded the technological levels and generated a structural reconfiguration of modern social power. The creation and development of social media networks and platforms have fundamentally modified the way individuals, institutions, and states communicate, share information, and build realities. As Castells (2009, 38-42) mentions, the shift towards a society of networks has transformed the way communication works in an environment where information becomes a strategic currency.

Once social media platforms, such as Facebook (2004), YouTube (2005), Twitter (2006), or later Telegram, Instagram, and TikTok, have become more popular, everyone has changed their status from a passive consumer to an active agent by creating and disseminating information. This democratic process of communication was initially perceived as a vector of freedom and civic mobilization, very well manifested during the Arab Spring. However, the new openness to free expression involved systemic vulnerabilities, mainly due to a lack of editorial filters, speed of dissemination, and dependence on the algorithmic logic of attention (Chadwick 2017, 19-22).

Social networks cannot be seen anymore as mere cultural and societal interaction spaces, but rather as strategic infrastructures, where information and cognitive confrontations become the centerpieces of modern conflicts. They allow both social mobilization and political manipulation. As Benkler, Faris, and Roberts (2018, 14-23) mention, the digital platforms' architecture favors emotional polarization and distorted narratives dissemination, thus creating the ideal environment for coordinated disinformation campaigns. After 2014, events such as the conflict in Ukraine, electoral implications in the United States, or medical conspiracies during COVID-19, altogether made it clear that social media has grown into a new global threat that might seriously affect national security. By using these platforms, different actors can influence perceptions, undermine public trust in governmental institutions, and destabilize democracy without any kind of military intervention. As a response, organizations such as NATO, the European Union, or the Council of Europe officially recognized information manipulation and external interferences as forms of hybrid threats (EEAS 2025b, 7-11, NATO 2022, 3-6).

Through this article, we aim to explore the way in which social media instruments have become central tools in shaping modern conflicts, focusing on the tactical and strategic use of disinformation that affects national security and public trust. Also, it seeks to identify the mechanisms through which digital ecosystems enable the dissemination and normalization of manipulative narratives. The overarching objective is to provide an analytical framework for understanding the causal chain of disinformation in the digital environment, from disinformation tactics to cognitive effects and ultimately to security implications affecting social cohesion, institutional legitimacy, or state-citizen relationships.

1. Methodology

This article employs a deductive, qualitative literature synthesis, combined with a conceptual framework-building approach. The analytical framework was not meant to conduct a statistical meta-analysis, but rather synthesized peer-reviewed literature, institutional reports, and policy documents addressing disinformation, hybrid warfare, cognitive warfare, and platform governance, published primarily between 2016 and 2025. The synthesis helped develop an analytical model explaining how disinformation tactics can be combined with social media platforms to obtain strategic results with implications for national security. Sources were identified through systematic searches of academic databases (Scopus, Web of Science) and grey literature repositories (RAND, EEAS, NATO), using the search terms “disinformation tactics”, “social media manipulation”, “cognitive warfare”, “hybrid threats”, and “information operations”. Inclusion criteria required that sources address either the mechanisms of disinformation production and the dissemination or their security-level effects, ensuring analytical relevance to both the tactical and strategic dimensions of the framework.

The sources selection consisted of a thematic and conceptual coding procedure. First, disinformation mechanisms were identified and coded as tactical categories, including content fabrication, source deception, coordination and amplification, infrastructure exploitation, discourse disruption, and AI-enabled production tactics. Second, broader objectives regarding disinformation campaigns were coded as strategic categories, including delegitimization of institutions, polarization, confusion, attention control, normalization, crisis exploitation, and erosion of democratic resilience. Each of the two categories was the subject of further codification by three criteria: recurrence across multiple analyzed sources or documented campaigns, functional role within the disinformation process, and strategic significance in producing measurable security-level effects.

The two-tier analytical framework – distinguishing between disinformation tactics (micro-level operational mechanisms) and disinformation strategies (macro-level objectives) – was developed deductively, drawing on established theoretical models including the information disorder framework ([Wardle and Derakhshan 2017, 23-32](#)), affordance theory as applied to social media platforms ([Wu, Wu and Xiao 2025, 1-5](#)), and RAND studies on strategic influence operations ([Paul and Matthews 2016, 2-9](#); [Mazarr, et al. 2019, 11-27](#)). The categorization and interdependency logic presented in Table 1 represent the synthesized output of this analytical process. The framework is conceptual rather than empirical, but to strengthen the empirical grounding of the framework, the article shows an application of the model on three cases related to Russia’s disinformation campaigns in the war against Ukraine, such as Zelensky’s surrender deepfake, Bucha massacre disinformation, and Operation Overload. The three cases are not intended as a statistical validation method, but rather as a concrete illustration of the model’s analytical applicability.

2. Theoretical Framework – Disinformation, Hybrid warfare, and Cognitive warfare

If during the 20th century, the state had the power to broadcast filtered and manipulated information through governmental channels in order to control the population, the information flow nowadays has become completely decentralized, being interactive, participatory, driven by algorithms, and orchestrated by state and non-state actors. This shift in standards has led to a democratization of communication, and at the same time, has opened a gate to new forms of systemic manipulation.

Disinformation, considered once an auxiliary part of hybrid warfare, has become a central instrument of modern warfare. In the current context, it can be seen as the most sophisticated expression of combining technology with psychology and geopolitics. In other words, it can be defined as the deliberate dissemination of false or distorted information to influence perceptions, behaviors, and decisions (Wardle and Derakhshan 2017, 20-21; Baines, O'Shaughnessy and Snow 2019, 56-59). Unlike misinformation, which represents an unintended error, disinformation involves strategic intentionality, planning, and coordination. In this article, we will focus specifically on disinformation because it involves this intentional aspect that is manipulative and has a strategic finality. In current European terminology, these phenomena are part of a new concept – FIMI – *Foreign Information Manipulation and Interference*, as defined by the European External Action Service (EEAS 2025a, 4-8), which consists of a set of coordinated actions meant to alter information and undermine democratic activities.

Through its nature, disinformation acts simultaneously on three complementary dimensions: communication, psychology, and institution. For the first dimension, disinformation is used to intentionally distort the narrative framework, using real content in false contexts, or create and disseminate persuasive messages to target emotions. The second dimension is based on cognitive biases, such as confirmation bias or motivational thinking, exploiting an individual's natural predisposition to accept information that confirms their personal identity and values (Lewandowsky, Ecker and Cook 2017, 353-369). For the institutional dimension, the main role of disinformation is to diminish trust in authorities, mass media, and the capacity of institutions to distinguish between what is true and what is false.

When we think about the institutional dimension mentioned above, we also think of institutional security. But if we expand it further, we can refer to national security. This concept of national security cannot be limited anymore to only territorial and military actions, taken to protect the critical physical infrastructures in the traditional way. Recent literature shows that security needs to be understood also by reference to information resilience, and the institutions' capacity to maintain the

public trust of the population, to adapt the information dissemination mechanisms to current threats, and to help society respond coherently to information distortions (Dragomir, Ruas-Araujo and Horowitz 2024, 1-10; Uusikylä, et al. 2024, 1-18). From this perspective, the vulnerability of a state does not come only from direct external constraints, but also from weakening the internal functions that are able to affect social coordination, institutional legitimacy, or democratic processes.

This multidimensional approach does not necessarily start and end with these three extents, but rather it explains why disinformation is such an essential element in *hybrid warfare*. The concept of hybrid warfare describes how state and non-state actors employ a combination of conventional and non-conventional means (military, cyber, economic, information, diplomatic) to achieve political objectives without escalating to open armed conflict. Within this spectrum, disinformation is the element with a great capacity to act psychologically and cognitively, because it does not affect physical infrastructures, but rather takes over public perception.

After the annexation of Crimea and pro-Kremlin campaigns targeting the European information space, it has become clear that hybrid warfare is supported by a strong cognitive component. Through disinformation, actors do not just aim to convince, but also to create confusion amongst people. By flooding the public space with multiple and contradictory versions of the “truth”, which most of the time cannot be fact-checked fast enough, the trust in public institutions and official information sources starts to erode, ultimately making citizens perceive reality as an unstable construct. Pomerantsev (2019, 123, 164) refers to this strategy as “post-truth era”, where manipulation and content control are not made of clear lies, but through constant relativity of truth.

This recent evolution in the strategic thinking of affecting people’s minds has been conceptualized as *cognitive warfare*, defined as the most sophisticated type of modern conflict where the human mind becomes the operational domain. In the strategic literature, cognitive warfare depicts the combination of actions that aim to influence cognitive processes, such as perception, attention, emotion, and rational thinking, factors that can be manipulated to obtain political objectives without physical contact (Bernal, et al. 2020, 9-11). RAND analysis shows that this approach is an extension of influential operations (information/influence), switching from persuasion to affecting the decision-making process of the target, including information overload, strategic ambiguity, or bias exploitation (Paul and Matthews 2016, 2-9, Mazarr, et al. 2019, 11-27). Therefore, the main objective of cognitive warfare is to make people act voluntarily against their will. Here is where the reflexive control takes shape (de Goeij 2023, 97-108), as the mechanism through which an actor provides filtered and apparently neutral information, but conceived in such a way as to manipulate the adversary to make decisions that are beneficial to the offender. This strategy is most of the time amplified by algorithms, microtargeting, and influential networks.

If the cyber domain involves technological infrastructures, the cognitive domain aims for mental infrastructures (perceptions and behaviors). A main role in this equation is played by social networks, because of their technological design, algorithms, and manipulative content (Vosoughi, Roy and Aral 2018, 1146-1153). Unlike traditional propaganda, which was dependent on centralized control of mass media, current digital dissemination allows dispersed control, based on the voluntary participation of users. The European Union has tried to respond to these challenges by adopting the Digital Service Act, meant to raise transparency about social media platforms and each user's responsibility. However, there is a structural asymmetry between the efforts required to fact-check and the ease of spreading false information. Truth demands time, expertise, and validation, whilst falsehood only needs channels and networks through which it can circulate freely and instantaneously. This asymmetry represents the main strategic advantage for modern actors that use disinformation as a weapon.

If we consider the flow of (dis)information through social media in society nowadays, as mentioned above, we can follow a sequential escalation process through which disinformation grows from platform-level tactics into strategic security effects. Starting from opportunities offered by social media platforms, such as algorithmic recommendations, network virality, or low effort visibility, actors have the structural conditions to apply and shape manipulation. By using this environment, they can deploy disinformation tactics to maximize dissemination and influence. These tactics, combined in sequence or simultaneously, can generate cognitive effects at the individual or small group level, involving confusion, misperception, or emotional activation, which later will be translated into behavioral responses, engaging people in sharing content, blaming the authorities or institutions, or manifesting outrage towards governments. By using repetition and algorithmic dissemination through networks, these actions form social amplification loops that transform individual encounters into collective ones. Over time, these processes enable the consolidation of disinformation strategies, understood as the macro-level objectives, including polarization or delegitimization of institutions. In this sense, the strategies do not develop on their own but are implemented through the repeated and coordinated use of tactical mechanisms, which, over time, are able to weaken social cohesion, reduce trust in institutions, and affect national security.

Although this sequence captures the big picture of the escalation from platform dynamics to national security implications, this paper focuses specifically on the disinformation tactics and strategies and the relationship between them. To analyze these dynamics systematically, we will address a two-tier analytical model that distinguishes between the tactics and strategies used in the dissemination of disinformation. **Tactics** refer to the micro-level mechanisms through which disinformation operates in social media environments, including practices such as narrative engineering, coordinated inauthentic behavior (CIB), automated amplification, or algorithmic exploitation to increase visibility and engagement

(Bradshaw and Howard 2018, 11-15; Metzler and Garcia 2024, 735-748). **Strategies**, on the other hand, refer to the macro-level objectives that these mechanisms are intended to advance, including delegitimization, polarization, or deterrence by confusion. Although there are no separate frameworks that capture the evolution of disinformation from tactics to strategies that affect national security, there are several models that support individual phases. The information disorder framework (Wardle and Derakhshan 2017, 23-32) conceptualizes disinformation as a process involving agents, messages, and interpreters, while affordance-based models (Wu, Wu and Xiao 2025, 1-5) show how platform features influence cognitive, affective, and behavioral responses. Also, studies on strategic communication, hybrid threats, and cognitive warfare explain how sustained manipulation can produce political and security effects (Dov Bachmann, Putter and Duczynski 2023, 1-10). By considering these models, this article proposes an integrative model, illustrated below in Figure 1.

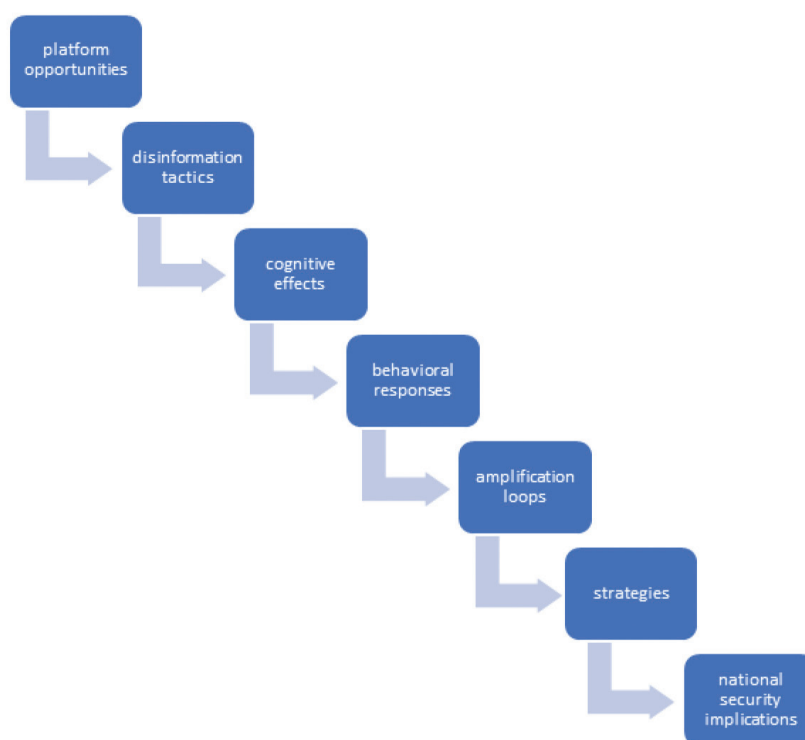


Figura 1 The process through which disinformation evolves from social media platforms to national security threats
Source: Author's interpretation.

3. Tactics and Mechanisms of Disinformation on Social Media

As we mentioned before, disinformation is not a random phenomenon but rather a deliberate, structured process used as a key pillar in hybrid and cognitive warfare strategies. Its success derives from blending technologies such as social media platforms with their algorithms, psychological manipulation, and coordinated amplification of messages. To understand how disinformation operates at the micro-level, we will analyze it through the main categories of tactics. These are isolated techniques, but can be combined in different ways across content,

communication channels, sources, distribution, visibility, or reception. Studies on this subject suggest that disinformation needs to be analyzed from the perspective of the process involving the interaction between content, network amplification, and user engagement on social media platforms in various forms ([Chadwick and Stanyer 2022](#), 1-17). Based on this starting point and other studies ([Bradshaw and Howard 2018](#), 9-15; [Kruijver, et al. 2025](#), 6-20), we can distribute tactics in different categories, each corresponding to a distinct dimension of manipulation.

3.1. Content fabrication and manipulation tactics

This category focuses on the information substance of messages. From production of the content (text, video, audio), to more subtle forms of distortion, disinformation does not rely solely on false information, but also combines facts with manipulative framing, emotional narratives, or conspiracy-based descriptions that provide a simplified and more acceptable interpretation of reality ([Egelhofer and Lecheler 2019](#), 97-111).

Fully fabricated content is one of the most visible mechanisms of this category, by promoting entirely invented facts, under different forms (posts, articles, breaking news, rumors, or pseudo reports). There are also other subtle tactics, such as placing real images or facts in falsified contexts, omitting information that might change users' interpretation, or using narrative engineering to rearrange and organize information related to an event in such a manner that it gives a different meaning, such as betrayal, corruption, censorship, or "us versus them" conflict. In these cases, manipulation lies less in inventing reality and more in distorting the conditions under which reality is interpreted. Other tactics manipulate credibility and evidence by invoking "experts" from different fields (politicians, medics, fabricated witnesses), pseudo-documents, or so-called leaks from the government, big companies, or influential people. More advanced and modern forms include deepfakes and synthetic media, by using AI to impersonate public figures or fabricate events ([Farid 2025](#), 1-9), and false flag content, which is designed to appear as if it originated from another actor, group, or community, thereby avoiding legal measures that can be taken against them ([Ferreira 2022](#), 1537-1540). These two tactics are strategically significant because they involve an increase in uncertainty around the authenticity and attribution, making it hard for audiences to know exactly who is responsible for a specific piece of content, being closely related to the next category of tactics.

Content fabrication and manipulation tactics have the role of distorting the relationship among information, evidence, and interpretation. Their effectiveness does not rely solely on the production of falsehood but also on their capacity to alter context, manipulate credibility, and intensify emotion, making them central to strategies such as delegitimization, polarization, confusion, or crisis exploitation.

3.2. Content identity or source tactics

Another important category of tactics that manipulate perceptions of credibility and authenticity of the content refers to the source or sources of the content. Going beyond the content alteration, these tactics target the perceived origin of messages,

such as fake personas or pseudo-sources that mimic legitimate ones. In a social media environment, users rely on elements such as the identity of an account, popularity, repetition, or apparent credibility to interact with it. Therefore, manipulating who appears to speak, what and how many voices support a narrative, and whether they seem authentic, is a great mechanism of influence used by actors.

One of the most common tactics used in this category is the use of fake personas, or sock puppet accounts, which are fake online identities created to praise, defend, support, or denigrate a person, group, or entity, to manipulate the population's decisions. This tactic is used to disseminate specific content online, while the source might be blocked or restricted. It is effective through the simulation of ordinary users, making coordinated manipulation look like a spontaneous public opinion. Closely related are bots – automated accounts used for posting and sharing content artificially, according to predefined instructions. They can reduce the cost of dissemination and increase the speed and volume of engagement, allowing actors to grow the visibility of a selected narrative ([Alkathiri and Slhoub 2025](#), 1-7). If bots are automated mechanisms, trolls are usually human-operated accounts that take part in the disinformation process aggressively, ironically, or provocatively to push specific narratives, or to discourage the opposition ([Hameleers 2023](#), 4-6). Another complex form of source deception is represented by coordinated inauthentic behavior (CIB), a tactic based on networks of authentic accounts, which are duplicated, falsified, and operated automatically or manually, coordinated in such a manner that they hide the real author and simulate organic behaviors ([Murero 2023](#), 3-4). Astroturfing, close to CIB, involves an organized activity that gives the impression of an organic and spontaneous behavior in favor of or against an idea or opinion, to give it popular consensus, but that does not exist. CIB and astroturfing are relevant for disinformation because they do not distort information, but rather falsify the social media environment in which information is engaged, evaluated, and utilized ([Hameleers 2023](#), 4-6).

3.3. Coordination and amplification tactics

By using these types of tactics, disinformation is scaled beyond the initial point of appearance. They exploit ways in which visibility and repetition can improve, giving the impression that certain contents are organically widespread, urgent, or socially validated. Paul and Mathews ([2016](#), 1-10) depicted this logic through the firehose of falsehood model, highlighting how high volume and repetitive content can overwhelm audiences and their rational thinking.

These tactics include automated amplification, where bots increase visibility through artificial posts, shares, and reactions; coordinating posting where multiple accounts push the same narrative across groups to create an initial impulse; and hashtag or keyword hijacking, where actors insert manipulative narratives in already popular groups and environments, to increase visibility and credibility ([Mustafa, Luczak-Roesch and Johnstone 2025](#), 48-54). Other forms include comment flooding, which overwhelms users with an avalanche of comments and replies, to confuse, intimidate, and finally incapacitate them from deciding; and influencers laundering, where the

content is taken over by recognizable figures so it appears to be more organic and believable.

Socially, these tactics distort the apparent distribution of opinion by bringing manipulated narratives to the front, to appear mainstream. Users' engagement with this content translates into more visibility, creating feedback loops, and ultimately into shaping perception, credibility, and group behavior.

3.4. Platform infrastructure exploitation tactics

Rather than focusing on audience persuasion, these tactics are used to manipulate the algorithms, recommendation systems, and engagement metrics to increase visibility and persistence. They help place strategic content within platform ecosystems, based on preferences, thereby maximizing exposure among specific audiences (Clemons, et al. 2024, 5-11). By using these tactics, actors enable the use of social media platforms as a force multiplier for influence. There are a few tactics, such as optimizing messages which help the recommendation systems of the algorithms to give users specific content for their interests; search flooding, where actors push results, stories, or narratives to dominate specific searches associated with names, events, or topics; and microtargeting, which are used by actors to deliver tailored messages to specific audience segments, based on their interests, vulnerabilities, identities, or behavioral patterns (Kruijver, et al. 2025, 15-16).

These tactics have a great impact through visibility manipulation and audience segmentation. By using algorithmic exploitation, these tactics make selected narratives appear more popular, relevant, or more important than they are. Repeated exposure can increase familiarity and perceived credibility, while personalized messaging can exploit pre-existing fears or vulnerabilities. Also, the impact of microtargeting, as exposing different groups to different versions of reality, can end up in a faulty collective understanding and interpretation of an event, representing a starting point for polarization in society.

3.5. Tactics of suppression and discourse disruption

In this category of tactics, the objective consists of weakening opposing voices to respond effectively. Coordinated harassment, intimidation, or agenda diversion are just a few of those tactics aimed to silence critics and opposing views, discrediting experts, or shifting attention away from subjects that matter. Such practices help develop an environment in which misleading narratives become a normality and can circulate without much resistance.

Harassment, one of the most visible tactics in this category, involves coordinated attacks on experts, or individuals and organizations that contest disinformation narratives. The effect is not focused only on the direct target, but also signals to others that contesting the dominant narrative can generate social punishment, reputational damage, or psychological stress. A complementary tactic is silencing through intimidation, which, on the same logic, discourages others from publicly correcting

misleading claims, even when they possess relevant knowledge. The impact is that manipulated narratives become more accepted, popular, and less contested, whilst credible voices become less visible. Report brigading complements these practices, at the account level, allowing actors to reduce the visibility of adversarial accounts, or even suspend users who oppose their narratives (Wardle 2024, 12-17).

What these tactics do is weaken the counter-discourse. Intimidation discourages experts and ordinary people from intervening, while repeated attacks can diminish trust in those who provide correct information. For the disinformation process, these tactics make it more resilient, not necessarily because of their persuasive character, but because resisting it makes it more costly for the users.

3.6. Artificial Intelligence-enabled tactics

A distinct category of tactics regarding disinformation is the use of Artificial Intelligence (AI) and advanced automation, as an extension of traditional ways to influence the population. The development of technology helps AI to support the phenomenon of disinformation with increasing content production speed, its volume, realism, and personalization capacity of digital messages. Recent literature shows that generative AI does not necessarily change the objectives of disinformation, but contributes to costs, pace, and scalability (Romanishyn, Malytska and Goncharuk 2025, 3-5; Park and Nan 2024, 1502-1504).

One of the most important tactics based on AI is the generation of synthetic content and personas. This includes texts, images, videos, audios, or apparent authentic online identities created or modified by AI. Actors can generate large volumes of content and create credible figures to disseminate that specific material. This can help support or denigrate any agendas or contexts in favor of different actors. Complementarily, AI-assisted microtargeting can help actors to adapt narratives, tone, emotional framing, or claims to specific audience segments to make disinformation more persuasive by aligning messages with users' identities, fears, or ideological orientations.

These categories present different tactics that might be considered innovative and effective, but they cannot work in isolation. For a disinformation campaign to reach its objectives, these tactics must be combined in such a way that their impact derives from coordination, repetition, and adaptation to platform-specific dynamics. Therefore, the significance of these tactics lies in their capacity to be combined, scaled, and sustained over time, generating results that go beyond their individual effects. Also, the identified mechanisms above do not rely solely on absolute falsehood, but rather work through distortion, recontextualization, and manipulation, indicating the necessity of focusing on multiple dimensions (framing, repetition, algorithms), not just on the true-false value. Understanding these mechanisms is essential to both analyzing how disinformation operates at the micro level and explaining how they contribute to broader specific objectives, as well as strategies that derive from them.

4. Disinformation strategies in social media ecosystems

By shifting from the micro level to the bigger picture, we can use, guide, and coordinate these tactical interventions to create disinformation strategies, to influence perceptions, disrupt social cohesion, and alter political and institutional dynamics ([Chadwick and Stanyer 2022](#), 10-14). With these types of objectives in mind, we can refer to strategies as goals that cannot be isolated, but rather as sustained patterns of action, obtained from the coordinated involvement of tactics across time, platforms, or audiences. We are now going to discuss the main categories of strategies that are currently used to support disinformation in social media. Just like in the case of tactics, it is not an exhaustive list of strategies, but it comprises the ones that are used the most and have a great impact on society nowadays.

4.1. Delegitimization of institutions and authorities

This category focuses on eroding trust in governmental institutions, media organizations, scientific experts, or the democratic process; therefore, being a great threat to a few foundation pillars of society. Trust is nowadays replaced with falsehood alternatives, repetitive messages, and large volumes of information, which generate skepticism and questionable thoughts in identifying credible content. Research shows that persistent exposure to disinformation, by using the tactics above, significantly reduces institutional trust and undermines trust in democratic processes (2016 US presidential elections), public health communications (COVID-19), and governance overall ([Surjatmodjo, et al. 2024](#), 1-12).

The causal mechanisms of delegitimization operate through repetition, emotional framing, and diminishing credibility in epistemic authorities. Narratives that present governments as incompetent, corrupt, or not acting in the interest of citizens weaken people's willingness to accept official communications, therefore discrediting those institutions ([Lukavska, et al. 2025](#), 1-11), while attacks on traditional media frame journalism as biased, manipulated, or controlled. On the same page, there are the attacks on scientific expertise that question professional knowledge in areas such as public health or security, replacing fact-checked content with pseudo-science ([Lindberg and Denniss 2025](#), 1-7). Electoral legitimacy can also be the target of promoting and supporting the idea that elections are fraudulent or unfair, or structurally controlled, diminishing confidence in democratic procedures.

As a result, this category of strategies involves suspicion, cynicism, and distrust towards sources that should be guidance and support for social wellbeing. If citizens no longer trust legitimate institutions, expert figures, or electoral procedures, disagreement becomes harder to resolve through institutional channels. The impact of these strategies is not reflected only in the low credibility in institutions, but also in a broader destabilization of the relationship among citizens, knowledge, and authority.

4.2. Polarization and social fragmentation

Considered as central objectives in current disinformation campaigns, the strategies from this category exploit social, political, or cultural divisions and amplify them

through emotional narratives that trigger individual or collective identities. By focusing on the “us versus them” strategy, disinformation increases the erosion of shared reality and reduces the idea of compromise or reaching a consensus. Empirical studies have shown that misinformation related to politics amplifies polarization and fosters ideological approaches (Tucker, et al. 2018, 30-49). What this strategy does is that it affects social cohesion and diminishes people’s capacity to react collectively to threats, either internal or external.

Existing social tensions are used by actors to amplify identity conflicts through emotional activation combined with hardening political, ethnic, linguistic, religious, gendered, or other cultural boundaries. The related narratives encourage communities to interpret facts through increasingly antagonistic frames, which, over time, can contribute to radicalization, as users are pushed toward more extreme positions. A plus to this strategy can come from the creation and reinforcement of echo chambers, limiting exposure to alternative perspectives and keeping users within like-minded communities.

When groups of people do not share a standard reference point anymore, social cohesion and collective response capacity start to become more fragile. Public debates become more hostile and move away from solving social problems, therefore diminishing society’s ability to react to internal or external threats. Polarization functions both as a political and social effect of disinformation and also as a security strategy, by dividing public opinion, reducing trust between groups, and lowering the capacity to respond to daily challenges.

4.3. Confusion

These strategies shift the focus of disinformation from persuasion towards disruption. Actors do not promote one single coherent narrative that supports a specific agenda, but they disseminate contradictory, ambiguous, or overwhelming information to generate uncertainty and cognitive overload. The firehose of falsehood model clearly illustrates the way how volume, repetition, rapidity, and inconsistency contribute to destabilizing information environments (Paul and Matthews 2016, 2-9). This type of action helps in diminishing the possibility of acquiring strong beliefs and discourages engagement with public discourse, as people are uncertain of what is true and what is not.

The central mechanism of this category is deterrence by confusion, involving enough contradiction and ambiguity spread over the internet, so it makes users disengage from the main issues and institutions struggle with coordination (Hedling and Ördén 2025, 969-974), presenting a mechanism that works on multiple layers. Closely related to this is information flooding, an effect of the firehose of falsehood model, where the information space is saturated with such a high volume of information that users become confused and struggle to distinguish valid information from noise. In this case, the strategic effect, both socially and psychologically, is not persuasion, but paralysis.

4.4. Attention control

These strategies shape what the public notices, discusses, and prioritizes. Instead of confusion, flooding the information environment with competitive narratives,

sensational content, or irrelevant controversies will result in users' attention being redirected from the main issues or inconvenient facts (Loru, et al. 2025, 1-10). Currently, when engagement is more important than relevance, these strategies take advantage of timing and visibility to shift attention as unnoticed as possible.

The functional process of this category often begins with agenda diversion, where actors use alternative topics to redirect attention away from policy issues, failures, and damaging events. Later, this is combined with the sensational element, where content becomes emotionally charged to generate engagement and algorithmic visibility. Also, if content is released at key moments, such as elections or crises, the effect is maximized, as people are continuously searching for explanations and quick reactions. The objective does not always refer to convincing audiences of a specific narrative, but to controlling what becomes visible, what can be treated as urgent, and what disappears from collective attention. Therefore, the effect lies in society's reaction to shift its attention to new, outrageous, and fearful content, making it more fragmented and unstable.

4.5. Normalization

Repeated exposure to misleading content, or out-of-order manipulative content, can gradually shift perceptions of what is acceptable, credible, or plausible. In time, narratives that would normally be excluded can become normal through enough repetition, familiarity, or social context reinforcement. The *illusory truth effect* best portrays this process, as repeated statements are more likely to be perceived as true, regardless of their factual value (Pennycook, Cannon and Rand 2018, 2-7). These strategies are important as they reduce resistance to manipulation and enable disinformation to be accepted as normal in everyday actions.

When actors use narratives in a repeated way, users become more familiar with the information. This strategy supports the normalization of distrust, where suspicion towards institutions and experts seems like common sense. For a better effect, this strategy can work together with confusion strategies. Once audiences become more familiar with a subject, more radical or ideological claims can be introduced gradually, being received as less disruptive than the first ones. What these mechanisms bring to the table is that they reduce resistance to surprising information, shifting the limits of acceptable discourse.

4.6. Crisis exploitation and opportunistic manipulation

A further important strategy involves the exploitation of crises and moments of uncertainty. Nowadays, elections, pandemics, or geopolitical conflicts are the events that get the most attention. During such periods, the demand for reliable information increases abruptly, while verification mechanisms are slow or not trained enough to keep up. Disinformation actors take advantage of these vulnerabilities by introducing misleading narratives that can influence ways of thinking and decision-making processes, affecting on a bigger scale the trust in institutions or the response to a crisis. As Vosoughi et al. have shown, misinformation spreads up to six times faster during crises and can significantly affect public behavior negatively towards

health measures or trust in official communication more than fact-checked content (Vosoughi, Roy and Aral 2018, 1146-1153).

Introducing misleading narratives to harden or redirect attention from political debates, contradict or question official information during emergencies (COVID-19), or spreading false interpretations of an event before reliable official information stabilizes, are just a few strategies that work by combining uncertainty with fear and urgency. The main effect is that disinformation can influence perception and behavior at precise moments when trust, coordination, and institutional communication are most needed.

4.7. Erosion of democratic resilience

The main strategy that encompasses all those mentioned above is represented by the erosion of democratic resilience and national security. This is a cumulative strategic objective of many disinformation campaigns that can weaken trust, polarize societies, or disrupt the collective decision-making process. Whether a threat is internal or external, there is no need for a massive disruption of society, because even partial disruption of trust and coordination can have significant strategic consequences in time by applying the tactics and strategies above (Chadwick and Stanyer 2022, 1-17).

5. Discussions

While tactics and strategies can be analyzed separately, their relationship within the disinformation process is fundamentally interconnected and non-linear. There is no strict formula linking isolated tactical interventions to strategic outcomes; instead, disinformation operates through repeated, coordinated, and adaptive interactions among multiple tactics, which together advance macro-level objectives over time. Critically, this relationship is many-to-many: the same tactic may support multiple strategies simultaneously, and the same strategy may be operationalized through different tactical configurations depending on social context, platform dynamics, and actors' interests. For example, delegitimization depends on the interaction of narrative framing, source deception, amplification, and suppression of corrective voices, while polarization emerges from combinations of emotional activation, coordinated inauthentic behavior, and information saturation. Table 1 maps these interdependencies in detail.

The framework presented in Table 1 can be illustrated through the case of Russian disinformation operations targeting Ukraine and Western European audiences, particularly in the period following the full-scale invasion of February 2022. This case has been extensively documented and provides a concrete example of how tactical mechanisms escalate into strategic security effects. At the tactical level, Russian state-affiliated actors deployed a combination of fabricated content (including doctored images attributed to Ukrainian forces), false flag narratives (presenting Ukrainian defensive actions as aggression), coordinated inauthentic behavior through networks of amplifier accounts across Telegram and Twitter/X, and firehose of falsehood techniques involving simultaneous dissemination of contradictory narratives –

TABLE 1. Strategies and tactics configuration in the social media disinformation ecosystem

Strategy	Tactics core configuration	Supporting tactics	Interdependency logic
Delegitimization of institutions	fabricated content + framing manipulation + conspiracy narratives + content identity and source tactics (fake experts, impersonating, astroturfing)	Coordinated amplification; influencer laundering; harassment of journalists, experts, or officials; algorithmic amplification	Institutions are weakened when negative narratives are repeatedly amplified, appear to originate from credible, authentic sources, and are reinforced by attacks on legitimate voices.
Polarization	Framing manipulation and identity-based narratives + coordinated inauthentic behavior + bots/trolls	Microtargeting; engagement-driven amplification; hashtag manipulation; synthetic personas	Polarization appears when emotionally charged identity narratives are amplified through coordinated networks and reinforced within specific online communities, increasing resentment.
Confusion	Firehose of falsehood + contradictory narratives + misleading or fabricated content	bots; algorithmic exploitation; deepfakes; agenda diversion	Confusion is generated by overwhelming audiences with high volume, repetitive, or contradictory information, making it difficult to distinguish between credible and false content.
Attention control	Platform infrastructure exploitation tactics (algorithmic exploitation) + hashtag manipulation + coordination and amplification tactics	Influencer laundering; coordinating posting; agenda diversion; selective omission	Public attention is redirected when actors manage to exploit platform visibility and algorithms to artificially increase interest in selected narratives while real issues and topics are overshadowed.
Normalization	Amplification tactics, especially repetition + framing manipulation + pseudo-journalistic sources	Influencer laundering; synthetic personas; bots; troll networks; algorithmic recommendation systems	Repeated exposure to specific narratives gradually increases familiarity with the content, making it more acceptable and setting it as the new normal, which helps introduce distrust and misleading frames into everyday discourse.
Crisis exploitation	Fabricated or misleading content related to crisis + emotional framing + fast coordinated amplification	Deepfakes; microtargeting; hashtag manipulation; automated synthetic content	During crises, uncertainty and urgency lower verification processes, allowing narratives to spread rapidly and influence public perceptions, emotions, and behaviors, before official, reliable information is released.
Erosion of democratic resilience	most of the tactics regarding delegitimization, polarization, confusion, or amplification tactics	Suppression and discourse disruption tactics; AI-enabled content; manipulative narrative saturation	Democratic resilience is gradually diminished when multiple strategies and tactics are combined, reducing institutional legitimacy, contributing to polarization, and collective response to crises and internal or external threats.

Source: The author.

denying atrocities, attributing them to other parties, and claiming they were staged (Dov Bachmann, Putter and Duczynski 2023, 1-10). Deepfake content, including a fabricated video of Ukrainian President Zelensky reportedly calling for surrender, demonstrated the deployment of AI-enabled tactics (Farid 2025, 1-9). At the strategic level, these combined operations pursued the delegitimization of Ukrainian governmental and military institutions, the polarization of Western publics around support for Ukraine, the confusion created through information overload that made fact-checking difficult to sustain at scale, and the erosion of trust in NATO and EU institutional communications (EEAS 2025b, 7-11). The interdependency logic visible in this case aligns directly with the many-to-many structure proposed in Table 1: the same coordinated inauthentic behavior networks simultaneously served delegitimization, confusion, and polarization objectives, while the polarization strategy itself drew on framing manipulation, emotional content, and amplification tactics applied across different audience segments in different languages. This case thus validates the analytical utility of the framework proposed in this article, while also confirming that real-world disinformation campaigns are far more fluid and adaptive than any static taxonomy can fully capture.

The Ukraine case discussed above illustrates this logic empirically, showing how the same networks of amplifier accounts simultaneously served delegitimization, confusion, and polarization objectives. This convergence confirms that analytical frameworks focusing on individual tactics or single causal chains will systematically underestimate the scope and adaptability of coordinated disinformation. The key analytical insight is that strategic effects emerge from the sustained, overlapping deployment of multiple tactics – not from any single mechanism acting in isolation.

To strengthen the empirical foundation of the proposed model above, the Ukrainian case can be divided into more specific micro-cases, allowing the seven stages to be illustrated in a clearer manner. Therefore, we chose three well-documented cases, such as President Zelensky's surrender deepfake, Bucha massacre disinformation, and Operation Overload (Matryoshka), compared below in Table 2. The first case refers to March 2022, after the start of the Russian invasion, when a deepfake video circulated on multiple platforms, portraying Volodymyr Zelensky asking the Ukrainians to surrender and go back to their families (Allyn 2022, Bohacek and Farid 2022, 1-3). The Bucha case was based on confusion, denial of identity, and contradictions. After evidence emerged regarding the killing of civilians in Bucha, pro-Kremlin sources negated Russian implications and promoted ideas of fabricated, staged, or falsely attributed content to the aggressor. The "Denying Bucha" study (Fredheim, Ahonen and Pamment 2023, 4-22) showed that these sources posted contradictory and framed information to undermine Western analyses and statements regarding the massacre. The third case, different from the first two, focused more on the amplification loop phase, aiming for journalists, researchers, and fact-checking organizations. It was considered a propaganda effort from the Kremlin meant to undermine the war efforts of Ukraine and destabilize Western democracies (Atanasova, Poldi and Kuster 2025, 8-9).

TABEL nr. 2. Comparative application of the proposed model to three Russian disinformation cases

Phase of the model	Zelensky's surrender deepfake	Bucha massacre disinformation	Operation Overload/ Matryoshka
Platform opportunities	Wartime uncertainty and confusion, public need for coordinated information, speed and visibility offered by platforms, and favorable conditions for fabricated leadership content to gain attention	The impact produced by reports and images from Bucha created an environment where audiences needed visual evidence, continuous updates, and official answers	Platform speed, cross-platform circulation, visibility of journalists, experts, and fact-checkers, and low cost of AI content creation
Disinformation tactics	AI-enabled synthetic videos, Impersonating President Volodymyr Zelensky, Crisis-time exploitation	Denial narratives, false-flag framing, contradictory explanations, firehose messages from different media sources	Fabricated content (images, videos), AI-generated content, impersonation of public figures, fake news formats, coordinated dissemination
Cognitive effects	Uncertainty, panic, and doubt regarding leadership and message credibility	Confusion about attribution and responsibility, doubt regarding visual evidence, and uncertainty about credibility in media sources	Doubt about authenticity, fact-check fatigue, confusion about sources, authorities, and the overload of authorities in fact-checking large volumes of content
Behavioral responses	Rapid cross-platform sharing, Debunking/ fact-checking, public discussion	Online debates, engagement with contradictory claims, public arguments over attribution and responsibility	Public figures, journalists, and fact-checkers were forced to debunk, verify, and react to the overflow of manipulated content
Amplification loops	The video became viral due to platform sharing, media coverage, analysis activity, and public discussion about deepfakes during wartime	Repetition by pro-Kremlin channels, same agenda for all media channels, social media accounts, and global analysis of the event	Content was covered multiple times for debunking and gaining more visibility
Strategies	Crisis exploitation, delegitimization of Ukrainian leadership, and attempted disruption of morale and command credibility	Deterrence by confusion, Delegitimization of Ukrainian and Western institutions, and agenda diversion	Attention control, agenda manipulation, and normalization of anti-Ukraine and pro-Kremlin narratives
National security implications	Potential weakening of trust in leadership, morale, and credibility in public institutions	Public outrage, accountability, and doubt of Western support for Ukraine	Weakening of media and fact-checking entities, increased public uncertainty, and erosion of trust in legitimate institutions

Source: The author.

This table does not validate the model statistically, but rather shows that each stage can be applied to different cases. We chose the three instances related to the Russian invasion in Ukraine because they illustrate different forms of escalation: from a rapid episode of AI manipulation in a crisis context, to a campaign of denial and contradictions regarding an atrocity, and a recent information overload operation exploiting the fact-checking ecosystem. As stated above, we can observe that the process is not a perfect recipe, such as a linear process, but rather adaptive, depending on the context, platform, and audience.

All these tactics and strategies above highlight the fact that disinformation operates through interconnected and mutually reinforcing processes. Tactics are the operational tools through which manipulation occurs at the micro level, whilst strategies represent the broader objectives that these mechanisms aim to achieve over time. They are dependent on each other, but they are not related in a linear or one-dimensional way. Regarding the situations encountered, we can see that there are tactics that can be used to multiple strategic objectives, whilst a single strategy can be implemented through the coordinated deployment of multiple tactics across various platforms, for different audiences, and in different time contexts.

The tactics and strategies analyzed above represent the most operationally significant mechanisms documented in the current literature on digital disinformation. Several cross-cutting insights emerge from the analysis:

- An important aspect is that disinformation on social media should be understood as a multi-level escalation process, and not as a simple flow of false or misleading content. Disinformation grows through a sequence of interconnected levels, from possibilities offered by platforms that enable tactic manipulation, to cognitive and behavioral responses, then amplification through algorithms, and finally, if sustained over time, to applying strategies at the societal level. This shows the shift from content-centered approaches to a process in which manipulation at the micro level can obtain macro-level strategies.
- A second aspect refers to social media functioning as a connective infrastructure between tactics and strategies. Platforms offer different features, such as visibility, rapidity, algorithm recommendation, or low-cost dissemination, which do not necessarily facilitate the dissemination of information, but they shape the conditions under which tactical mechanisms can be scaled and sustained.
- A third important characteristic is that the relationship between tactics and strategies is not straightforward as one link, but rather as many-to-many. One single tactic can be part of multiple strategies, while a strategy can depend on multiple tactics. As an example, CIB might have an important contribution to delegitimization, polarization, normalization, or agenda manipulation, whereas, for example, polarization might require fake experts, fabricated

content, amplification, or framing manipulation. Therefore, disinformation campaigns can be constructed through an overlapping and adaptive relationship between tactics and strategies.

- Also, for specific strategies, there are multiple tactical configurations, depending on the context, objectives, or societal vulnerabilities. There is no straight way of constructing a strategy from a specific tactic. This suggests that the analytical focus should be placed on linking specific tactics in order to obtain the most efficient result, instead of focusing on only one tactic.
- By focusing on the last category of strategies mentioned, regarding the erosion of democratic resilience, we could indicate that disinformation on social media is cumulative rather than immediate. Disinformation rarely undermines trust, cohesion, or institutional legitimacy through a single video, audio, or text, or in a manner of short time. Instead, its effects appear through repetition, coordination, amplification, and persistence. In time, repeated narratives can normalize distrust, intensify polarization, or increase confusion. Following this logic makes it easier to understand disinformation as a process, rather than a collection of messages.
- The last important aspect is represented by the role of social media in undermining social security. Social media acts indirectly towards achieving goals, being an enabler of conditions through which disinformation tactics can become strategic processes. Cognitive and behavioral loops, amplification through algorithms, consistency, or repetition are a few features of social media platforms that work behind the scenes to help actors reach their goals.

Together, these observations confirm that social media functions not merely as a communication environment but as a strategic infrastructure – one that enables disinformation tactics to be coordinated, amplified, and sustained until they produce macro-level security effects.

The original contribution of this article lies in the integrative framework that shows the evolution of disinformation campaigns from platform capabilities to national security implications, going through the intermediate phases mentioned earlier. While existing frameworks approach the steps of the disinformation process, they rarely clarify how platform tactical mechanisms evolve into larger strategic objectives. The proposed model addresses this issue by illustrating how social media platforms enable micro-level manipulation to be enhanced and sustained to the point that it supports strategies such as delegitimization, polarization, deterrence by confusion, agenda manipulation, normalization, and crisis exploitation. Its primary value lies in offering a structured instrument for examining the evolution of disinformation from isolated tactical actions into persistent strategic influence with potential security relevance.

Conclusion

This article has examined the role of social media in undermining national security by mapping the relationship between disinformation tactics and strategies. Rather

than treating social media as a passive channel through which false content circulates, the analysis has demonstrated that disinformation operates as a multi-level escalation process: platform affordances enable tactical manipulation, tactical mechanisms generate cognitive and behavioral responses, and sustained coordinated deployment transforms these responses into strategic security effects. Social media is thus a strategic infrastructure that enables society-level manipulation with measurable political and security consequences.

The article distinguished two analytical levels: disinformation tactics (micro-level mechanisms including content fabrication, framing manipulation, source deception, coordinated amplification, and AI-enabled production) and disinformation strategies (macro-level objectives including delegitimization of institutions, polarization, confusion, normalization, crisis exploitation, and erosion of democratic resilience). As the framework and the Ukraine case study confirm, these levels are connected through adaptive, overlapping, many-to-many relationships rather than linear causal chains. One tactic may serve multiple strategies; one strategy may draw on multiple tactical configurations depending on context and target vulnerabilities. The security implications of disinformation are therefore cumulative: strategic effects – weakened institutional trust, intensified polarization, eroded democratic resilience – accumulate through the sustained, coordinated application of tactical mechanisms over time, affecting the information, cognitive, and institutional foundations on which democratic societies depend.

These results also suggest a few several practical implications. First, counter-disinformation policies should switch their focus from the correction of individual false claims and address the broader process through which this information distortion is amplified, repeated, and made socially credible. To achieve this, there is a need for closer cooperation between legitimate institutions, platform companies, researchers, fact-checkers, and social organizations, especially during important events, which necessitates more resources to prevent and debunk disinformation. Second, media literacy and digital literacy programs should extend their focus from identifying false content to understanding trends, manipulation techniques, source deception, or coordinated amplification for a better understanding of where users should be more alert. Third, by analyzing the proposed model, democratic resilience should be improved by finding the elements of the model where it necessitates more attention and development, so the link to national security implications is broken.

References

- Alkathiri, Nasser, and Khaled Slhoub.** 2025. "Challenges in machine learning-based social bot detection: a systematic review." *Discover Artificial Intelligence* 5 (214): 1-40. <https://doi.org/10.1007/s44163-025-00448-w>.
- Allyn, Bobby.** 2022. *Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn.* 03 16. <https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia>.

- Atanasova, Aleksandra, Francesco Poldi, and Guillaume Kuster.** 2025. "Operation Overload, More Platforms, New Technology, Powered by AI." Analysis report.
- Baines, Paul, Nicholas O'Shaughnessy, and Nancy Snow.** 2019. *The SAGE Handbook of Propaganda*. SAGE Publication Ltd.
- Benkler, Yochai, Robert Faris, and Hal Roberts.** 2018. *Network Propaganda - Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.
- Bernal, Alonso, Cameron Carter, Ishpreet Singh, Kathy Cao, and Olivia Madreperla.** 2020. *Cognitive warfare an attack on truth and thought*. Johns Hopkins University.
- Bohacek, Matyas, and Hany Farid.** 2022. "Protecting world leaders against deep fakes using facial, gestural, and vocal mannerisms." *Proceedings of the National Academy of Sciences of the United States of America* (National Academy of Sciences) 119 (48): 1-3. <https://doi.org/10.1073/pnas.2216035119>.
- Bradshaw, Samantha, and Philip N. Howard.** 2018. "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." *Computational Propaganda Research Project*. Oxford Internet Institute, University of Oxford. 11-15.
- _____. 2018. "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." *Computational Propaganda Research Project*. Oxford Internet Institute, University of Oxford. 11-15.
- Castells, Manuel.** 2009. *Communication Power*. New York: Oxford University Press.
- Chadwick, Andrew.** 2017. *The Hybrid Media System: Politics and Power*. 2nd Edition. New York: Oxford University Press.
- Chadwick, Andrew, and James Stanyer.** 2022. "Deception as a Bridging Concept in the Study of Disinformation, Misinformation, and Misperceptions: Towards a Holistic Framework." *Communication Theory* 32 (1): 1-24. <https://doi.org/10.1093/ct/qtab019>.
- Clemons, Eric K., Andrej Savin, Maximilian Schreieck, Stina Teilmann-Lock, Jan Trzaskowski and Ravi Waran.** 2024. "A face of one's own: The role of an online personae in a digital age and the right to control one's own online personae in the presence of digital hacking." *Electronic Markets* 34 (1): Article 31. <https://doi.org/10.1007/s12525-024-00713-3>.
- de Goeij, Maria W.R.** 2023. "Reflexive control: Influencing Strategic Behavior." *Parameters: The US Army War College Quarterly* 53 (4): 97-108. <https://doi.org/10.55540/0031-1723.3262>.
- Dov Bachmann, Sascha-Dominik, Dries Putter, and Guy Duczynski.** 2023. "Hybrid warfare and disinformation: A Ukraine warperspective." *Policy Insights* 858-869. <https://doi.org/10.1111/1758-5899.13257>.
- Dragomir, Marius, Jose Ruas-Araujo, and Minna Horowitz.** 2024. "Beyond online disinformation: assessing national information resilience in four European countries." *Humanities and Social Sciences Communications* 11: 101. <https://doi.org/10.1057/s41599-024-02605-5>.
- EEAS.** 2025a. *2024 Report on EEAS Activities to Counter Foreign Information Manipulation and Inference (FIMI)*. FIMI, Brussels: European External Action Service, 4-8. <https://www.eeas.europa.eu/sites/default/files/2025/documents/2024%20Report%20on%20EEAS%20Activities%20to%20Counter%20FIMI.pdf>.
- _____. 2025b. "EEAS Report on Foreign Information Manipulation and Interference Threats." Report on FIMI Threats, 7-11.

- Egelhofer, Jana Laura and Sophie Lecheler.** 2019. "Fake news as a two-dimensional phenomenon: a framework and research agenda." *Annals of the International Communication Association* 43 (2): 97-116. <https://doi.org/10.1080/23808985.2019.1602782>.
- Farid, Hany.** 2025. "Mitigating the harms of manipulated media: Confronting deepfakes and digital deception." *PNAS Nexus* 4 (7): pgaf194. <https://doi.org/10.1093/pnasnexus/pgaf194>.
- Ferreira, Ricardo Ribeiro.** 2022. "Liquid Disinformation Tactics: Overcoming Social Media Countermeasures through Misleading Content." *Journalism Practice* 16 (8): 1537-1558. <https://doi.org/10.1080/17512786.2021.1914707>.
- Fredheim, Rolf, Anneli Ahonen, and James Pamment.** 2023. *Denying Bucha - The Kremlin's Influence tactics in the aftermath of the 2022 Bucha atrocity*. Research report, Lund University.
- Hameleers, Michael.** 2023. "Disinformation as a context-bound phenomenon: toward a conceptual clarification integrating actors, intentions and techniques of creation and dissemination." *Communication Theory* 33 (2): 1-10. <https://doi.org/10.1093/ct/qtad004>.
- Hedling, Elsa, and Hedvig Ördén.** 2025. "Disinformation, Deterrence and the Politics of Attribution." *International Affairs* 101 (3): 967-986. <https://doi.org/10.1093/ia/iiaf012>.
- Kruijver, Kimberley, Neill Bo Finlayson, Beatrice Cadet, and Sico van der Meer.** 2025. "The disinformation lifecycle: an integrated understanding of its creation, spread and effects." *Discover Global Society* 3 (1): 1-26. <https://doi.org/10.1007/s44282-025-00194-5>.
- Lewandowsky, Stephan, Ullrich K.H. Ecker, and John Cook.** 2017. "Beyond Misinformation: Understanding and Coping with the 'Post-Truth' Era." *Journal of Applied Research in Memory and Cognition* 6 (4): 353-369. <https://doi.org/10.1016/j.jarmac.2017.07.008>.
- Lindberg, Rebecca, and Emily Denniss.** 2025. "Social media and the spread of misinformation: infectious and a threat to public health." *Health Promotion International* 40 (2): daaf023. <https://doi.org/10.1093/heapro/daaf023>.
- Loru, Edoardo, Alessandro Galeazzi, Anita Bonetti, Emanuele Sangiorgio, Niccolò Di Marco, Matteo Cinelli, Max Falkenberg, Andrea Baronchelli, and Walter Quattrociocchi.** 2025. "Ideology and polarization set the agenda on social media." *Scientific Reports* 15 (35816): 1-13. <https://doi.org/10.1038/s41598-025-19776-z>.
- Lukavska, K., R. Gabrhelík, M. Miovský, N. Hynek, B. Gavurova, L. Stastna, M. Bartak, B. Petruzelka, and V. Moravec.** 2025. "Exploring Disinformation: The interplay of exposure, trust, and sharing." *Computers in Human Behavior Reports* 18: 100686. <https://doi.org/10.1016/j.chbr.2025.100686>.
- Mazarr, Michael, Abigail Casey, Alyssa Demus, Scott Harold, Luke Mathews, Nathan Beaucham-Mustafaga, and James Sladden.** 2019. *Hostile Social Manipulation*. Santa Monica: RAND Corporation. https://www.rand.org/pubs/research_reports/RR2713.html.
- Metzler, Hannah, and David Garcia.** 2024. "Social Drivers and Algorithmic Mechanisms on Digital Media." *Perspectives on psychological science: a journal of the Association for Psychological Science* 19 (5): 735-748. <https://doi.org/10.1177/17456916231185057>.
- Murero, Monica.** 2023. "Coordinated inauthentic behavior: An innovative manipulation tactic to amplify COVID-19 anti-vaccine communication outreach via social media." *Frontiers in Sociology* 8: 1141416. <https://doi.org/10.3389/fsoc.2023.1141416>.

- Mustafa, Hassan, Markus Luczak-Roesch, and David Johnstone.** 2025. "Conceptualizing the Evolving Nature of Computational Propaganda: A Systematic Literature Review." *Annals of the International Communication Association* 49 (1): 45-60. <https://doi.org/10.1093/anncom/wlaf001>.
- NATO.** 2022. *Strategic Concept*. Brussels: NATO. <https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf>.
- Park, Seyeon, and Xiaoli Nan.** 2024. "Generative AI and misinformation: a scoping review of the role of generative AI in the generation, detection, mitigation, and impact of misinformation." *AI & Society* 41 (2): 1501-1515. <https://doi.org/10.1007/s00146-025-02620-3>.
- Paul, Christopher, and Miriam Matthews.** 2016. "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It." *RAND Corporation*. July 11. <https://doi.org/10.7249/PE198>.
- Pennycook, Gordon, Tyrone Cannon, and David Rand.** 2018. "Implausibility and illusory truth: Prior exposure increases perceived accuracy of fake news but has no effect on entirely implausible statements." *Journal of Experimental Psychology General* 147 (12): 2-7. <https://doi.org/10.1037/xge0000465>.
- Pomerantsev, Peter.** 2019. *This is Not Propaganda*. London: Faber & Faber.
- Romanishyn, Alexander, Olena Malyska, and Vitaliy Goncharuk.** 2025. "AI-driven disinformation: policy recommendations for democratic resilience." *Frontiers in Artificial Intelligence* 8: 1569115. <https://doi.org/10.3389/frai.2025.1569115>.
- Surjatmodjo, Dwi, Andi Alimuddin Unde, Hafied Cangara, and Febri Alem Sonni.** 2024. "Information Pandemic: A Critical Review of Disinformation Spread on Social Media and Its Implications for State Resilience." *Social Sciences* 13 (8): 418. <https://doi.org/10.3390/socsci13080418>.
- Tucker, Joshua, Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan.** 2018. "Online Content and Political Polarization." *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*. William and Flora Hewlett Foundation. 30-49.
- Uusikylä, Petri, Harri Jalonen, Valdemar Kallunki, Anssi Keinänen, and Silvia Sommarberg.** 2024. "Introduction to Information Resilience in the Context of National Preparedness." In *Information Resilience and Comprehensive Security*, by Petri Uusikylä, H Jalonen, and A Jokipii, 1-18. Palgrave Macmillan, Cham.
- Vosoughi, Soroush, Deb Roy, and Sinan Aral.** 2018. "The Spread of True and False News Online." *Science* 359: 1146-1151. <https://doi.org/10.1126/science.aap9559>.
- Wardle, Claire.** 2024. *A Conceptual Analysis of the Overlaps and Differences between Hate Speech, Misinformation, and Disinformation*. New York: United Nations.
- Wardle, Claire, and Hossein Derakhshan.** 2017. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Strasbourg: Council of Europe, 20-21.
- Wu, Manli, Tailai Wu, and Yushan Xiao.** 2025. "Why people share misinformation on social media? An integration of affordance and flow theories." *Humanities and Social Sciences Communications* 12: 1129. <https://doi.org/10.1057/s41599-025-05511-6>.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

<https://buletinul.unap.ro/index.php/en/>

The Information Asymmetry of Military Decision-Making. ISR and the Challenge of Situational Understanding

Captain Alexandru PÎNTEA, Master's Student*

*"Carol I" National Defence University, Bucharest, Romania
e-mail: pintea@unap.ro

 <https://orcid.org/0009-0009-9165-7027>

Abstract

The commander's decision-making depends structurally on the quality of the information received, yet the explosion of data volumes generated by contemporary sensors has transformed this dependence into a reverse problem, that of abundance. This article argues that the classical architecture of the Intelligence, Surveillance and Reconnaissance (ISR) system is built predominantly to support the perception and comprehension of environmental elements, leaving the capacity for cognitive projection that quality decision-making requires insufficiently covered. Drawing on the cognitive decision-making models proposed by Klein, Boyd, and Endsley and on the distinction between situational awareness and situational understanding articulated by Yufik and Malhotra, the paper identifies a structural asymmetry between collection capabilities and projection capabilities, assessing within this framework the integration of artificial intelligence into the ISR decision chain. The article concludes that decisional superiority is achieved through the redesign of the architecture that functionally connects ISR to the cognitive act of decision-making, rather than through the mere accumulation of sensors or of data.

Keywords:

ISR; Decision-Making; Situational Awareness; Situational Understanding;
Command and Control; Artificial Intelligence; Decision Superiority.

Article info

Received: 10 April 2026; Revised: 30 April 2026; Accepted: 3 June 2026; Available online: 30 June 2026

Citation: Pintea, A. 2026. "The Information Asymmetry of Military Decision-Making. ISR and the Challenge of Situational Understanding."
Bulletin of "Carol I" National Defence University, 15(2): 51-68. <https://doi.org/10.53477/2284-9378-26-18>



© „Carol I” National Defence University Publishing House

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution ([CC BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/))

Introduction

The commander's decision is the central element of military command, being "the bridge to translate the strategic vision into tangible actions". The quality of this act exceeds in the operational context the professional dimension, becoming "a matter of life and death". The history of military operations confirms this centrality: the quality of situation assessment and decisions made by commanders has consistently been associated with the success or failure of campaigns ([D'Alessio, et al. 2024](#), 2-3).

The current operational reality amplifies the stakes of this dependence through speed, structural uncertainty, the multi-domain character of confrontation, and massive volumes of data generated by distributed sensors. The commander faces the challenge of transforming the abundance of data into an actionable decision within increasingly narrow time windows. Allied doctrine explicitly states that "ISR (Intelligence, Surveillance and Reconnaissance) exists to provide the right data to the right user at the right time to support decision-making, creation of effects and conducting operations" ([Development, Concepts and Doctrine Centre 2023a](#), 5). In this understanding, ISR exceeds its traditional role as an auxiliary capability, becoming a fundamental infrastructure of the military decision-making process.

Yufik and Malhotra (2021, 1) raise the conceptual problem of the differences between what the commander needs and what is provided through ISR. Doctrine and the technological investments associated with it are built around the concept of situational awareness, defined as "immediate knowledge of the conditions of the operation". The commander, however, needs situational understanding, defined as "the product of analyzing and judging relevant information to determine relationships among mission variables, facilitating decision-making". The distinction is operational rather than terminological, because sensors provide answers to the questions *what?*, *where?*, and *when?*, while the decision rests on *what does it mean?*, *what comes next?* And *what are the implications?*. More data and more processing power do not automatically produce a better decision if the ISR-decision chain is built to maximize situational awareness rather than understanding.

This article seeks to show that the answer to this problem requires redesigning the architecture that connects ISR to decision-making, rather than expanding collection capabilities. The proliferation of sensors and ever-growing data volumes does not automatically produce a better decision when the structures of processing, analysis, and dissemination remain anchored in the logic of an era in which the dominant problem was information scarcity. The argument supports this position by examining military decision-making models, ISR doctrines, and the tensions generated by the integration of artificial intelligence into the ISR-decision chain.

This article is addressed primarily to the structures involved in the design and use of ISR capabilities, as well as to the decision-makers responsible for guiding

investments in the modernization of these capabilities. The approach seeks to offer them a conceptual framework through which to assess not only the volume or the technical performance of collection systems, but also their actual contribution to the quality of the decision-making act.

Methodologically, the article rests on a conceptual analysis of the specialized, unclassified, and publicly available literature, articulating three distinct bodies of work: the cognitive models of decision-making, ISR doctrine, and recent research on the integration of artificial intelligence. The confrontation of these three perspectives allows the construction of a unified framework for interpreting the relationship between ISR and the decision-making act, a framework that the existing literature treats only in fragmented form.

The research also presents a number of limitations. The approach is theoretical and interpretive rather than empirical, resting on the analysis of sources rather than on original data. The argument relies predominantly on doctrine and literature from the Anglo-Saxon space, a fact explained by the maturity of the debate in that space, but one that leaves open the need for subsequent validation. The conclusions of the article are theoretical in nature and remain open to verification. They could be tested through case studies applied to recent operations, in which the relationship between ISR products and commanders' decisions can be traced concretely. Furthermore, their transposition to the context of the Romanian Armed Forces, with its particularities of structure and resources, constitutes a distinct research direction that the present article does not cover.

1. Anatomy of Military Decision-Making. Patterns, Tempo, and Situational Awareness

Understanding the relationship between ISR and the command act requires a prior examination of military decision-making as a cognitive process. The way in which the commander transforms information into action has been theorized in several stages, each bringing successive adjustments to the assumptions about the role of reason, experience, and time in combat decision-making. Reviewing these models allows the identification of the common element that this article will subsequently exploit, namely, the structural dependence of the decision on the quality of informational input.

The rationalist-analytical tradition treated decision-making as a four-step process: identifying the problem, generating options, evaluating them against predefined criteria, and choosing the optimal option. The model, with roots in neoclassical economics and expected utility theory (von Neumann and Morgenstern 1953), influenced military doctrine through procedures such as MDMP (Military Decision-Making Process). Its applicability in real combat conditions was, however, contested as early as the 1950s by Herbert Simon, who introduced the concept of

bounded rationality. The commander does not have the time, complete information, or cognitive capacity to optimize, instead choosing the first option that exceeds a threshold of acceptability, a process Simon called “satisficing” ([Simon 1955](#)).

Simon’s critique opened the way for naturalistic decision-making research, later developed by Gary Klein. Studying fire chiefs, military pilots, and police officers in real operating conditions, Klein found that experts do not compare options but recognize patterns. The Recognition-Primed Decision (RPD) model proposed by Klein describes a process in which accumulated experience builds a repertoire of situational prototypes, and the encounter with a new situation triggers the identification of the closest prototype and the activation of the associated course of action ([Klein 2017](#), 24). Subsequent studies have confirmed that experienced officers resort to recognition-based strategies in 95% of decisions, of which 87% involve direct matching with a known prototype ([Endsley 1995](#), 34). The military expert’s decision is, from this perspective, an act of recognition, not of comparison.

On the ground opened by naturalistic research, John Boyd formulated the OODA model (Observe, Orient, Decide, Act) in the 1970s, transposing cognitive findings into a competitive framework. The loop describes four recursive phases through which an actor gathers data about the environment, interprets it through the filters of experience and culture, chooses a course of action, and executes it, thereby modifying the environment in which the next loop will operate ([Boyd 2012](#)). Boyd’s conceptual contribution does not lie so much in the description of the phases, but in the observation that two forces in confrontation traverse decision-making loops at different speeds. The force that decides and acts more quickly penetrates the “inside” of the adversary’s loop, forcing it to respond to a reality that has already changed. This advantage, called decision superiority, remains today one of the doctrinal pillars of military thinking. OODA articulates in operational terms what RPD describes cognitively, namely that decision-making, in a military context, is a process governed by tempo, and the commander wins by choosing a sufficiently good option sufficiently quickly, rather than a perfect option obtained through exhaustive analysis. [Bollmann and Heltberg \(2023, 155\)](#) observe that contemporary technologies, particularly artificial intelligence, are used precisely to accelerate the observation and orientation phases of the loop, compressing decision-making time and expanding situational awareness.

Naturalistic models of military decision-making, although different in purpose and level of analysis, converge on a structural observation. The quality of the decision depends directly on the quality of the information input that the commander receives. RPD presupposes a rich repertoire of patterns, but this repertoire is built through direct experience and through intelligence products that extend the commander’s indirect experience. OODA presupposes an observation phase rapid and comprehensive enough to feed orientation. In both cases, the primary source of informational input in a military context is ISR.

RPD and OODA describe the mechanism of decision-making but leave open the question of the cognitive content the commander manipulates when recognizing patterns or traversing the decision-making loop. The most influential answer comes from the works of Mica Endsley, who in 1995 proposed the concept of situational awareness as an internal representation of the operational environment that the decision-maker continuously constructs and updates. The author defines situational awareness as “the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future” (Endsley 1995, 36). The model organizes this representation into three hierarchical levels. Level 1, perception, involves detecting the status, attributes, and dynamics of the relevant elements in the environment, whether enemy forces, system parameters, or terrain features. Level 2, comprehension, goes beyond mere awareness of the elements present and involves “an understanding of the significance of those elements in light of pertinent operator goals”, while Level 3, projection, represents the ability to anticipate the future actions of the elements in the environment and provides “the knowledge (and time) necessary to decide on the most favorable course of action to meet one’s objectives” (Endsley 1995, 36-37).

Endsley’s major conceptual contribution is the firm distinction between situational awareness, decision-making, and performance, treated as three separate constructs with different causal factors. “Even the best-trained decision makers will make the wrong decisions if they have inaccurate or incomplete SA. Conversely, a person who has perfect SA may still make the wrong decision [...] or show poor performance”, the author shows (Endsley 1995, 36), emphasizing that this separation allows for the precise diagnosis of the source of failure in complex operations. Its applicability to the military context is direct, providing an analytical framework for locating decision-making vulnerabilities between the collection of information, its interpretation, and the anticipation of evolutions.

Recent empirical validation of the model in a military context comes from the study by Hærem et al. on multiteam systems engaging targets with limited time windows. The authors compared distributed and co-located configurations, measuring situational awareness at the three Endsley levels and correlating it with operational performance. The central result is telling. “Level 3 SA was the only SA level that significantly predicted all three performance dimensions – process performance, speed, and accuracy – while Level 2 SA correlated only with accuracy and Level 1 SA had no significant relation to performance” (2022, 7). The measured correlations confirm this pattern ($r = 0.58$ for process performance, $r = 0.41$ for speed, $r = 0.68$ for accuracy). In the distributed configuration, scores at Level 3 dropped to approximately 25%, a value equivalent to “random guessing”, while in the co-located configuration, scores remained high, at an average of 72%. The co-located teams performed approximately 50% better and were 1.75 times faster than the distributed ones (Haerem, et al. 2022, 7-8).

From the ISR-decision perspective, the perception of raw data, however comprehensive, is not sufficient for a quality decision. Contextualized comprehension partially reduces the gap, but the true performance difference comes from the projection capacity, namely from the anticipation of the situation's evolution. Endsley shows that this capacity is the product of the mental models that experience builds over time, which "can largely circumvent these limits by providing for the integration and comprehension of information and the projection of future events (the higher levels of SA), even based on incomplete information and under uncertainty" (1995, 49). The expert commander does not decide better because he processes faster, but because his mental models allow him to reach Level 3, where the novice remains stuck at Levels 1 and 2.

This observation sets the agenda of the article. If quality decision-making depends structurally on Level 3 of situational awareness, then the informational infrastructure that feeds this level becomes the central stake. The examination of ISR as such shows that its doctrinal architecture is built predominantly to support Levels 1 and 2, and adapting to the requirements of cognitive projection constitutes the main challenge of operations.

2. ISR as Integrated Infrastructure. Definitions, Processes, and Recent Transformations

The term ISR covers a complex reality that has evolved significantly over the last two decades and that brings together activities, processes, capabilities, and organizations into an integrated system. The examination of this architecture in the present section will successively cover the doctrinal definition, its components, the TCPED (Task, Collect, Process, Exploit, Disseminate) operational process, the collection disciplines, and the recent transformations generated by commercial ISR and by the explosion of open sources.

American doctrine defines ISR as an activity that "synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations" (U.S. Army 2013, I-11). The updated U.S. Air Force doctrine complements this definition by stating that ISR operations "comprise the primary activities that feed data and information into the joint intelligence process" (U.S. Air Force 2025, 1). British doctrine offers the most comprehensive formulation, describing joint ISR as "an integrated intelligence and operations set of capabilities, which synchronises and integrates the planning and operations of all collection capabilities with the processing, exploitation, and dissemination of the resulting information in direct support of the planning, preparation, and execution of operations" (Development, Concepts and Doctrine Centre 2023a, 3).

Three observations emerge from these definitions. The first concerns the integrated character of ISR, which brings together under the same umbrella collection,

processing, and dissemination, eliminating their treatment as separate functions. The second refers to the dual nature, simultaneously of operations and intelligence, with ISR belonging to both domains and being reducible to neither, while the third concerns its explicit orientation toward the direct support of operations, which unequivocally establishes the decision-making finality of the entire architecture. British doctrine synthesizes this finality by identifying three sets of primary ISR missions, namely the direct support of operations, support to the targeting process, and support to the intelligence cycle ([Development, Concepts and Doctrine Centre 2023a, 8](#)).

Although it operates as an integrated system, ISR retains in its doctrine important distinctions among the three components. Intelligence refers to all collection disciplines, the associated capabilities, and the products delivered to commanders. Surveillance refers to “the systematic observation across all operational domains, the information environment, and across the cognitive, physical, and virtual dimensions of places, persons, or objects by various means”, while reconnaissance is regarded as “a mission to obtain, by visual observation or other detection methods, information about adversary activities and resources, or data concerning the meteorological, hydrographical, or geographic characteristics of an area” ([Development, Concepts and Doctrine Centre 2023a, 3-4](#)) ([Development, Concepts and Doctrine Centre 2023b, 176, 179, 180](#)). The functional relationship among the three components is hierarchical. Surveillance and reconnaissance activities produce data and information, which are then transformed into proper intelligence products through the intelligence cycle. ISR is, in this logic, an activity subordinated to intelligence, conducting the collection of the data needed to satisfy intelligence requirements ([U.S. Air Force 2025, 2](#)).

The operational core of ISR is the TCPED process. The five phases represent the model through which ISR capabilities are directed and operated in order to achieve the outcomes desired by the commander ([Development, Concepts and Doctrine Centre 2023b, 86](#)).

The tasking phase involves receiving external direction and the planning, resourcing, and internal allocation of ISR capabilities in relation to the expected outcomes, including the validation and prioritization of ISR requirements ([Development, Concepts and Doctrine Centre 2023a, 5](#)). Collection represents the acquisition of information through ISR means, whether technical sensors or human sources, with the aim of delivering raw data ([U.S. Air Force 2025, 18](#)). Processing translates raw data into a format usable for subsequent exploitation, storage, or dissemination, and can be carried out by human operators or by technological processes, depending on the nature of the data ([Development, Concepts and Doctrine Centre 2023b, 87](#)). Exploitation involves the examination of data in order to derive and attribute value, through entity extraction (detection, recognition, classification, identification) and through contextual analysis that adds knowledge and experience to observations. The final step, dissemination, ensures access to the resulting data, information, and

intelligence products, either in near real time or sequentially, following rigorous processing and exploitation ([Development, Concepts and Doctrine Centre 2023a, 5](#)). The fundamental doctrinal observation regarding TCPED is that, in the context of modern ISR, these processes “are not linear or circular, being dynamically employed depending on the required outcome, and can be used sequentially, concurrently, or independently” ([Development, Concepts and Doctrine Centre 2023a, 4](#)).

ISR has undergone a structural transformation in the last two decades, moving from a fragmented, platform-centric approach to an integrated capability. British doctrine observes that “technological advancements have blurred the lines between operational domains, with ISR capabilities in one domain now able to support others simultaneously”. Access to information is shifting from a hierarchical, top-down model toward an access-based model, in which information flows freely across all levels of command ([Development, Concepts and Doctrine Centre 2023a, 9](#)). Hoehn and Smagh describe this transformation as a shift “from a manpower-intensive force optimized for permissive environments to an automation-intensive force capable of defeating peer adversaries in highly contested environments” ([Hoehn and Smagh 2020, 2](#)).

One of the most significant developments is the growing importance of commercial ISR capabilities. British doctrine acknowledges that these capabilities, whether government-owned and contractor-operated or contractor-owned and contractor-operated, “can sometimes exceed those of military and government sources, particularly in space-based collection and the PED of publicly available information” ([Development, Concepts and Doctrine Centre 2023a, 40](#)). These capabilities are subject to the same tasking mechanisms as military ISR, but may have contractual, political, or legal constraints specific to each provider.

The emergence of OSINT as a major discipline represents probably the most disruptive recent evolution. British doctrine explicitly states that ISR, “traditionally reliant on specialized military platforms, is now seeing publicly available information vastly exceed defense sources in volume and variety”, including data from social media, smart devices, the internet, and urban sensors ([Development, Concepts and Doctrine Centre 2023a, 40](#)). With the increasingly widespread global use of social media, publicly available information has become “a vital source of battlespace information, offering insights into adversary intent, capability, and operational execution” ([Hoehn and Smagh 2020, 16](#)).

The doctrinal response to these transformations is reflected in concepts such as Joint All-Domain Operations (JADO) and Joint All-Domain Command and Control (JADC2). The U.S. Department of Defense aims to “connect ISR sensors across all warfighting domains (space, air, land, sea, and cyber) directly with commanders and weapon systems, accelerating data sharing to enable U.S. and allied forces to outthink, outpace, and outmaneuver adversaries” ([Hoehn and Smagh 2020, 2](#)). This reconfiguration represents an abandonment of ISR operations organized by service

and a shift toward integrated multi-domain capabilities, in which “the right data is available to the right actors at the right time to focus on delivering effects” ([Bollmann and Heltberg 2023](#), 156).

ISR relies on several collection disciplines, known generically in international literature as INTs. These include Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Geospatial Intelligence (GEOINT), Measurement and Signature Intelligence (MASINT), Open-Source Intelligence (OSINT), Technical Intelligence (TECHINT), Cyber Intelligence (CYBINT), and Acoustic Intelligence (ACINT) ([Development, Concepts and Doctrine Centre 2023b](#), 77-81). Recent doctrine emphasizes multi-INT operations and all-source fusion, recognizing that “no single sensing type provides a complete solution and individual sensor observations reveal their true value when collated, correlated, and analyzed together” ([Development, Concepts and Doctrine Centre 2023a](#), 56). Fusion, defined as “the blending of intelligence, information, and data from multiple sources or agencies into a coherent picture where the origin of individual items is no longer apparent” ([Development, Concepts and Doctrine Centre 2023b](#), 28), goes beyond simple correlation and adds context, insight, and foresight. Doctrine acknowledges, however, that the traditional linear fusion model has limitations at the operational and higher tactical levels, being insufficiently adapted to fleeting targets and to “unknown unknowns” type uncertainties ([Development, Concepts and Doctrine Centre 2023a](#), 56).

The transformation of ISR, however, exceeds the technological dimension. The concept of problem-centric ISR “changes linear intelligence processes and the practice of undertaking processing, exploitation, and dissemination within disciplinary channels by adopting greater mission command within the ISR enterprise”. This type of organization “task organizes resources around the operational outcome required, combining analysis, PED, and collection against specific operational problems” ([Development, Concepts and Doctrine Centre 2023a](#), 65). The conceptual evolution reflects a doctrinal awareness in which the classical ISR architecture, organized by disciplines and platforms, is insufficiently adapted to the rhythm and complexity of current operations.

3. The ISR-Decision Chain. Situational Awareness as Cognitive Articulation

The previous chapters have established, separately, that quality military decision-making depends on the commander’s capacity to anticipate the evolution of the situation and that ISR represents an integrated architecture for the collection, processing, and dissemination of operational data. The articulation of ISR functions with the three levels of the Endsley model allows for a precise analysis of the contribution of each phase of the TCPED process and, at the same time, the identification of its conceptual limits. Sensors and collection platforms feed Level 1,

providing the raw perceptual input, whether imagery, electromagnetic, human, or geospatial. Processing and exploitation operate partially at Level 2, transforming raw data into contextualized understanding through entity extraction and sensor fusion. Level 3 of situational awareness, namely cognitive projection, however, exceeds the proper perimeter of ISR. Intelligence estimates, the anticipation of enemy courses of action, and anticipative products are outputs of the intelligence cycle and of human analytical judgment that intervene after the dissemination phase of TCPED. This observation fixes the conceptual limit of ISR as infrastructure. ISR can support the commander's decision only up to the level of comprehension. Projection, essential for quality decision-making, presupposes cognitive processes distinct from the technological ones of collection and processing.

The central argument of this chapter starts from the observation that the classical ISR architecture is built predominantly to support Levels 1 and 2 of situational awareness, while quality decision-making depends structurally on Level 3. The study by Hærem et al. has empirically demonstrated this asymmetry, identifying Level 3 as the only significant predictor for all dimensions of operational performance (Haerem, et al. 2022, 7). The implication is that massive investments in collection capabilities produce diminishing decisional returns if they are not accompanied by proportional investments in the capacity for cognitive projection, whether human or technologically augmented.

This asymmetry is implicitly recognized by operational practice as well. Hoehn and Smagh observe that the purpose of ISR is to “inform commanders to enable decision-making, support military planning by anticipating adversary actions and defining the operational environment, warn friendly forces of threats, support deceptive techniques and counter adversary deception, identify adversary vulnerabilities [...] and assess combat effectiveness” (2020, 3-4). The list attributes to ISR functions that go far beyond the simple provision of data, entering firmly into the territory of Level 3 of situational awareness. Nevertheless, the capacity to deliver this anticipatory value remains dependent on the quality of the human analysis that intervenes between raw data and the final product.

Yufik and Malhotra synthesize this tension through the distinction they operate between situational awareness, defined as “immediate knowledge of the operation's conditions, geographically constrained in time, essentially, knowing what is currently happening around Soldiers”, and situational understanding, defined as “the product of analyzing and judging relevant information to determine relationships among mission variables, facilitating decision-making” and which “enables commanders to understand the implications of current events and forecast future occurrences” (2021, 1). Current collection systems efficiently produce the first type of output. Producing the second remains a structural problem, since it presupposes cognitive capacities for constructing relationships and for mental simulation that the classical ISR architecture does not address directly.

In classical architecture, the ISR-decision flow follows a linear sequence. The commander issues intelligence requirements through planning documents, intelligence structures task ISR capabilities, the collected data is processed and exploited at the discipline level, and is subsequently disseminated to the intelligence cycle or directly to specific recipients. ISR products that enter the intelligence cycle are fused and analyzed and are then disseminated to decision-makers. The model presupposes a separation between collection operations and the analytical process, between raw data and the intelligence product, between the collection phase and the exploitation phase. Hoehn and Smagh (2020, 4) describe the mechanism in explicitly decisional terms: “analysts then derive meaning from information, resulting in intelligence and generating a picture of adversary activity that answers the commander’s information needs and ultimately drives decision-making.”

The advantages of the classical model are verifiability and analytical quality. Filtering raw data through the disciplines, multi-source fusion, and contextualized human analysis reduces the risk of interpretive error, adversarial deception, and information noise. The disadvantage is speed. The process described consumes hours, days, sometimes weeks, depending on the complexity of the requirement and on the workload of the analytical structures. In operational environments with large time windows, the model works adequately. In contemporary operations, marked by fleeting targets and compressed decisional rhythms, the model becomes insufficient.

The doctrinal response to the limits of the classical model consists of the compression of the ISR decision chain. British doctrine explicitly states that ISR “can directly support operations by providing real-time monitoring and direct passage of situational awareness and force protection information to a commander or other force elements” (Development, Concepts and Doctrine Centre 2023a, 5-6). This formulation amounts to a redefinition of the relationship between ISR and the intelligence cycle, with ISR being doctrinally authorized to deliver directly operational products without mandatory passage through the complete analytical filter. The concepts that formalize this compression are “sensor-to-shooter” and the F3EAD cycle (Find-Fix-Finish-Exploit-Analyze-Disseminate) from the targeting process. Both describe flows in which ISR products reach the decision-maker unmediated or directly trigger kinetic actions, particularly in counter-terrorism and counter-insurgency operations. The exploitation and analysis phases are displaced after the action, feeding the classical intelligence cycle retrospectively for the planning of future missions.

The gain in speed, however, comes with a structural cost. Hoehn and Smagh (2020, 5) identify the declared objective of the U.S. military as the conduct of the ISR process at “machine speed, an accelerated pace achieved by employing artificial intelligence and cloud computing”, capable of compressing the cycle to “seconds to single-digit minutes, enabling U.S. and allied forces to outthink, outpace, and outmaneuver its adversary on the battlefield”. Achieving this objective, however, presupposes the

transfer of certain analytical functions from human operators to automated systems, which raises the problem of verification and of trust in algorithmically processed ISR products.

Bollmann și Heltberg (2023, 9) synthesize this tension through the observation that the abundance of data and the ever-increasing speed of the decision cycle can produce “information overload and information over-reliance”, leading to “inertia and paralysis of action” and leaving decision superiority in the adversary’s favor. The compression of the ISR-decision chain does not, therefore, solve the fundamental problem of the articulation between data and decision. It reformulates it at a higher speed, shifting the question from the temporal plane to the qualitative one. Who validates ISR products processed at machine speed, and what mechanisms ensure that speed does not compromise the quality of the cognitive projection that decision-making requires?

The synthesis of this chapter leads to a conclusion with direct implications for the orientation of investments in ISR capabilities. Situational awareness as a bridge between ISR and decision-making is not an automatic product of the volume of data collected, but the result of an architecture that functionally links the sensors to the cognitive capacity of the decision-maker. This architecture has three simultaneous components: a collection component, which feeds Level 1; a processing and fusion component, which builds Level 2; and an anticipation and projection component, which sustains Level 3. The weakening of any of the three components compromises the quality of the decision, regardless of the robustness of the others. At present, operations disproportionately stress the projection component through temporal pressure and through the volume of data. The doctrinal response through chain compression addresses speed, but leaves open the question of how situational understanding is built under conditions of automated processing.

Artificial Intelligence and the Limit of Understanding. Augmentation or Substitution?

Collection capabilities produce ever-growing volumes of data, feeding Levels 1 and 2 of situational awareness, while the capacity for cognitive projection, essential for quality decision-making, remains limited by human cognitive constraints. Artificial intelligence (AI) is proposed in the literature and in doctrine as a response to this asymmetry. Examining this proposal, however, requires a nuanced approach that avoids both technological enthusiasm and reflexive rejection, identifying with precision what AI can and cannot do in the ISR-decision chain.

The most telling indicator of the problem that AI seeks to solve is the distribution of intelligence analysts’ time. Hoehn and Smagh point out that analysts spend approximately 80% of their time searching for data and only 20% interpreting it, a ratio that exactly inverts the priorities that the process should serve (2020, 16).

The cause is structural. The volume of collected data far exceeds human processing capacity, and the classical TCPED architecture treats each disciplinary flow separately, fragmenting the analytical effort. AI and machine learning are the technologies that promise to automate the search and filtering phase, freeing the analyst's cognitive capacity for the comprehension and projection phases.

This promise is also explicitly reflected in British doctrine, which states that "automation, artificial intelligence (AI), and machine learning (ML) are increasingly central to ISR, particularly in processing, exploitation, and dissemination (PED), due to the finite capacity of human analysts". The technology can offer "speed, concurrency, scalability, and accuracy advantages over humans in processing and analyzing vast and diverse datasets" ([Development, Concepts and Doctrine Centre 2023a](#), 73). Meerveld and Lindelauf (2025, 106) describe the role of AI as that of an "oracle-like adviser", capable of mitigating information overload and analyst fatigue, supporting in particular the observation and orientation phases of the OODA loop.

The application of AI in ISR has moved beyond the experimental phase, with several operational programs of the U.S. military illustrating the current technological maturity. Project Maven, launched in 2017, develops computer vision algorithms for the characterization and identification of targets from video footage and imagery ([Pellerin 2017](#)). Minotaur, developed by Johns Hopkins Applied Physics Laboratory, is an automated intelligence correlation processor that analyzes data from multiple sensors and enables rapid filtering and prioritization ([Koscak 2022](#)). TITAN (Tactical Intelligence Targeting Access Node) is an AI/ML-assisted mobile intelligence processing station, designed for the rapid dissemination of intelligence products directly exploitable for targeting ([Palantir n.d.](#)).

The empirical results of applying AI to aerial situational awareness are telling. Li et al. present a unified architecture based on graph neural networks and computer vision for the automatic recognition of aerial swarm configurations. The system achieves an accuracy of over 90.1% in the recognition and partitioning of aerial formations, over 85% in tactical scenarios with irregular flight intervals, and over 80.4% even under significant disturbances of position and heading ([Li, et al. 2025](#), 1). The system operates at a latency of milliseconds, with a throughput of approximately 30 frames per second ([2025](#), 13). These values translate the declared objective of "machine speed" into concrete performance, demonstrating that AI can perform recognition and classification tasks at speeds and volumes incompatible with human processing. The aggregate effect on analytical capacity is equally significant. Hoehn and Smagh (2020, 34) estimate that AI-assisted tools can enable analysts to process two to three times as much data within the same timeframe. This gain is not, however, a simple multiplication of existing capacity, but a qualitative redistribution of analytical effort from search and filtering toward interpretation and anticipation.

The application of AI in ISR can be mapped onto the Endsley model, which allows for a precise evaluation of its contribution to the commander's decision-making. At Level 1, AI extends perceptual coverage, automating the detection and classification of objects in volumes of data that the human operator could not parse. At Level 2, horizontal multi-source fusion systems and automated correlation systems build integrated contextual images, going beyond the limits of classical disciplinary channels. The real challenge appears at Level 3, where AI has to support cognitive projection, namely the anticipation of the situation's evolution and the understanding of the implications for decision-making.

Yufik and Malhotra propose the concept of the “gnostron”, a theoretical architecture based on virtual associative networks and active inference, which seeks to confer on the technology the capacity for situational understanding, defined as the formation of mental models that approximate human comprehension. The difference from the classical paradigm of machine learning is structural. “Conventional AI and cognitivist psychology have focused on learning and reasoning while being *fanatically uninterested* in the role of understanding”, the authors observe, adding that current machine learning systems “are capable of detecting and identifying objects, but are limited in apprehending relations and explaining their decisions”. A proof-of-concept demonstrator for target recognition showed a reduction in complexity of nearly two orders of magnitude, while preserving an acceptable error amplitude (2021, 8,16). These results suggest that moving beyond Level 2 toward Level 3 is technologically possible, but requires a conceptual reconfiguration of AI that treats understanding as an objective distinct from detection and classification.

The integration of AI into the ISR-decision chain also raises a series of risks that the literature treats seriously. One of these is algorithmic opacity. Yufik and Malhotra (2021, 20) synthesize the black box problem, stating that neural networks with millions or billions of parameters make it impossible to fully understand the mode of operation, and the responses to all possible inputs remain unknown. This opacity creates a justified reluctance in delegating critical decisions to AI, particularly in situations where errors, such as the misidentification of an aircraft, can have catastrophic consequences. Bollmann and Heltberg (2023, 156) confirm that trust in AI for decision-making remains problematic due to the difficulty of justification and of compliance with ethical and legal perspectives, especially in the case of self-learning algorithms.

Another category of risks concerns the cognitive rigidity of automated systems. Yufik and Malhotra (2021, 6) draw attention to the phenomenon of “pathological tunnel vision”, in which mental models, whether human or technological, shaped by experience, can consolidate interpretive rigidities. Historical military errors are often the consequence of judgments confined within flawed templates. The transfer of these templates into AI does not solve the problem, but automates it at a higher speed and with a higher degree of institutional trust in the output.

A third category of risks concerns the organizational and cognitive effects of direct access to data for all levels of command. Bollmann and Heltberg (2023, 160) identify the temptation of micromanagement, through which strategic leaders with access to real-time imagery intervene in tactical decisions, undermining subordinate initiative and the principle of mission command. At the same time, abundant access to data can paradoxically produce a cognitive distance from the battlefield, particularly when tactical decision-makers do not possess the technological knowledge to understand the limits of the tools they use. Vasile (2026, 21) describes this tension at the strategic scale through the concept of a “battlefield singularity”, in which the volume and speed of information generated by AI exceed the capacity of human commanders to understand it in context. Meerveld and Lindelauf (2025, 111) warn that these risks are insufficiently addressed in the formal science literature, being treated predominantly by the social sciences, which produces a disciplinary asymmetry in the understanding of the phenomenon.

AI does not solve, in its current form, the fundamental problem of the articulation between data and decision. Automated detection and classification systems extend processing capacity at Levels 1 and 2 of situational awareness, but leave open the question of the cognitive projection required at Level 3. The research directions represented by the “gnostron” suggest that overcoming this limit is possible, but implies a conceptual reconfiguration of AI that integrates understanding as a distinct objective. The short-term operational answer lies in hybrid human-machine architectures, in which AI augments the capacity of analysts and commanders without substituting their judgment. Yufik and Malhotra (2021, 21) describe this aspiration as a “shared situational understanding” between human and machine, capable of amplifying the human grasp of the situation, increasing trust, and reducing costly errors through substantive-level interaction rather than through the sharing of computational details. Such an architecture presupposes that the human remains the final decision-maker, while AI functions as an instrument of cognitive extension, not as an autonomous arbiter of the decision. This requirement is, at the same time, the condition of the legal and ethical compatibility of AI integration into military operations, particularly with regard to the use of lethal force.

Conclusions

The commander’s decision remains, despite all technological transformations, an essentially human act, in which responsibility is indivisible, and the consequences are measured in lives. Everything discussed in the previous pages gravitates around this fundamental observation. No quantity of data, no speed of processing, no algorithmic accuracy absolves the commander from the burden of deciding and of being accountable for the decision made. This reality sets the stakes of the article and, at the same time, the limits of any reflection about ISR.

The argument built throughout this work has sought to show that decision superiority is not born from the abundance of information, but from the capacity to transform that information into understanding. The cognitive models of decision-making, from Klein's pattern recognition to Boyd's competitive loop and to Endsley's situational awareness, converge on the same observation. The commander wins when he/she correctly projects the evolution of the situation, and this projection is the product of a cognitive architecture that experience builds over time, and that only quality information input can feed. ISR is, in this logic, the infrastructure that makes projection possible. Without ISR, the commander decides in a vacuum. With a poorly calibrated ISR process, he/she decides on the basis of an incomplete or distorted image of reality. With an ISR well-articulated with the cognitive process of decision-making, he has the chance, but not the guarantee, of a good decision.

The asymmetry identified in this article lies precisely here. Massive investments in collection capabilities have produced an architecture capable of flooding with data, but incapable, by its very construction, of systematically producing situational understanding. Sensors answer questions about what is seen, where, and when. The decision, however, rests on questions about what it means, what comes next, and what its implications are. The distance between the two sets of questions is not bridged by more sensors, but rather by a reconfiguration of the entire ISR-decision chain, in which processing, fusion, and anticipation gain the same importance as collection. Artificial intelligence offers powerful tools for this reconfiguration, but it does not realize it automatically. It can extend perception and comprehension, accelerate multi-source fusion, and thin the data volume for the analyst. Situational understanding, in the proper sense of the term, remains, however, a cognitive competence that is not, for the moment, solved by algorithms.

The modernization of ISR in allied armed forces, including in the Romanian Armed Forces, must not be a race to acquire more sensors or to integrate more platforms. It must be a process of redesigning the relationship between human and technology, between collection and analysis, between data and decision. The wisest investments will be those that reduce the gap between Level 1 of situational awareness, excessively fed by sensors, and Level 3, undernourished by projection capacities. These investments are less spectacular than the acquisition of a drone or a satellite system, but more consistent with the commander's real need. They encompass the training of analysts, the development of fusion tools, the integration of AI as a cognitive assistant, and, above all, the cultivation of that intangible competence called "digital coup d'œil", the commander's capacity to discern meaning in the midst of abundance.

How is a hybrid human-machine architecture practically built, in which the commander remains the decision-maker, but AI systematically augments his projection capacity? What are the institutional mechanisms that can guarantee that the speed of the technology does not turn into decisional precipitation, and that algorithmic opacity does not erode the individual responsibility of the commander?

How do these requirements translate into national doctrine and into officer training programs? The answers to these questions will not come solely from the specialized literature, but will require a sustained conversation between those who build the capabilities, those who use them, and those who reflect on their strategic and ethical implications.

References

- Bollmann, Anders Theis, and Therese Heltberg.** 2023. "The Strategic Corporal, the Tactical General, and the Digital Coup d'oeil -- Military Decision-Making and Organizational Competences in Future Military Operations." *Scandinavian Journal of Military Studies* 6 (1): 9-160. doi:10.31374/sjms.190.
- Boyd, John R.** 2012. *The Essence of Winning and Losing*. https://slightlyeastofnew.com/wp-content/uploads/2010/03/essence_of_winning_losing.pdf.
- D'Alessio, Ivan, Umberto Aitella, Anna Maria Giannini, and Jessica Burrai.** 2024. "What about Military Decision-Making?: A Bibliometric Review of Published Articles." *Behavioral Sciences* 14 (7): 2-3. doi:10.3390/bs14070514.
- Development, Concepts and Doctrine Centre.** 2023a. "Joint Doctrine Note 1/23, Intelligence, Surveillance and Reconnaissance." UK Ministry of Defence. 3-73.
- _____. 2023b. „Joint Doctrine Publication 2-00 - Intelligence, Counter-intelligence and Security Support to Joint Operations." UK Ministry of Defence. 28-180.
- Endsley, Mica R.** 1995. "Toward a Theory of Situation Awareness in Dynamic Systems." *Hum Factors* 37 (1): 34-49. doi:10.1518/001872095779049543.
- Haerem, Thorvald, Sigmund Valaker, Eric Arne Lofquist, and Bjorn Tallak Bakken.** 2022. "Multiteam Systems Handling Time-Sensitive Targets: Developing Situation Awareness in Distributed and Co-located Settings." *Front. Psychol.* 13: 7-8. doi:10.3389/fpsyg.2022.864749.
- Hoehn, John R, and Nishawn S Smagh.** 2020. "Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition." 2-34.
- Klein, Gary.** 2017. *Sources of power: how people make decisions*. 20th Anniversary Edition. London: The MIT Press.
- Koscak, Paul.** 2022. *Innovative Tech Helps AMO Combat Smugglers*. Accessed May 08, 2026. <https://www.cbp.gov/frontline/air-and-marine-operations-minotaur>.
- Li, Leyan, Rennong Yang, Anxin Guo, and Zhenxing Zhang.** 2025. "A Unified GNN-CV Framework for Intelligent Aerial Situational Awareness." *Sensors* 26 (1): 1-13. doi:10.3390/s26010119.
- Meerveld, Herwin, and Roy Lindelauf.** 2025. „Data Science in Military Decision-Making: Foci and Gaps." *Global Society* 39 (2): 106-111. doi:10.1080/13600826.2024.2353657.
- Palantir.** n.d. *TITAN: Deploying the U.S. Army's first AI-defined vehicle*. Accessed May 09, 2026. <https://www.palantir.com/titan/>.

Pellerin, Cheryl. 2017. *Project Maven to Deploy Computer Algorithms to War Zone by Year's End.* <https://www.war.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/>.

Simon, Herbert A. 1955. „A Behavioral Model of Rational Choice.” *The Quarterly Journal of Economics* 69 (1): 99. [doi:10.2307/1884852](https://doi.org/10.2307/1884852).

U.S. Air Force. 2025. “Air Force Doctrine Publication 2-0, Intelligence.” March. 1-18.

U.S. Army. 2013. “Joint Publication 2-0, Joint Intelligence.” October. I-11.

Vasile, Dumitru-Cătălin. 2026. „Artificial Intelligence as a Geostrategic Vector in Reshaping the 21st Century Balance of Power.” *Bulletin of "Carol I" National Defence University* 15 (1): 17-26. [doi:10.53477/2065-8281-26-01](https://doi.org/10.53477/2065-8281-26-01).

von Neumann, John, and Oskar Morgenstern. 1953. *Theory of Games and Economic Behaviour.*

Yufik, Yan, and Raj Malhotra. 2021. “Situational Understanding in the Human and the Machine.” *Front. Syst. Neurosci.* 15: 1-9. [doi:10.3389/fnsys.2021.786252](https://doi.org/10.3389/fnsys.2021.786252).

DECLARATION OF CONFLICTING INTERESTS

The author declares that there are no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

DECLARATION ON THE USE OF AI

Claude Opus 4.7 was used to improve readability and language, as well as to assist with the translation of the article into English. After using this tool, the author reviewed and edited the text as necessary and takes full responsibility for the content of the article.

Strategic Autonomy without Alliances: Indonesia's Defence Dilemma

Lecturer and Researcher Nora LELYANA*

Dr. Aris SARJITO**

*Hang Tuah University

e-mail: nora.lelyana@hangtuah.ac.id

 <https://orcid.org/0000-0001-6619-4010>

**Defense Policy and National Security Studies Republic of Indonesia Defense University (RIDU)

e-mail: arissarjito@gmail.com

 <https://orcid.org/0000-0001-6319-2714>

Abstract

This article examines how intensifying alliance policies in the Indo-Pacific is reshaping the strategic choices of non-allied middle powers. As rivalry among major powers deepens and new security alignments expand, states face increasing pressure to strengthen deterrence, secure technology access, and clarify strategic positions. Indonesia presents a distinctive case because it has historically avoided formal alliances and continues to favour strategic autonomy grounded in sovereign decision-making, diplomatic flexibility, and regional multilateralism. The study asks whether strategic autonomy can remain viable without alliances amid growing regional competition. Drawing on qualitative analysis of secondary data, including policy documents, strategic reports, defence assessments, and scholarly sources, the article evaluates Indonesia's current posture and its emerging constraints. The findings indicate that strategic autonomy remains possible but is becoming more demanding. Capability gaps, fragmented procurement, maritime pressure in surrounding waters, grey-zone competition, and rising deterrence requirements all increase the costs of maintaining independence without external guarantees. Indonesia has responded through hedging, selective defence partnerships, and gradual modernisation rather than formal alignment. The article contributes by introducing the concept of a middle-power non-aligned defence dilemma, in which sovereignty and policy discretion are preserved, but strategic burdens rise as competition intensifies. The Indonesian case suggests that future autonomy will depend less on distance from partnerships than on the capacity to combine independence with credible capability and adaptive cooperation.

Keywords:

Defence Modernisation; Defence Policy; Indo-Pacific Security;
Indonesia; Non-Alignment; Strategic Autonomy.

Article info

Received: 4 April 2026; Revised: 4 May 2026; Accepted: 8 June 2026; Available online: 30 June 2026

Citation: Lelyana, N., and A. Sarjito. 2026. "Strategic Autonomy without Alliances: Indonesia's Defence Dilemma."
Bulletin of "Carol I" National Defence University, 15(2): 69-90. <https://doi.org/10.53477/2284-9378-26-19>



© „Carol I” National Defence University Publishing House

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC-SA)

1. Introduction

1.1. Background

The Indo-Pacific has become the main arena of contemporary strategic competition, shaped largely by the intensifying rivalry between the United States and China. What began as economic competition has increasingly expanded into military modernisation, technological contestation, maritime disputes, and competing visions of regional order. The South China Sea, the Taiwan Strait, critical sea lines of communication, and digital infrastructure have emerged as interconnected theatres in which power transition dynamics are increasingly visible (Cooper and Carr 2023). As rivalry deepens, regional states face a more uncertain security environment characterised by heightened deterrence signalling, defence spending growth, and institutional fragmentation.

One major response to this changing environment has been the revival of alliance systems and the rise of minilateral security arrangements. The United States has strengthened bilateral alliances with Japan, Australia, the Philippines, and South Korea while simultaneously encouraging more networked forms of defence cooperation. In parallel, the Quadrilateral Security Dialogue (Quad) has evolved into a more structured mechanism for strategic coordination, while AUKUS has introduced a new layer of advanced defence-technological collaboration centred on undersea warfare, cyber capabilities, and emerging technologies (Koga 2025). These developments indicate that security cooperation in the Indo-Pacific is increasingly moving toward flexible coalition-building rather than relying solely on traditional multilateral institutions. At the same time, new forms of regional multilateralism reflect unresolved questions about order, legitimacy, and strategic leadership (Wirth and Jenne 2022).

For small and middle powers, this environment creates growing pressure to clarify strategic preferences. While many states seek to avoid explicit alignment, intensifying great-power competition narrows room for manoeuvre. Choices concerning military procurement, infrastructure financing, diplomatic language, technology standards, and maritime cooperation increasingly carry geopolitical implications. Southeast Asian states have attempted to preserve agency amid strategic competition rather than passively accept external pressures (Khoo 2022). Yet, maintaining such agency requires increasingly sophisticated diplomacy and credible national capabilities.

Indonesia occupies a distinctive position within this landscape. Historically, Indonesian foreign policy has been guided by the principle of *bebas aktif* – remaining independent from great-power blocs while actively contributing to peace and regional stability. This tradition has informed Jakarta's support for ASEAN centrality, inclusive regionalism, and resistance to exclusive security architectures. Indonesia has also preferred strategic flexibility, allowing cooperation with multiple partners without entering formal alliance commitments. Such behaviour resembles hedging,

whereby states pursue selective engagement while mitigating risks associated with uncertainty (Kuik 2023). Indonesia's advocacy of the ASEAN Outlook on the Indo-Pacific further reflects an effort to preserve regional inclusivity and middle-power agency through norm entrepreneurship (Putra, Cangara, and Darwis 2024). However, as strategic competition sharpens, the sustainability of autonomy based primarily on diplomatic flexibility increasingly depends on whether it is matched by credible defence capacity. Indonesia's pursuit of strategic autonomy reflects a rational response to intensifying great-power rivalry, yet capability limitations continue to constrain policy independence.

1.2. Problem Statement

Indonesia seeks strategic autonomy while refusing formal alliances. This posture has long offered political benefits: it protects sovereignty, preserves diplomatic flexibility, reduces entrapment risks, and supports Indonesia's image as an independent regional actor. However, the same posture is becoming more difficult to sustain under contemporary strategic conditions.

First, defence modernisation requires substantial and sustained investment. As a vast archipelagic state located astride major maritime routes, Indonesia must develop naval reach, air surveillance, missile defence, cyber resilience, and joint-force readiness. These capabilities are capital-intensive and technologically demanding. Without alliance-based burden sharing or external security guarantees, most costs must be carried domestically.

Second, maritime pressure around the Natuna Islands and wider South China Sea has increased the practical need for deterrence. While Indonesia is not a formal claimant in the central South China Sea disputes, repeated incidents involving fishing fleets, coast guard presence, and jurisdictional assertions have demonstrated that sovereignty protection requires persistent maritime domain awareness and enforcement capacity (Scott 2019). Strategic ambiguity may preserve diplomatic space, but it does not automatically generate deterrent credibility.

Third, Indonesia remains dependent on foreign suppliers for major weapons systems, maintenance ecosystems, advanced sensors, and defence-industrial inputs. Procurement diversification can reduce overdependence on any single source, yet reliance on external technology also creates vulnerabilities related to sanctions, delays, interoperability gaps, and supply-chain disruption. Indonesia's strategic culture values autonomy, but material capability generation still depends significantly on external partnerships (Subagyo et al. 2024).

Fourth, Indonesia's deterrence capacity remains limited relative to the complexity of threats in the surrounding region. Non-traditional threats, grey-zone coercion, maritime incursions, and major-power military presence require integrated responses beyond symbolic force posture. The central dilemma is not whether

Indonesia should abandon non-alignment, but whether non-allied autonomy can remain credible without sufficient defence capacity, maritime awareness, and strategic signalling. Accordingly, Indonesia's challenge is not a binary choice between alliance and neutrality, but the question of how to preserve autonomy when capability-building needs are steadily rising.

1.3. Research Gap

Existing international relations literature has extensively examined alliance formation, balancing, bandwagoning, and the strategic behaviour of secondary states under power rivalry. More recent studies also analyse ASEAN hedging strategies, regional neutrality narratives, ASEAN centrality, and the rise of minilateral institutions such as the Quad and AUKUS (Koga 2025; Sullivan de Estrada 2023). These works provide important insights into how states respond to uncertainty and changing order structures.

However, less attention has been given to autonomy strategies without alliance commitments. Specifically, insufficient analysis exists regarding the way in which middle powers such as Indonesia seek to maintain strategic autonomy without formal security guarantees while operating in a highly contested region. There is also limited conceptual discussion of the burdens generated by non-allied autonomy, including capability gaps, procurement dependence, and signalling dilemmas. Indonesian middlepowermanship and strategic culture are increasingly discussed, yet the defence costs of preserving autonomy remain underexplored (Maulana Prasetya, Ladiqi, and Salleh 2025). This article addresses that gap by focusing on autonomy as a strategy that requires material foundations, not merely diplomatic posture.

1.4. Research Questions

This article investigates Indonesia's defence dilemma through three interrelated questions. First, why does Indonesia continue to maintain strategic autonomy without entering formal alliances despite a more polarised Indo-Pacific environment? Second, what strategic, operational, and procurement dilemmas emerge from this posture as regional competition intensifies? Third, can non-allied autonomy remain a viable long-term strategy amid expanding great-power rivalry, coalition-building, and rising deterrence demands? These questions aim to evaluate both the logic and limits of Indonesia's current strategic orientation.

1.5. Contribution

This article contributes to the literature in the field by extending debates on strategic autonomy toward the concept of autonomy without alliances. Using Indonesia as a case of a non-aligned middle-power state, the article contributes to debates on how states preserve strategic autonomy without formal alliances while confronting increasing deterrence, capability, and security demands. It bridges defence policy analysis, hedging theory, middle-power behaviour, and alliance studies. Empirically, it clarifies how autonomy can generate hidden costs in capability development

and strategic signalling. Practically, it offers policy relevance for states seeking to preserve sovereign decision-making while avoiding formal alliance commitments in an increasingly competitive regional order.

2. Methods

2.1. Research Design

This study employs a qualitative explanatory design based on secondary-source analysis to examine how Indonesia pursues strategic autonomy while avoiding formal alliance commitments under conditions of intensifying Indo-Pacific competition. A qualitative approach is appropriate because the subject of inquiry concerns state strategy, defence posture, foreign policy behaviour, institutional preferences, and strategic dilemmas that cannot be adequately captured through a single quantitative indicator. Indonesia's defence choices are shaped not only by measurable variables such as expenditure levels or force structure, but also by perceptions of threat, historical doctrine, signalling preferences, and political calculations regarding sovereignty and external dependence.

Explanatory qualitative methods are particularly useful for tracing policy logic and interpreting how decision-makers reconcile competing objectives, including autonomy, deterrence, flexibility, and regional legitimacy. For middle powers, strategic behaviour often reflects layered responses rather than binary alignment choices, requiring contextual analysis of speeches, official documents, and policy outcomes (Gerstl 2022; Le Dinh 2021). This design, therefore, allows the study to assess not merely what Indonesia does, but why particular choices persist despite changing strategic conditions.

2.2. Data Sources

The analysis relies exclusively on publicly available and verifiable documentary sources. Domestic sources include Indonesian Defence White Papers, Ministry of Defence strategic planning documents, presidential speeches, Ministry of Foreign Affairs statements, and relevant parliamentary records concerning defence procurement, budget priorities, or national security debates. These materials are important for identifying official threat perceptions, force development priorities, and the normative foundations of Indonesia's strategic autonomy.

International and comparative sources are used to situate Indonesia within the broader regional security environment. These include SIPRI military expenditure and arms transfer datasets, which provide consistent indicators of defence spending trends and procurement patterns; IISS *The Military Balance*, which offers comparative force structure and readiness assessments; ASEAN communiqués and official statements relevant to regional security norms; and peer-reviewed journal articles analysing Indo-Pacific strategic competition, hedging, and Southeast Asian agency (Putra 2026; Wilson 2018). The study also draws on policy papers from

recognised think tanks such as CSIS, ISEAS – Yusof Ishak Institute, the Lowy Institute, RAND, and similar institutions, particularly where these provide current assessments of maritime security, defence diplomacy, and regional military balance (de Medeiros and Mazat 2019; Paribatra 2025).

Triangulating these sources improves analytical reliability by reducing dependence on any single institutional narrative or dataset. Official Indonesian documents illuminate internal strategic intentions, while international databases and external assessments help evaluate actual capabilities, procurement dependencies, and the surrounding threat environment. Combining domestic and international materials is therefore necessary to compare stated policy autonomy with material constraints and external pressures. This approach is informed by the literature on strategic autonomy, which emphasises the relationship between sovereign decision-making, external dependencies, and structural pressures in the international system (Chung 2026; Kuik 2023).

2.3. Analytical Method

The article applies thematic analysis to identify recurring patterns across documents, datasets, and expert assessments. Themes include autonomy logic, alliance avoidance, capability constraints, procurement dependence, maritime vulnerability, external strategic pressure, and hedging behaviour. These themes were selected because they recur consistently in debates on Indonesian defence policy and broader Southeast Asian strategic responses.

Sources are compared to identify areas of consistency, contradiction, and policy evolution. For example, official claims of independent posture are assessed alongside procurement trends, defence modernisation needs, and regional security developments. This comparative reading enables the study to distinguish rhetorical continuity from practical adaptation and to derive policy implications regarding the sustainability of non-allied autonomy (Anwar 2020; Gindarsah and Priamarizki 2021).

2.4. Ethics & Transparency

All data used in this study were drawn from public, legal, and citable sources. No classified materials were accessed, and no interviews or human participants were involved. Accordingly, the research presents no direct ethical risk to individuals. All interpretations, judgements, and analytical conclusions remain solely the responsibility of the author.

3. Results

3.1. Why Indonesia Rejects Alliances

The findings indicate that Indonesia's continued rejection of formal military alliances is rooted less in temporary policy preference than in durable strategic culture. Across official discourse, defence planning narratives, and foreign policy behaviour, alliance avoidance appears embedded in the long-standing doctrine of *bebas aktif*

– an independent and active foreign policy orientation that emerged in the early post-independence period. In contemporary practice, this doctrine functions as a strategic identity that emphasises autonomous decision-making, diplomatic initiative, and resistance to bloc politics. Rather than signalling passivity, it frames Indonesia's role as an actor able to engage all major powers while remaining formally uncommitted ([Karim 2026](#)).

Patterns across sources also show that sovereignty sensitivity remains a central factor. Indonesia's historical experience with colonial domination, territorial fragmentation risks, and external intervention has generated a strong political norm against binding security dependence. Formal alliances may be interpreted domestically as constraints on sovereign discretion, particularly if treaty obligations could draw Indonesia into conflicts unrelated to its direct national interests. This helps explain Jakarta's preference for flexible partnerships over codified commitments. Strategic culture studies similarly note that Indonesian defence diplomacy often prioritises autonomy, status, and non-subordination in external relations ([Arif 2025](#)).

A related theme is the anti-dependence tradition. The evidence suggests that Indonesian policymakers remain cautious about relying excessively on any major power for security guarantees. While defence cooperation with external partners is accepted, guaranteed protection by another state could create vulnerabilities of political leverage, conditionality, or abandonment. Alliance commitments are therefore viewed not only as potential shields but also as possible sources of strategic constraint. This concern has become more salient in an era where great-power competition is fluid, and long-term reliability cannot be assumed.

Domestic political legitimacy further reinforces alliance reluctance. Findings from broader Indonesian foreign policy studies indicate that national elites and public opinion often reward visible independence while scrutinising signs of external dependency ([Mietzner 2025](#)). Formal alliances could invite criticism from nationalist constituencies, opposition actors, or bureaucratic factions concerned about sovereignty dilution. Even where practical cooperation is desirable, treaty-based arrangements may impose domestic political costs disproportionate to their benefits.

Finally, Indonesia's support for ASEAN centrality offers an institutional rationale for rejecting alliances. Jakarta has consistently favoured inclusive regional multilateralism over exclusive bloc structures. Formal alliance membership could complicate Indonesia's claim to impartial leadership within ASEAN or weaken its ability to mediate among members with divergent external alignments. Under intensified rivalry, ASEAN centrality has faced constraints, yet adaptation rather than abandonment remains the dominant response ([Rüland 2024](#)).

Taken together, the findings show that Indonesia rejects alliances because such arrangements are perceived to conflict with national strategic identity, sovereignty

norms, domestic legitimacy, and regional leadership preferences. Alliance avoidance is therefore best understood as a structural feature of Indonesian statecraft rather than a short-term tactical posture.

3.2. Strategic Benefits of Non-Alignment

The evidence suggests that non-alignment continues to generate tangible strategic benefits for Indonesia when managed pragmatically. The first benefit is diplomatic flexibility. Without treaty obligations, Indonesia retains discretion to calibrate responses to crises, participate selectively in security initiatives, and avoid automatic involvement in disputes among major powers. This flexibility is particularly valuable in a volatile Indo-Pacific environment where alignments are increasingly issue-specific rather than permanent. Strategic ambiguity can therefore function as a source of manoeuvrability for middle powers ([Goh 2022](#)).

A second benefit is the ability to engage the United States and China simultaneously in different domains. Indonesia can deepen defence exchanges, training, and maritime cooperation with Washington and its partners while sustaining robust trade, investment, and infrastructure ties with Beijing. This dual-track approach reduces the costs of choosing sides and allows Jakarta to extract benefits from multiple relationships. Findings across recent studies on Indonesian hedging indicate that such calibrated engagement remains central to Jakarta's external strategy ([Iksan and Soong 2023](#)).

Third, non-alignment supports procurement diversification. Indonesia has historically sourced military equipment from a range of suppliers, including Western, Asian, and other partners. This can reduce excessive dependence on a single provider and create bargaining leverage in price, technology transfer, and delivery negotiations. Diversification also helps mitigate risks associated with sanctions or policy shifts by any one supplier.

Fourth, autonomous positioning enhances Indonesia's diplomatic standing within ASEAN. Because it is not formally tied to any bloc, Indonesia can more credibly advocate dialogue, restraint, and inclusive regional mechanisms. This strengthens its image as a convening actor and supports leadership ambitions within Southeast Asia.

Overall, the findings indicate that non-alignment remains strategically useful because it maximises flexibility, preserves diversified partnerships, and sustains diplomatic legitimacy. Its value, however, depends on careful management and sufficient national capability to support independent choices.

3.3. Emerging Defence Dilemmas

While non-alignment provides benefits, the findings also reveal growing defence burdens associated with autonomy without alliances. The most fundamental constraint is the absence of an external security guarantee. Indonesia cannot rely

on treaty partners to provide automatic military assistance in a crisis. As a result, deterrence must rest primarily on national capabilities, credible signalling, and the expectation that external partners might assist voluntarily rather than by obligation.

This creates a substantial burden of self-strengthening. Indonesia must independently finance readiness, maritime patrol capacity, intelligence-surveillance-reconnaissance systems, air and naval modernisation, cyber resilience, and logistics depth across a geographically vast archipelago. For an island state with extensive sea lines and dispersed territories, these requirements are resource-intensive. Maritime security assessments show that persistent domain awareness and presence operations demand sustained investment rather than episodic deployments ([Bateman 2015](#)).

The evidence also points to slow modernisation pressures. Defence ambitions have often exceeded budget realities, producing delays in recapitalisation and uneven capability growth. Where acquisition plans depend on long procurement cycles, shifting exchange rates, or fiscal reprioritisation, force modernisation can lag behind regional developments. Studies of Indonesia's defence modernisation identify persistent gaps between planning targets and realised capability outcomes ([Febrica 2023](#)).

A further dilemma concerns fragmented procurement. Although diversification offers autonomy benefits, sourcing from multiple suppliers can generate interoperability problems, maintenance complexity, training burdens, and supply-chain inefficiencies. Different platforms may require separate sustainment ecosystems, munitions compatibility solutions, and technical standards. Regional procurement research indicates that diversification without integration can reduce operational coherence.

Maritime enforcement gaps are another recurring concern. Indonesia's Natuna waters and outer maritime zones require continuous patrol presence, legal enforcement capacity, and rapid response mechanisms. Intermittent deployments may signal resolve politically, but are less effective operationally when facing persistent grey-zone pressure or repeated incursions. The evidence suggests that geography magnifies the costs of autonomy because sovereignty assertion requires constant rather than symbolic presence.

Finally, crisis vulnerability remains significant. In coercive scenarios involving stronger external actors, Indonesia may face harder choices without formal alliance backing. Even if partners offer political support, uncertainty regarding the timing, scale, and scope of assistance can weaken deterrence in advance of a crisis. This does not mean Indonesia is strategically isolated, but it does imply higher risk exposure. The findings, therefore, show a central paradox: autonomy preserves sovereign freedom of action while simultaneously increasing the material and strategic burden required to make that freedom credible.

3.4. Current Coping Strategy

The evidence suggests that Indonesia manages this dilemma through pragmatic adaptation rather than pure independence. Hedging remains the core mechanism. Jakarta avoids exclusive alignment while engaging multiple powers in overlapping economic, diplomatic, and security relationships. This allows Indonesia to preserve room for manoeuvre while reducing exposure to any single partner ([Iksan and Soong 2023](#)).

A second coping tool is a limited strategic partnership. Indonesia has expanded defence cooperation, exercises, training, and technology dialogues with a range of states without entering treaty alliances. Such arrangements improve capacity while preserving legal autonomy. Military exercises are particularly significant because they enhance interoperability, operational familiarity, and readiness without requiring permanent commitments.

Indonesia has also shown selective openness to minilateral engagement where interests align, especially in maritime awareness, humanitarian assistance, disaster response, and practical security cooperation. Southeast Asian responses to emerging minilateral formats indicate a preference for functional participation over bloc membership ([Allès and Fournol 2025](#)).

At the domestic level, official rhetoric increasingly emphasises defence self-reliance, local production, and industrial upgrading. Although implementation remains uneven, these efforts seek to reduce long-term procurement dependence and strengthen sovereign capability generation.

Overall, the findings indicate that Indonesia sustains strategic autonomy through networked partnerships, diversified cooperation, and gradual capability enhancement. Its posture is therefore not isolationist neutrality, but adaptive non-alignment designed to preserve freedom of choice under competitive regional conditions.

4. Discussion

4.1. Strategic Autonomy vs Strategic Isolation

The findings suggest that Indonesia's commitment to strategic autonomy remains politically rational and strategically understandable in an era of intensified great-power rivalry. Strategic autonomy offers three enduring advantages. First, it preserves sovereign decision-making by reducing external influence over national security choices. Second, it provides diplomatic flexibility, enabling Indonesia to engage multiple partners simultaneously while avoiding binding commitments. Third, it lowers the risk of entrapment in conflicts generated by the strategic priorities of larger powers. For many middle and secondary states, these advantages are especially valuable when rivalry among major powers is fluid and uncertain ([Lee, Yang, and Son 2025](#)).

However, strategic autonomy should not be conflated with strategic detachment. Autonomy refers to the capacity to decide independently; isolation refers to insufficient strategic connectivity with relevant security networks, technological ecosystems, and deterrence frameworks. A state may formally preserve autonomy while becoming materially vulnerable if it lacks partnerships that enhance resilience and strategic awareness. This distinction is increasingly relevant in the Indo-Pacific, where defence relationships are no longer limited to treaty alliances but increasingly include intelligence sharing, logistics access, joint exercises, supply-chain cooperation, and issue-based minilateral mechanisms (Ye 2025).

From a strategic perspective, deterrence credibility is produced not only by sovereign intent but also by visible capability, coherent signalling, and external relationships that shape an adversary's calculations. States that remain overly distant from meaningful security cooperation may retain legal independence while losing practical influence over regional security outcomes. In such circumstances, autonomy risks becoming symbolic rather than operational. New partnership geometries across Asia indicate that states increasingly seek deterrence through layered networks rather than solely through traditional alliances (Wilkins 2026).

For Indonesia, the practical implication is that non-alignment remains viable only if paired with sufficient connectivity to external sources of training, technology, maritime awareness, and crisis coordination. Complete distance from evolving

TABLE 1. Indonesia's Strategic Autonomy: Benefits vs Costs

Dimension	Strategic Benefits	Strategic Costs
Sovereignty	Preserves independent decision-making and avoids external control over defence policy.	Requires Indonesia to bear primary responsibility for its own security without guaranteed support.
Diplomacy	Enables flexible engagement with multiple powers simultaneously.	Ambiguity may reduce clarity of deterrence signalling during crises.
Alliance Risk	Avoids entrapment in conflicts driven by major-power interests.	Lack of formal backing may increase vulnerability to coercive pressure.
Regional Role	Strengthens Indonesia's credibility as an ASEAN-oriented and autonomous actor.	Limited alignment may reduce leverage in emerging security coalitions.
Procurement	Allows diversification of arms suppliers and bargaining flexibility.	Multiple suppliers can create interoperability, maintenance, and logistics problems.
Defence Posture	Supports an independent force-planning model tailored to national priorities.	Modernisation is slower and more expensive without alliance burden-sharing.
Maritime Security	Maintains freedom to calibrate responses in Natuna and surrounding waters.	Persistent maritime presence requires costly ISR, patrol, and rapid-response capacity.
Strategic Identity	Reinforces bebas aktif doctrine and domestic legitimacy.	Strategic identity may constrain adaptation to changing regional realities.

Source: Author's synthesis based on article findings and secondary sources.

security networks could unintentionally increase vulnerability, especially in maritime grey-zone contingencies or supply-chain disruptions. The findings, therefore, indicate that autonomy should be interpreted as selective engagement on Indonesia's own terms, not as deliberate separation from defence cooperation. In this sense, the central challenge is not preserving distance but preserving discretion while remaining strategically connected.

The preceding analysis indicates that Indonesia's strategic autonomy generates both enduring advantages and increasing operational burdens. While autonomy preserves sovereign discretion and diplomatic flexibility, it also requires Indonesia to independently sustain the capabilities necessary to deter coercion and manage regional uncertainty. To clarify these competing effects, Table 1 summarises the main benefits and costs associated with Indonesia's current strategic posture.

As shown in Table 1, strategic autonomy remains valuable politically and diplomatically, but its sustainability increasingly depends on Indonesia's ability to absorb rising defence costs. The central issue is therefore not whether autonomy should be preserved, but whether sufficient capabilities can be developed to support it under conditions of intensifying Indo-Pacific competition. In such an environment, misperceptions regarding Indonesia's deterrent capacity and the reliability of its strategic partnerships may weaken signalling effectiveness and increase the risks associated with non-aligned autonomy.

4.2. Middle Power Theory Perspective

The findings also help reposition Indonesia within contemporary middle power theory. Indonesia behaves neither as a classic balancer seeking explicit countercoalitions, nor as a bandwagoner aligning with the dominant power, nor as a treaty ally subordinating strategy to external guarantees. Instead, Indonesia is more accurately understood as a selective autonomous middle power.

Middle powers typically seek influence through diplomacy, institution-building, coalition management, and norm entrepreneurship rather than raw military dominance. In the Indo-Pacific context, they also attempt to preserve strategic space between competing major powers ([Shin, Alden, and Higgott 2026](#)). Indonesia's behaviour fits this pattern. It seeks agenda-shaping influence through ASEAN-led frameworks, diplomatic brokerage through inclusive regional dialogues, and strategic flexibility through diversified external relations. This reflects a broader model of middle power diplomacy that operates beyond simplistic balancing logic ([Xiao 2025](#)).

Indonesia's strategic assets reinforce this role. Geography gives it control over critical sea lanes and maritime chokepoints linking the Indian and Pacific Oceans. Diplomatic status as Southeast Asia's largest state provides convening authority. Its historical leadership within ASEAN offers institutional leverage, even if ASEAN

cohesion remains uneven. These attributes allow Indonesia to exercise influence disproportionate to formal alliance commitments.

At the same time, selective autonomy does not imply passivity. The findings indicate that Indonesia accepts limited security alignment in specific issue areas, such as maritime cooperation, exercises, defence industry engagement, and humanitarian coordination, while rejecting formal dependence. This behaviour is consistent with strategic choice models in which states calibrate commitment levels according to risk, domestic legitimacy, and uncertainty (Jones and Jenne 2022).

Thus, Indonesia should be understood not as indecisive, but as pursuing a middle-power strategy centred on controlled flexibility. Its challenge is sustaining this model as rivalry intensifies and the costs of ambiguity rise.

4.3. The Defence Dilemma

The core implication of the findings is that refusing alliances preserves sovereignty but increases capability burden. This constitutes Indonesia's principal defence dilemma and can be conceptualised through two linked dynamics: the autonomy-capability paradox and the sovereignty-security trade-off. Unlike the classical security dilemma, which emerges from reciprocal threat perceptions among states and the unintended escalation of insecurity, the defence dilemma identified in this study is primarily a capability-generation dilemma. It concerns the tension between preserving strategic autonomy and acquiring the military, technological, and institutional capabilities necessary to sustain that autonomy. The dilemma, therefore, originates not from how other states interpret Indonesia's actions, but from the growing burden of maintaining credible defence capacity without alliance-based security guarantees.

The autonomy-capability paradox arises because the more a state avoids formal alliances, the more it must independently generate the capabilities that alliances often help provide. These include deterrent force structure, readiness, intelligence-surveillance-reconnaissance systems, maritime presence, logistics resilience, cyber protection, and defence-industrial depth. Alliances can distribute some of these burdens through burden-sharing, interoperability, or guaranteed support. Without such mechanisms, the state must finance and sustain them domestically. Strategic autonomy, therefore, requires substantial material investment if it remains credible (Chung 2026).

For Indonesia, geography intensifies this burden. An archipelagic state with dispersed maritime approaches requires a persistent naval and air presence across wide operational spaces. Sovereignty defence is not merely a legal matter but a logistical one. Maintaining surveillance and response capacity in distant waters is inherently costly. If resources lag behind operational requirements, autonomy may endure politically while weakening operationally.

The second dynamic is the sovereignty-security trade-off. Maximising freedom from external commitments may reduce access to certain benefits commonly associated with deeper partnerships: advanced technology transfer, integrated training systems, interoperability gains, intelligence depth, and predictable crisis support. Even non-treaty partners may be less willing to commit resources where institutional expectations remain vague. This does not imply that alliances are cost-free, but it highlights that sovereignty can carry opportunity costs in security terms (Liow 2024).

The findings, therefore, suggest that Indonesia's challenge is not ideological non-alignment itself. Rather, it is the harder task of converting autonomy into credible power. A state can proclaim independence, yet if its deterrent posture is insufficient, external actors may discount its strategic preferences. Conversely, modest but well-designed partnerships can strengthen autonomy by reducing vulnerabilities. In practice, the relevant question is not whether Indonesia should choose sovereignty or security, but how to secure sovereignty through capability and selective cooperation.

The strategic logic identified in this study can be illustrated as a cumulative dilemma. Indonesia's desire to preserve autonomy encourages continued resistance to formal alliances. However, the absence of alliance-based burden sharing increases the demand for national self-reliance, which in turn risks widening capability gaps if defence modernisation does not keep pace with regional pressures. As these constraints deepen, the need for selective external partnerships becomes more pronounced. This relationship is summarised in Figure 1.

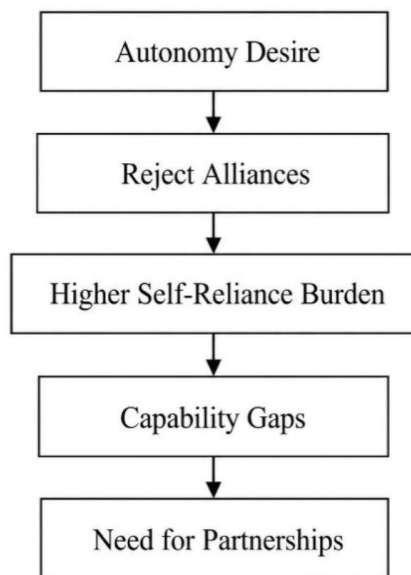


Figura 1 Indonesia's Defence Dilemma Model
 Source: Author's conceptual model based on findings of this study.

As seen in Figure 1, Indonesia's strategic dilemma is cyclical rather than binary. Efforts to maximise independence can unintentionally generate new dependencies when domestic capabilities remain insufficient. This suggests that strategic autonomy

should be understood not as separation from cooperation, but as the ability to manage external partnerships without surrendering decision-making authority. In practical terms, selective cooperation may therefore strengthen, rather than weaken, Indonesian autonomy.

4.4. Policy Options for Indonesia

Three broad strategic pathways emerge from the findings. The first is pure autonomy. Under this model, Indonesia would minimise external defence dependence, avoid deeper security networking, and prioritise national self-reliance. The benefits are clear: sovereignty is maximised, entrapment risk remains low, and policy discretion is fully preserved. Yet the costs are equally high. Force development becomes more expensive, deterrence accumulates more slowly, and crisis management burdens fall almost entirely on national institutions. In a rapidly changing Indo-Pacific, pure autonomy may be politically attractive but materially demanding.

The second pathway is flexible strategic partnerships. This model preserves non-alignment while expanding practical cooperation with multiple states. Benefits include access to training, maritime domain awareness, intelligence exchanges, defence technology collaboration, logistics familiarity, and regular exercises. Indonesia would retain freedom to choose partners issue by issue rather than through treaty obligation. The principal challenge is diplomatic management. Partnerships with one side may be interpreted by others as alignment, while ambiguity during crises may limit expectations of assistance. Even so, this pathway aligns closely with emerging regional patterns of alliance alternatives and functional security networking ([Chaudhry, Aqib, and Wassan 2025](#)).

The third pathway is a quasi-alliance network involving more structured and politically visible security cooperation with a smaller number of key partners. This could accelerate capability gains, improve deterrence signalling, and generate stronger external support in crises. However, it would likely face domestic political resistance, perceptions of abandoning *bebas aktif*, and possible retaliation or counter-pressure from competing powers. It may also narrow Indonesia's room for manoeuvre in diplomacy.

A more plausible pathway would be calibrated partnerships without treaty alliances. This approach accepts that Indonesia does not need to choose between isolation and alignment. Instead, it can preserve autonomy while deepening selective cooperation where interests are clear and sovereignty costs are manageable. Priority areas should include maritime domain awareness, coastal surveillance integration, defence technology partnerships, joint exercises, professional military education, secure communications, and supply-chain resilience. Issue-based multilateral arrangements focused on humanitarian assistance, disaster response, maritime safety, or non-traditional threats could also provide functional gains without symbolic alliance baggage ([Vinodan and Kurian 2024](#)).

From a policy standpoint, Indonesia should also strengthen domestic absorptive capacity so that external cooperation translates into sustainable national capability. Procurement reform, maintenance ecosystems, reserve logistics, and indigenous industry partnerships are as important as diplomacy. Strategic autonomy in the twenty-first century is less about standing alone than about retaining sovereign choice within networks of cooperation.

Accordingly, the most realistic recommendation is neither pure independence nor formal alliance entry, but adaptive non-alignment supported by credible capabilities and carefully structured partnerships. This would allow Indonesia to remain autonomous in decision-making while reducing the risks of strategic isolation.

The findings further suggest that Indonesia's future strategic posture is best understood as a choice among several policy pathways rather than a binary decision between alignment and neutrality. Each option offers distinct gains and constraints in terms of sovereignty, deterrence, domestic legitimacy, and strategic flexibility. Table 2 compares the principal alternatives available to Indonesia.

TABLE 2. Policy Options for Indonesia in Indo-Pacific Rivalry

Policy Option	Main Features	Advantages	Risks / Limitations	Overall Assessment
Pure Autonomy	Minimal security dependence, no formal alliances, emphasis on self-reliance.	Full sovereignty, low entrapment risk, maximum policy discretion.	Expensive force development, slower deterrence accumulation, high crisis burden.	Politically attractive but materially demanding.
Flexible Strategic Partnerships	Non-allied posture with selective defence cooperation, exercises, technology partnerships, intelligence exchanges.	Retains autonomy while improving readiness, maritime awareness, and capability access.	Requires careful balancing; support in crisis may remain uncertain.	Most realistic and sustainable option.
Quasi-Alliance Network	Structured long-term cooperation with key partners short of treaty alliance.	Stronger deterrence, faster interoperability, greater crisis supports potential.	Domestic backlash, perceived abandonment of <i>bebas aktif</i> , possible retaliation from rivals.	Effective but politically sensitive.
Formal Alliance	Treaty-based defence commitment with major power(s).	Highest deterrence credibility and security guarantee.	Loss of flexibility, entrapment risk, domestic legitimacy concerns.	Unlikely under the current Indonesian strategic culture.

Source: Author's comparative framework derived from discussion findings.

As seen in Table 2, the most plausible pathway for Indonesia is neither pure autonomy nor formal alliance entry, but calibrated strategic partnerships that preserve sovereign discretion while reducing capability shortfalls. Such an approach is consistent with Indonesia's historical doctrine, yet more responsive to contemporary requirements for deterrence, technology access, and maritime resilience.

Conclusions

This study has examined a central strategic puzzle: why Indonesia continues to pursue strategic autonomy while refusing formal alliances in an increasingly competitive Indo-Pacific environment. The analysis suggests that this posture is neither accidental nor merely rhetorical. Indonesia's alliance avoidance is deeply rooted in the doctrine of *bebas aktif*, a post-colonial sensitivity toward sovereignty, a long-standing preference for independent decision-making, and a diplomatic tradition that favours inclusive regional multilateralism through ASEAN. These foundations have given Indonesia a durable strategic identity that remains influential across successive administrations and changing external conditions.

The findings indicate that this approach still carries significant political and strategic value. By avoiding treaty commitments, Indonesia preserves domestic legitimacy and reduces concerns that national policy is being shaped by external powers. It also retains diplomatic flexibility, allowing engagement with multiple actors across security, economic, and technological domains without being drawn automatically into major-power rivalry. In practical terms, non-alignment lowers entrapment risk and supports Indonesia's aspiration to act as an autonomous regional actor rather than an adjunct to another state's strategy.

Yet the article has also shown that the regional environment is changing in ways that increase the costs of autonomy without alliances. Intensifying rivalry among major powers has elevated the importance of deterrence credibility, maritime domain awareness, rapid strategic decision-making, secure access to defence technologies, and resilience during coercive crises. In such an environment, autonomy cannot be sustained by diplomatic positioning alone. States that seek policy independence must also demonstrate the material capacity to protect that independence. Where capabilities lag behind strategic ambition, autonomy risks becoming increasingly difficult to defend in practice.

From a policy perspective, this means that strategic autonomy in the current era requires more than doctrinal consistency. It must be underpinned by defence readiness, credible maritime enforcement capacity, coherent procurement planning, reliable intelligence and surveillance systems, and resilient defence institutions capable of sustained adaptation. For Indonesia, the challenge is not whether to preserve *bebas aktif*, but how to modernise its practical meaning under

contemporary conditions. Sovereignty today is exercised not only through freedom from commitments, but through the ability to act effectively when pressure emerges.

The study further suggests that non-allied states still require meaningful external cooperation. Refusing alliances does not eliminate the need for networked partnerships, defence industrial collaboration, selective military exercises, minilateral coordination, and diversified strategic relationships. Carefully structured cooperation can strengthen autonomy by reducing technological dependence, improving readiness, and widening strategic options. In this sense, partnership and autonomy should not be viewed as opposites. Properly managed, they can be mutually reinforced. More broadly, the Indonesian case offers lessons for other middle powers navigating great-power rivalry. Strategic space can still be preserved, but it increasingly depends on combining diplomatic flexibility with credible capabilities and selective connectivity. The most sustainable path lies neither in rigid neutrality nor in automatic alignment but in adaptive statecraft that balances independence with practical cooperation.

Although the Indonesian case is embedded in the specific geopolitical dynamics of the Indo-Pacific, the broader implications extend beyond Southeast Asia. The findings suggest that states seeking to preserve strategic autonomy face a common challenge: balancing sovereign decision-making with the capability requirements needed to sustain credible defence and deterrence. While the institutional and geopolitical contexts of European middle and small powers differ considerably from Indonesia's, similar questions regarding dependence, strategic flexibility, capability development, and selective security cooperation have become increasingly relevant in a period of heightened geopolitical uncertainty. The concept of a defence dilemma developed in this study may therefore provide a useful analytical lens for examining how states manage the tension between policy independence and capability dependence, even under different regional and alliance arrangements. In this sense, the article contributes not only to understanding Indonesia's strategic choices but also to broader debates on strategic autonomy among middle and small powers.

In strategic terms, Indonesia's preference for autonomy remains understandable and potentially sustainable, but only if matched by continuous capability development to address maritime coercion, grey-zone challenges, and broader deterrence requirements in the Indo-Pacific, together with realistic external engagement. The future of Indonesian autonomy may depend less on rejecting alliances and more on redefining autonomy within networks of interdependence involving defence partners, technology providers, and regional security institutions.

References

- Allès, Delphine, and Thomas Fournol.** 2025. "Multilateral Foundations and Minilateral Developments: Navigating Institutional Evolution and Cooperative Saturation in the Indo-Pacific." In *Order and Agency in the Indo-Pacific*, edited by Delphine Allès, Christophe Jaffrelot, and Patrick Köllner, 45-70. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-89802-0_3.
- Anwar, Dewi.** 2020. "Indonesia and the ASEAN Outlook on the Indo-Pacific." *International Affairs* 96: 111-129. <https://doi.org/10.1093/ia/iiz223>.
- Arif, M.** 2025. "Strategic Culture and Indonesian Approach to Maritime 'Rules-Based Order.'" <https://doi.org/10.26181/30845066>.
- Bateman, Sam A. M.** 2015. "The Future Maritime Security Environment in Asia: A Risk Assessment Approach." *Contemporary Southeast Asia* 37(1): 49-84. <http://www.jstor.org/stable/24916514>.
- Chauhdry, K. T., S. Aqib, and I. A. Wassan.** 2025. "Geopolitics of the Indo-Pacific: Strategic Competition, Alliances, and Regional Security." *Research Journal for Social Affairs* 3(5): 503-520. <https://doi.org/10.71317/RJSA.003.05.0345>.
- Chung, K.** 2026. "Evolving Concept of Strategic Autonomy in Europe and Asia: The Role of US Restraint and Simultaneity of Conflicts." *Asia Europe Journal* 24(1): 27-40. <https://doi.org/10.1007/s10308-025-00736-1>.
- Cooper, Zack, and Eric Y. Carr.** 2023. "US Perspectives on the Power Shift in the Indo-Pacific." *The Pacific Review* 36(2): 284-304. <https://doi.org/10.1080/09512748.2022.2160793>.
- de Medeiros, Carlos A., and Numa Mazat.** 2019. "Geopolitics, Geoeconomics, and Development Strategies in the New Millennium." In *Development in Latin America: Critical Discussions from the Periphery*, edited by Victor Ramiro Fernández and Gabriel Brondino, 89-122. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-92183-9_5.
- Febrica, Senia.** 2023. *Indonesia and the Indo-Pacific*. London: Routledge.
- Gerstl, Alfred.** 2022. *Hedging Strategies in Southeast Asia: ASEAN, Malaysia, the Philippines, and Vietnam and Their Relations with China*. London: Routledge.
- Gindarsah, Iis, and Adhi Priamarizki.** 2021. "Explaining Indonesia's Under-balancing: The Case of the Modernisation of the Air Force and the Navy." *Journal of Asian Security and International Affairs* 8(3): 391-412. <https://doi.org/10.1177/23477970211039645>.
- Goh, Evelyn.** 2022. "The Asia-Pacific's 'Age of Uncertainty': Great Power Competition, Globalisation and the Economic-Security Nexus." In *From Asia-Pacific to Indo-Pacific: Diplomacy in a Contested Region*, edited by Robert G. Patman, Patrick Köllner, and Balazs Kiglics, 29-52. Singapore: Springer. https://doi.org/10.1007/978-981-16-7007-7_2.
- Iksan, M., and Jenn-Jaw Soong.** 2023. "The Political Economy of Indonesia's Development Strategy under China-USA Power Rivalry and Hegemonic Competition: A Middle Power with Its Hedging Strategy." *The Chinese Economy* 56(4): 304-320. <https://doi.org/10.1080/10971475.2022.2136696>.

- Jones, David M., and Nicole Jenne.** 2022. "Hedging and Grand Strategy in Southeast Asian Foreign Policy." *International Relations of the Asia-Pacific* 22(2): 205-235. <https://doi.org/10.1093/irap/lcab003>.
- Joseph, B. S.** 2025. "Redefining Asian Security: China, the Indo-Pacific, and the Contest for Regional Order." *China Quarterly of International Strategic Studies* 11(3): 345-366. <https://doi.org/10.1142/S2377740025500150>.
- Karim, M. F.** 2026. "Layered Incoherence in Middle Power Foreign Policy: Indonesia and the U.S.-China Rivalry." *Global Policy* 17(S1): S55-S64. <https://doi.org/10.1111/1758-5899.70093>.
- Khoo, Nicholas.** 2022. "Great Power Rivalry and Southeast Asian Agency: Southeast Asia in an Era of US-China Strategic Competition." *Political Science* 74(2-3): 141-154. <https://doi.org/10.1080/00323187.2023.2186251>.
- Koga, Kei.** 2025. "Tactical Hedging as Coalition-Building Signal: The Evolution of Quad and AUKUS in the Indo-Pacific." *The British Journal of Politics and International Relations* 27(1): 109-134. <https://doi.org/10.1177/13691481241227840>.
- Kuik, Cheng-Chwee.** 2023. "Shades of Grey: Riskification and Hedging in the Indo-Pacific." *The Pacific Review* 36(6): 1181-1214. <https://doi.org/10.1080/09512748.2022.2110608>.
- Le Dinh, Tuan.** 2021. "Where Great Powers Meet: America and China in Southeast Asia. By David Shambaugh." *Asian Politics & Policy* 13(4): 626-628. <https://doi.org/10.1111/aspp.12607>.
- Lee, K. S., H. Yang, and D. Son.** 2025. "US Allies' Foreign Policy Alignment in an Era of Great Power Competition: An Analysis of Domestic Politics." *Contemporary Security Policy* 46(4): 948-976. <https://doi.org/10.1080/13523260.2025.2474872>.
- Liow, Joseph Chinyong.** 2024. *Navigating Uncertainty: Our Region in an Age of Flux*. Singapore: World Scientific.
- Maulana Prasetya, Dion, Suyatno Ladiqi, and Mohd Affandi Salleh.** 2025. "Back to the Past: The Roots of Indonesian Middlepowermanship." *Asian Journal of Comparative Politics* 10(2): 97-112. <https://doi.org/10.1177/20578911241236518>.
- Mietzner, Marcus.** 2025. "Flirting with Autocracy in Indonesia: Jokowi's Majoritarianism and Its Democratic Legacy." *Journal of Current Southeast Asian Affairs* 44(3): 366-384. <https://doi.org/10.1177/18681034251318053>.
- Paribatra, M. L. P.** 2025. "The 'Indo-Pacific' Order: A Southeast Asian Perspective." *Asian Politics & Policy* 17(3): e70031. <https://doi.org/10.1111/aspp.70031>.
- Putra, B. A.** 2026. "Neutrality in Regional Organizations: The Case of Laos' Chairmanships in the Association of Southeast Asian Nations." *Asian Journal of Political Science*, 1-20. <https://doi.org/10.1080/02185377.2026.2636495>.
- Putra, Bama Andika, Abdul Razaq Cangara, and Darwis.** 2024. "Middle Power Norm Entrepreneur: Indonesia's Advocacy of the ASEAN Indo-Pacific Outlook." *SAGE Open* 14(4): 21582440241302148. <https://doi.org/10.1177/21582440241302149>.
- Rüland, Jürgen.** 2024. "ASEAN, Russia's Invasion of Ukraine and the Politics of Pragmatism." *International Affairs* 100(1): 385-406. <https://doi.org/10.1093/ia/iia286>.

- Scott, David.** 2019. "Indonesia Grapples with the Indo-Pacific: Outreach, Strategic Discourse, and Diplomacy." *Journal of Current Southeast Asian Affairs* 38(2): 194-217. <https://doi.org/10.1177/1868103419860669>.
- Shin, Seong-Ouk, Chris Alden, and Richard Higgott.** 2026. "Re-Imagining Middle Powers in an Age of Global Transformation." *Global Policy* 17(S1): S5-S13. <https://doi.org/10.1111/1758-5899.70126>.
- Stromseth, Jonathan R.** 2021. *Rivalry and Response: Assessing Great Power Dynamics in Southeast Asia*. New York: Bloomsbury Publishing.
- Subagyo, Agus, Yohanes Sulaiman, Muhammad Fauzan Alamari, and Mariane Delanova.** 2024. "A Traumatic Relationship: The United States and Indonesia-Russian Relationship." *Journal of Asian Security and International Affairs* 11(2): 214-232. <https://doi.org/10.1177/23477970241250097>.
- Sullivan de Estrada, Kate.** 2023. "India and Order Transition in the Indo-Pacific: Resisting the Quad as a 'Security Community.'" *The Pacific Review* 36(2): 378-405. <https://doi.org/10.1080/09512748.2022.2160792>.
- Vinodan, C., and Anju Lis Kurian.** 2024. "Strategic Autonomy and India's Hedging Policies in the Indo-Pacific." *Journal of Asian Security and International Affairs* 11(4): 475-495. <https://doi.org/10.1177/23477970241282095>.
- Wilkins, Thomas.** 2026. "A Paradigmatic Study of Strategic Partnerships in International Relations: Concepts, Debates and Theorizations." *Contemporary Security Policy* 47(2): 680-713. <https://doi.org/10.1080/13523260.2026.2622863>.
- Wilson, Jeffrey D.** 2018. "Rescaling to the Indo-Pacific: From Economic to Security-Driven Regionalism in Asia." *East Asia* 35(2): 177-196. <https://doi.org/10.1007/s12140-018-9285-6>.
- Wirth, Christian, and Nicole Jenne.** 2022. "Filling the Void: The Asia-Pacific Problem of Order and Emerging Indo-Pacific Regional Multilateralism." *Contemporary Security Policy* 43(2): 213-242. <https://doi.org/10.1080/13523260.2022.2036506>.
- Xiao, Y.** 2025. "Emerging Middle Powers' Balancing Diplomacy: Connotations, Motivations, and Implications." <https://orcid.org/0009-0004-8795-8322>.
- Ye, Xiaoqin.** 2025. "Hybrid Minilateralism: Explaining the Logic of the United States' Containment of China in Indo-Pacific." *The Pacific Review* 38(6): 990-1019. <https://doi.org/10.1080/09512748.2025.2467670>.

ACKNOWLEDGEMENTS

The author gratefully acknowledges the constructive insights provided by colleagues and peer reviewers whose comments helped improve the clarity and analytical direction of this article. Appreciation is also extended to the institutions and open-access data providers whose publications, strategic reports, and policy documents made this study possible. Any remaining errors or interpretations are solely the responsibility of the author.

FUNDING INFORMATION

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. The study was conducted independently by the author.

CONFLICT OF INTEREST STATEMENT

The author declares no conflict of interest regarding the research, authorship, and publication of this article. No financial, institutional, or personal relationships influenced the preparation or conclusions of this study.

DATA AVAILABILITY STATEMENT

The data supporting the findings of this study are derived exclusively from publicly available secondary sources, including official government documents, strategic reports, international databases, and published academic literature. All sources used in the analysis are cited in the reference list and can be accessed through their respective publishers or institutional repositories.

DECLARATION on AI use

Artificial intelligence tools were used solely to assist with language refinement, grammar checking, formatting, and editorial organisation during manuscript preparation. All substantive arguments, analytical interpretations, source selection, and final content decisions were undertaken by the author. The author accepts full responsibility for the accuracy, originality, and integrity of the article.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

<https://buletinul.unap.ro/index.php/en/>

The Tripartite of Food Security, Diplomacy and National Security in West Africa

Latifat Kehinde OLATINWO*
Jesuwaye Israel OLUSANMI-DARE***
Mohammed ABUBAKAR*****

Olooto Felicia MOTUNRAYO**
Isiaka Seriki ADAMU****
Emmanuel Oyewole LAMBE*****

*Department of Agricultural Economics and Extension Services, Kwara State University, Malete
e-mail: latifat.olatinwo@kwasu.edu.ng

**Department of Agricultural Economics and Extension Services, Kwara State University, Malete
e-mail: felicia.olotoo@kwasu.edu.ng

***Sociology Department, Faculty of Social Sciences, Fuoye
e-mail: Olusanmidare@gmail.com

****Department Of Public Administration, Kwara State Polytechnic, Ilorin
e-mail: adamsseriki50@gmail.com

*****Department of Public Administration, Kwara State Polytechnic Ilorin
e-mail: abbati1985@gmail.com

*****Politics and Governance, Kwara State University, Malete, Nigeria
e-mail: Emmanuel.lambe60@gmail.com

Abstract

Food insecurity remains a critical dimension of insecurity in West Africa, exacerbated by post-pandemic disruptions and the global effects of the Russia-Ukraine war. As one of the most climate-sensitive regions globally, the sub-region faces complex interactions between environmental stress, political instability, and economic vulnerability. This study examines the dynamics of food security-driven economic diplomacy in West Africa between 2015 and 2024, focusing on the roles of the Economic Community of West African States, the African Union, the European Union, China, and other multilateral institutions. Anchored in Regime Theory and adopting a mixed-methods approach, the study draws on data from 400 respondents across local communities, policymakers, and institutional actors, analysed using descriptive statistics and thematic techniques. The findings indicate that while regional initiatives such as food reserves and resilience programmes have improved short-term food availability and strengthened cooperative frameworks, their long-term impact remains limited by structural constraints, including weak governance, insecurity, and dependence on food imports. The study further reveals that food security diplomacy operates more effectively as a crisis management tool than as a mechanism for sustainable transformation. It concludes that although institutional cooperation in West Africa has expanded, significant gaps persist in translating diplomatic engagements into durable food security outcomes. The study underscores the need for stronger institutional coordination, context-specific interventions, and enhanced regional integration to achieve sustainable food security and stability.

Keywords: Food; Security; Stability; International Relations.

Article info

Received: 16 November 2025; Revised: 6 January 2026; Accepted: 8 May 2026; Available online: 30 June 2026

Citation: Olatinwo, L.K., O.F. Motunrayo, J.I. Olusanmi-Dare, I.S. Adamu; M. Abubakar, and E.O. Lambe. 2026. "The Tripartite of Food Security, Diplomacy and National Security in West Africa." *Bulletin of "Carol I" National Defence University*, 15(2): 91-110. <https://doi.org/10.53477/2284-9378-26-20>



© „Carol I” National Defence University Publishing House

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC-SA) 91

Introduction

Over the past decade, food security has re-emerged as a central axis in global development and diplomacy, driven by an unsettling recurrence of natural and environmental events and convergence of crises. The COVID-19 pandemic exposed the fragility of global food supply chains, which disproportionately impacted import-dependent regions ([Laborde, Martin, and Vos 2020](#)). This fragility was further compounded by the Russia-Ukraine war, which disrupted global grain and fertilizer exports, driving up food prices and intensifying hunger in vulnerable economies ([FAO 2022](#); [World Bank 2023](#)). Concurrently, the worsening effects of climate change, ranging from erratic rainfall to desertification, have undermined agricultural productivity, especially in regions that were already facing structural poverty and weak governance systems ([IPCC 2022](#)). These compounded shocks have forced a rethinking of food security not only as a developmental issue, but also as a diplomatic and security imperative ([Lambe 2025](#)).

In Africa, and particularly across the West African sub-region, food insecurity has taken on acute dimensions. Despite abundant arable land and a large youthful population, the region remains heavily reliant on food imports, leaving it vulnerable to price volatility and supply disruptions ([ECOWAS 2021](#)). Moreover, chronic underinvestment in agriculture, outdated production systems, and deepening land-use conflicts, especially between nomadic herders and sedentary farmers, have escalated local grievances and triggered recurrent violence ([Okoli and Atelhe 2020](#); [Nwoko 2023](#)). These crises have been described as not only developmental but also political, undermining state authority and fuelling instability across border regions.

In response, both regional and external actors have mobilized resources and diplomacy to address the worsening food crisis. The Economic Community of West African States (ECOWAS) and the African Union have pursued agricultural transformation strategies, while bilateral and multilateral partners, including China, the European Union, and the World Bank, have increasingly tied aid and investment to food security agendas ([NEPAD 2021](#); [EU External Action 2023](#)). However, despite all these, the effectiveness of these interventions remains contested, raising critical questions about ownership, alignment with local realities, and the geopolitical interests driving food-related economic diplomacy.

Food insecurity has become one of the most destabilizing forces in the contemporary global order, threatening not just livelihoods but also national cohesion, regional peace, and the credibility of development diplomacy. As of 2023, an estimated 735 million people face chronic hunger globally, an increase of over 122 million since 2019, primarily due to the COVID-19 pandemic, the Russia-Ukraine war, and climate-related shocks ([FAO 2023](#)). Nowhere is this convergence of crises more visible than in West Africa, where over 44.5 million people are projected to face acute food insecurity during the 2024 lean season alone, a nearly 70% increase from 2021 figures ([WFP&FAO 2024](#); [Cadre Harmonisé 2024](#)).

Despite its agro-ecological potential, West Africa remains heavily import-dependent for strategic food staples ([Ibrahim and Lambe 2024](#)), with countries like Nigeria, Senegal, and Ghana importing over 40–60% of their wheat and rice needs ([ECOWAS 2022](#)). This dependence exposes the region to global price shocks and external policy shifts, with food inflation reaching 28.4% in Nigeria and over 18% in Ghana by late 2023 ([AfDB 2023](#)). Concurrently, localized crises such as the farmer-herder conflicts, land degradation, and climate variability have disrupted domestic production and displaced millions, particularly in the Sahel belt ([IPCC 2022](#); [Okoli and Atelhe 2020](#)).

While several national and regional responses have emerged, including ECOWAS's Food Security Reserve and bilateral agreements with the EU, China, and Gulf states, insufficient empirical assessment can be noticed regarding the way these diplomatic and economic interventions have impacted actual food security outcomes in the region. Equally, it has been noted that aid conditionalities, infrastructure gaps, and poor policy coordination often dilute the effectiveness of these initiatives, while geopolitical interests continue to shape their design and implementation ([NEPAD 2021](#); [EU External Action 2023](#)).

In effect, West Africa is not just facing a humanitarian food crisis, but a complex developmental and geopolitical dilemma where food security has become both a tool and a terrain of economic diplomacy. So, the research gap that the study seeks to cover refers to how and to what extent these food diplomacy efforts have been able to translate into tangible improvements in food access, affordability, and resilience, especially for the most vulnerable population. Upon this, the study assesses the impact of food security-driven economic diplomacy in West Africa between 2015 and 2024, a period marked by compounding global shocks and intensified regional insecurity.

1. Literature Review

The nexus between food security, diplomacy, and national security in West Africa has attracted increasing scholarly attention, particularly in the context of rising food crises, climate variability, and regional instability. Existing literature converges around three dominant strands: institutional interventions and regional governance, structural drivers of food insecurity, and the security implications of food system vulnerabilities.

First, a significant body of work focuses on regional and international institutional interventions aimed at addressing food insecurity through coordinated policy frameworks and economic diplomacy. Regional organisations such as the Economic Community of West African States and the African Union have implemented initiatives, including the Regional Food Security Reserve and the West Africa Food System Resilience Programme, often in partnership with external multilateral actors such as the European Union, World Bank, and International Monetary Fund. These interventions are designed to stabilise food supply, promote agricultural productivity,

and enhance resilience. However, empirical evidence suggests that the effectiveness of these institutional frameworks remains contested. For instance, Nwozor and Olanrewaju (2020) argue that alignment with regional frameworks such as ECOWAP (the ECOWAS Regional Agricultural Policy) and CAADP (Comprehensive Africa Agriculture Development Programme) has not translated into meaningful food security gains in Nigeria, largely due to governance inefficiencies and weak policy implementation. Similarly, a European Commission (2022) report finds that increased public spending on agriculture in ECOWAS states has not significantly reduced undernourishment, highlighting a persistent gap between policy intent and outcomes.

Second, the literature identifies deep structural drivers of food insecurity that limit the success of diplomatic and institutional efforts. These include historical, political, and economic constraints. Isah (2023) attributes food insecurity in the region to colonial legacies, governance failures, and the commodification of food systems, while Muhammad and Babatunde (2023) emphasise trade barriers, weak regional integration, and infrastructural deficits. Notably, intra-regional food trade remains largely informal, reducing the effectiveness of formal trade policies.

Environmental and conflict-related factors further complicate this landscape. Gold (2024) demonstrates a long-run positive relationship between climate change indicators and food insecurity, underscoring the vulnerability of agricultural systems to environmental shocks. Likewise, Ujunwa, Okoyeuzu, and Kalu (2019) find that armed conflict significantly undermines food security across ECOWAS states, reinforcing the link between instability and food system disruption.

Third, a growing strand of literature situates food security within a broader national and human security framework. Empirical studies show that institutional quality, economic growth, and social protection mechanisms play critical roles in mitigating food insecurity. Osabohien et al. (2022), using a generalized method of moments approach across 15 ECOWAS countries, find that social protection programmes have a statistically significant positive effect on food security, suggesting that redistributive policies can buffer vulnerable populations against shocks. Complementary evidence from recent cross-country analyses indicates that strong institutions enhance food security outcomes, while dependence on natural resource rents and exposure to climate change exacerbate vulnerabilities.

Despite these insights, a critical gap persists in the literature. While existing studies examine food security from economic, environmental, or institutional perspectives, there is limited integration of food security with diplomatic strategy and national security considerations within a unified analytical framework. Most studies treat these dimensions in isolation, thereby underestimating the way how food insecurity can both shape and be shaped by regional diplomacy and security dynamics (Lambe 2025). This study addresses this gap by conceptualising food security not merely as a development issue, but as a strategic nexus linking economic diplomacy and national

security in West Africa. By doing so, it moves beyond fragmented analyses and offers a more integrated understanding of how regional cooperation, external partnerships, and internal governance structures interact to influence food security outcomes.

2. Theoretical Framework: Regime Theory

This study is anchored in Regime Theory as articulated by Robert O. Keohane, particularly in his seminal work *After Hegemony* (1984). Regime Theory provides a framework for understanding how cooperation is sustained in an anarchic international system through institutionalised arrangements among states and non-state actors.

At its core, Regime Theory conceptualises international regimes as sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given issue-area (Keohane 1984). These regimes reduce uncertainty, mitigate transaction costs, and address collective action problems, thereby enabling cooperation even in the absence of a central authority. Crucially, the theory departs from purely realist assumptions by demonstrating that cooperation is possible among actors with asymmetric power and divergent interests, provided institutional frameworks structure their interactions.

In the context of West Africa, food security governance increasingly reflects the characteristics of an emerging regional and transnational regime. Institutions such as the Economic Community of West African States and the African Union, alongside global actors like the World Bank, International Monetary Fund, and the European Union, collectively contribute to a structured system of norms and practices governing food security interventions. Programmes such as the Food System Resilience Programme and regional food reserves are not isolated initiatives; rather, they represent institutionalised responses embedded within a broader cooperative framework.

Regime Theory is particularly relevant in explaining how economic diplomacy operates within this institutional architecture. Financial assistance, technical cooperation, and policy harmonisation initiatives reflect negotiated outcomes within a regime where actors pursue both national interests and shared goals. For instance, external actors such as China engage in bilateral agricultural cooperation, while multilateral institutions provide funding conditionalities and policy guidance. Despite disparities in economic and political power, these interactions are sustained through agreed norms and mutual expectations, illustrating the regime logic of cooperation under asymmetry.

More importantly, the theory provides analytical leverage for understanding the link between food security and national security. Within a regime framework, persistent food insecurity signals not merely policy failure but institutional weakness within the regime itself. When rules are weakly enforced, coordination fails, or compliance is low, the result is systemic vulnerability, which can escalate into social unrest, conflict, and broader security threats. Thus, food insecurity becomes both an

outcome of regime inefficiency and a trigger for instability, reinforcing the need for effective institutional coordination.

However, Regime Theory also implies that the mere existence of institutions does not guarantee effectiveness. The performance of a regime depends on compliance, enforcement mechanisms, and the alignment of member state interests. In West Africa, variations in governance quality, political commitment, and resource capacity undermine the effectiveness of existing food security regimes. This explains why, despite the proliferation of initiatives and external support, food insecurity persists across the region.

Accordingly, this study employs Regime Theory not simply as a descriptive framework, but as an analytical tool to interrogate the effectiveness of institutional cooperation in addressing food security and its implications for national security in West Africa. It enables an integrated assessment of how regional and international actors interact, the extent to which institutional arrangements shape outcomes, and why gaps persist between policy design and real-world impact.

3. Methodology

This study adopts a mixed-methods research design, integrating quantitative and qualitative approaches to provide a comprehensive analysis of the nexus between food security, diplomacy, and national security in West Africa. The use of mixed methods is justified by the need to combine statistical generalisation with contextual depth, a strategy widely endorsed in social science research ([Creswell and Plano Clark 2018](#)).

The study focuses on selected countries within the West African sub-region under the institutional framework of the Economic Community of West African States. The geographical scope reflects areas significantly affected by food insecurity and actively engaged in regional and international food security interventions. The temporal scope covers the period 2015 to 2024, aligning with major policy interventions and food security programmes implemented by regional and global actors.

The target population comprises two principal categories:

- **Primary actors:** farmers and local community members directly affected by food security dynamics;
- **Institutional actors:** policymakers, representatives of international organisations, and development stakeholders.

The sample size was determined using the Taro Yamane formula, ensuring statistical representativeness at an acceptable margin of error ([Yamane 1967](#)). Based on this, a total sample size of 400 respondents was derived and proportionally distributed across the identified categories to reflect their relative significance within the study population.

To enhance sampling rigour, a stratified sampling technique was employed. This allowed for the categorisation of respondents into homogeneous groups (farmers,

community members, policymakers, and institutional actors), after which random sampling was applied within each stratum to minimise bias and improve representativeness.

3.1. Data Presentations

Data were collected from both primary and secondary sources. Primary data were obtained through the administration of two structured questionnaires:

- The first targeted farmers and local community members, focusing on lived experiences of food insecurity, access to agricultural support, and perceptions of government and international interventions.
- The second targeted policymakers and institutional stakeholders, capturing perspectives on policy design, implementation challenges, and the role of economic diplomacy in food security governance.

The questionnaires were administered both physically and electronically, depending on respondent accessibility, over a defined period within the 2015–2024 study window. Field administration was supported by trained research assistants to ensure clarity of responses and improve response rates.

Table 1 reveals mixed perceptions among farmers and residents regarding food security and food diplomacy initiatives. Responses were relatively distributed across all Likert scale categories, suggesting the absence of overwhelming consensus on most issues. A considerable proportion of respondents agreed that climate change, insecurity, and farmer-herder conflicts significantly contribute to food insecurity in their communities. However, opinions on the effectiveness of ECOWAS, AU interventions, and food diplomacy efforts remained divided, indicating uncertainty about the practical impact of these regional and international initiatives.

Table 2 indicates that policymakers, donor organizations, civil society actors, and agencies generally perceive structural challenges as major obstacles to food security in West Africa. A large majority strongly agreed that corruption, insecurity, farmer-herder crises, and overdependence on imported food undermine food sovereignty and food security outcomes. However, responses regarding the effectiveness of food security diplomacy in improving food availability and affordability were more divided, reflecting concerns about the limited practical impact of these initiatives. Overall, the findings suggest that while international support and diplomacy are acknowledged, systemic governance and security issues continue to constrain meaningful progress.

3.2. Discussion of the Findings

Theme 1: Regional Disparities in the Impact of Food Security Diplomacy in West Africa

The regression analysis of West African food security diplomacy revealed a considerable regional difference in the impact of such programs. On the one hand, urban areas, in particular, revealed a statistically significant positive impact on food availability due to diplomatic interventions, which aligns with the success of regional

TABLE 1. Survey Response from Farmers and Locals

Item C	Response	Frequency	Percentage (%)	Std. Dev
I am aware of regional/ international food security efforts since 2015.	Strongly Disagree	83	20.75%	1.40
	Disagree	89	22.25%	
	Neutral	76	19.00%	
	Agree	81	20.25%	
	Strongly Agree	71	17.75%	
Climate change has worsened food insecurity in my region.	Strongly Disagree	91	22.75%	1.45
	Disagree	71	17.75%	
	Neutral	78	19.50%	
	Agree	77	19.25%	
	Strongly Agree	83	20.75%	
Food diplomacy has improved domestic food production.	Strongly Disagree	83	20.75%	1.40
	Disagree	80	20.00%	
	Neutral	81	20.25%	
	Agree	85	21.25%	
	Strongly Agree	71	17.75%	
These efforts have improved food affordability in my community.	Strongly Disagree	82	20.50%	1.40
	Disagree	66	16.50%	
	Neutral	88	22.00%	
	Agree	91	22.75%	
	Strongly Agree	73	18.25%	
ECOWAS and AU responses have been timely and effective.	Strongly Disagree	79	19.75%	1.42
	Disagree	74	18.50%	
	Neutral	87	21.75%	
	Agree	75	18.75%	
	Strongly Agree	85	21.25%	
My community has benefited from food aid or agriculture diplomacy.	Strongly Disagree	80	20.00%	1.40
	Disagree	76	19.00%	
	Neutral	83	20.75%	
	Agree	87	21.75%	
	Strongly Agree	74	18.50%	
Food diplomacy prioritizes local food systems.	Strongly Disagree	87	21.75%	1.44
	Disagree	78	19.50%	
	Neutral	76	19.00%	
	Agree	77	19.25%	
	Strongly Agree	82	20.50%	

Source: Researchers survey, 2024-2025.

TABLE 2. Questionnaire Response from policy makers, Donor organizations, Civil Society and Agencies

Question	Strongly Agree (5)	Agree (4)	Neutral (3)	Disagree (2)	Strongly Disagree (1)	Total Responses
Q1. Food security diplomacy efforts have improved food availability in my country.	80	40	12	208	40	400
Q2. These initiatives have improved access to affordable food in my community.	3	76	2	139	80	400
Q3. Foreign assistance has improved access to agricultural technologies and knowledge.	89	36	5	180	70	400
Q4. Corruption and elite capture significantly limit the impact of food security diplomacy.	307	67	1	3	22	400
Q5. Insecurity and farmer-herder crises disrupt food supply chains and production.	280	89	1	10	20	400
Q6. Overreliance on imported food continues to undermine food sovereignty in West Africa.	367	12	0	4	21	400

Source: Researchers survey, 2024-2025.

food assistance programs by organizations such as ECOWAS and the World Food Programme (WFP). These programmes, which were directed at emergency relief, were more easily applied in urban areas where infrastructure, logistical capacity, and local governance structures are better established. On the other hand, the rural areas, especially in Nigeria, Benin, and Mali, bore a significant negative correlation ($B = -0.274$) as far as the success of food security diplomacy initiatives was concerned. Lack of viable distribution channels, coupled with infrastructural deficits and socio-economic vulnerabilities, significantly compromised the coverage and effectiveness of the programs in more rural and remote settlements.

Moreover, qualitative findings from interviews with farmers in these localities corroborate this mismatch. A farmer in Benue, for example, remarked: *“We hear of food aid coming from other countries, but it never reaches us. We are left to struggle with local problems, and nothing changes”*. Similarly, farmers in Plateau were skeptical of the success of regional diplomacy efforts, pointing to the poor road networks and disorganization of local distribution channels as primary reasons for the failure of international aid to reach them (Lambe and Lambe 2026).

On their part, city policymakers in Lagos, Abidjan, and Cotonou valued the benefits of food security diplomacy, particularly during food crises and emergencies. In the words of a Benue policymaker, *“Food security diplomacy has helped a lot in cities facing emergencies, particularly after the floods of 2018. However, we must invest more in rural areas, where farmers are still facing difficulties in terms of access to seeds, fertilizers, and markets.”*

Trend Analysis

This geographical divide in food security diplomacy effectiveness is also present in other literature and event reports. For example, according to Bryceson (2017), food security programs have always enjoyed higher success rates in the urban areas because of improved access to logistical support as well as the robustness of the governance institutions. This puts rural areas even more behind in terms of proper program consideration, mostly through problems of missing infrastructure and accessibility of governance.

Schneider et al. (2018) highlight the issue of donor-driven programs that are prone to neglecting rural concerns in favour of blanket urban-oriented interventions. These interventions have failed to address the specific needs of the smallholder farmers and food systems at the local level, especially where access to markets and storage capacity are not part of the provision of food aid.

One of the most recent ECOWAS programmes, the 2017 ECOWAS Food Reserve Programme, is a good case study. Although the programme with an objective to stabilize West Africa food prices was successful in urban marketplaces, within rural areas, there were some programme implementation challenges in terms of weak road network infrastructure and dominant local systems of government. A 2018 analysis of the initiative quoted that supply chain inefficiencies and local corruption were prime reasons why the scheme had been unable to reach rural communities effectively (ECOWAS 2018). Furthermore, the 2019 ECOWAS Regional Food Reserve Policy reiterates this issue. Even though it was effective in cities, it was highly criticized for failing to integrate cohesive rural development plans, hence exacerbating the gap between the levels of urban and rural food security in the region (Adebayo 2020).

Regional variations in urban-rural food security diplomacy in West Africa are stunning. In Nigeria, the largest country in the region, Northern states such as Kano, Borno, and Yobe still struggle with chronic insecurity, exacerbated by insurgency and banditry, which adversely affect food security initiatives. In contrast, more

Panel Data 1: Comparative Trends in Food Aid, Food Security, and Governance Indicators in Selected West African States (2015–2024)

Country	Year	Food Aid Received (USD million)	Food Security Index (GFSI Score)	Conflict Incidents (ACLED Count)	GDP per Capita (USD)	Cereal-Grain Production (MT)	Governance Score (WGI)
Nigeria	2015	150	38.5	1,200	2,640	25.0 million	-0.85
Nigeria	2016	160	39.0	1,350	2,700	24.5 million	-0.88
Nigeria	2017	170	39.5	1,400	2,750	24.0 million	-0.90
Nigeria	2018	180	40.0	1,450	2,800	23.5 million	-0.92
Nigeria	2019	190	40.5	1,500	2,850	23.0 million	-0.95
Nigeria	2020	200	41.0	1,550	2,900	22.5 million	-0.97
Nigeria	2021	210	41.5	1,600	2,950	22.0 million	-0.98
Nigeria	2022	220	42.0	1,650	3,000	21.5 million	-1.00
Nigeria	2023	230	42.5	1,700	3,050	21.0 million	-1.02
Nigeria	2024	240	43.0	1,750	3,100	20.5 million	-1.05
Ghana	2015	50	45.0	200	1,600	3.0 million	-0.30
Ghana	2016	55	45.5	210	1,650	3.1 million	-0.28
Ghana	2017	60	46.0	220	1,700	3.2 million	-0.26
Ghana	2018	65	46.5	230	1,750	3.3 million	-0.24
Ghana	2019	70	47.0	240	1,800	3.4 million	-0.22
Ghana	2020	75	47.5	250	1,850	3.5 million	-0.20
Ghana	2021	80	48.0	260	1,900	3.6 million	-0.18
Ghana	2022	85	48.5	270	1,950	3.7 million	-0.16
Ghana	2023	90	49.0	280	2,000	3.8 million	-0.14
Ghana	2024	95	49.5	290	2,050	3.9 million	-0.12
Burkina Faso	2015	100	35.0	500	700	2.5 million	-1.20
Burkina Faso	2016	110	35.5	550	720	2.6 million	-1.22
Burkina Faso	2017	120	36.0	600	740	2.7 million	-1.24
Burkina Faso	2018	130	36.5	650	760	2.8 million	-1.26
Burkina Faso	2019	140	37.0	700	780	2.9 million	-1.28
Burkina Faso	2020	150	37.5	750	800	3.0 million	-1.30
Burkina Faso	2021	160	38.0	800	820	3.1 million	-1.32
Burkina Faso	2022	170	38.5	850	840	3.2 million	-1.34
Burkina Faso	2023	180	39.0	900	860	3.3 million	-1.36
Burkina Faso	2024	190	39.5	950	880	3.4 million	-1.38
Senegal	2015	30	50.0	100	1,200	1.5 million	-0.50
Senegal	2016	35	50.5	110	1,250	1.6 million	-0.48
Senegal	2017	40	51.0	120	1,300	1.6 million	

Source: Researchers' compilation across various reports.

peaceful areas in the Southwest and South-south, such as Lagos and Port Harcourt, significantly benefit from regional food diplomacy efforts. This regional divide shows that more context-specific and localized interventions are desperately needed. Similarly, in Mali and Burkina Faso, Bamako and Ouagadougou have a distinct advantage of food diplomacy and foreign aid, particularly in times of crisis. The rural areas of northern Mali that are affected by Islamist insurgencies have no or limited access to these programs, reflecting the challenges of delivering aid in conflict zones. In Benin and Togo, while urban centres like Cotonou benefit from the WFP-led initiatives, rural farmers continue without adequate access to food aid and farming services, and this underscores the need for a more multi-level, integrated approach to food security in both countries.

Theme 2: The Effectiveness of Food Security Diplomacy in Conflict-Prone Regions of West Africa

The study identified a moderate positive correlation between food security diplomacy and a reduction in food-related conflicts. However, this relationship was not uniform across the region. While food diplomacy, defined as the strategic use of food aid and agricultural partnerships to manage conflict and foster cooperation, showed success in reducing tensions in stable or semi-stable areas, it was less impactful in deeply entrenched conflict zones, especially those suffering from herder-farmer violence, banditry, and insurgency.

Qualitative evidence from community-level interviews confirms this disparity. In Kogi, a state frequently affected by low-scale communal violence, a community leader stated: “*We’ve received food aid, but conflicts have continued due to deeper issues like herder-farmer violence.*” Similarly, in Plateau, where the farmer-herder conflict has ethnic and historical undertones, a farmer amongst the interviewees noted: “*Food aid helps, but it cannot solve the ongoing tensions between farmers and herders. The violence is systemic.*”

These responses are in agreement with the quantitative results, which suggest that while food diplomacy may suppress conflict intensity in the short run, it is insufficient where food insecurity is coupled with identity-based grievances, land disputes, and weak governance.

Even among policymakers, there was a nuanced perception, a Benue senior official observed: “*When food was provided in areas of conflict, it would pacify, but it was never a solution.*” This is a sign of a gap between emergency diplomacy and sustainable peacebuilding, especially in areas like the Middle Belt of Nigeria, the Liptako-Gourma region, and Northern Mali, where food insecurity and conflict fuel each other in a cycle of violence.

The West African sub-region has experienced several instances where food diplomacy was put to use to address hunger caused by conflict, primarily by foreign actors such as the WFP, FAO, and ECOWAS. The interventions, however, have varying impacts depending on the nature of the conflict.

A good example is the Lake Chad Basin crisis (2015–2021) that struck northeast Nigeria, Cameroon, Chad, and Niger. The WFP Emergency Operation 200777, launched in 2015, managed to relieve acute hunger among Internal Displaced Persons camps in Borno and Yobe States, but did not halt Boko Haram recruitment, land grabbing, or community displacement. Barrett (2020) states, *“Food aid is effective in keeping people alive, but without governance and security reform, it cannot end conflict”*.

The other example is the 2019 ECOWAS Regional Stabilization Strategy that included a food security component for northern Nigeria and the Sahel. While the project provided over 10,000 metric tons of cereals to conflict-affected regions in Burkina Faso and Niger, it failed to address mobility constraints, food corridor taxation by terrorists, and distrust between the state and local communities.

In Benue and Plateau, two of Nigeria’s agrarian conflict foci, state cooperation with development partners such as USAID’s Feed the Future and GIZ’s Green Innovation Centres attempted to synergize food diplomacy with livelihood support. Nevertheless, the scope of the programmes was narrow, the monitoring systems were weak, and implementation was spasmodic, diluting the scope of these programmes to diffuse structural tensions.

Cochrane (2019) criticizes the overdependence on food aid as a foreign policy tool in areas of conflict, arguing that lone food interventions, not framed in peace-building, justice system reform, or resource management, have a tendency to yield short-term results. He cites the breakdown of the 2019 ECOWAS peace talks in the Lake Chad basin as a manifestation of this. The food element, though well-received, could not supplant a common approach to settling conflicts.

To support this, Hendrix and Brinkman (2013) found that land stress and food price volatility were the key drivers of violence in rural West Africa and that efforts to only address food distribution without addressing land tenure, herding controls, and climate pressures usually failed to end conflict cycles.

Theme 3: Local Needs vs. Global Priorities in Food Security Diplomacy

One of the central findings of this study is the misalignment between international food diplomacy initiatives and the specific needs of local communities. Quantitative analysis revealed a statistically significant negative correlation between local needs and the effectiveness of global food diplomacy efforts, suggesting that diplomatic initiatives often failed to resonate with or address local food security concerns.

This theme was reinforced by the qualitative data, where farmers and community leaders consistently highlighted a disconnect between global priorities and local realities, as a farmer from Plateau stated: *“Food security programs sound good on paper, but they don’t account for our actual struggles. We need local solutions, not just food supplies”*. Similarly, an interviewee noted that *“Foreign donors often prioritize their own agendas over the needs of the people they claim to help”*. This sentiment underscores the frustration of local stakeholders, who feel that external aid often overlooks contextualized agricultural systems and indigenous food practices.

This misalignment has been widely discussed in the literature. Schneider et al. (2018) argue that food diplomacy often reflects donor interests, rather than addressing the specific needs of local populations. A prime example is the 2018 EU food security initiative, which, despite its large-scale aid, was criticized for prioritizing trade liberalization over direct food sovereignty, which is a crucial concern for many West African farmers.

Moreover, Bryceson (2017) discusses how global food diplomacy programs, especially those led by China and the EU, often fail to integrate local agricultural practices into their policy frameworks, thus undermining local resilience. The 2018 African Union Agricultural Transformation Agenda was similarly critiqued for its top-down approach, which disregarded local knowledge and community engagement in favour of broader global agricultural policies.

Theme 4: Institutional Coordination and Transparency in Food Security Diplomacy in West Africa

The study reveals a moderately strong positive correlation between inter-institutional coordination and the success of food security diplomacy, suggesting that when foreign donors, national governments, and local institutions align effectively, food diplomacy efforts are more likely to achieve their stated goals. However, this correlation was highly contingent on the presence of transparency mechanisms and direct beneficiary engagement.

Qualitative data from rural interviewees, such as smallholder farmers and community members, highlighted continued problems of food aid misallocation, elite capture, and intermediaries. As the farmer from Kogi illustrated: *“Aid is often given to middlemen, rather than directly to us. The transparency is not there, and most often it’s wasted or diverted”*. Complaints to the same effect came from parts of Benue and Northern Ghana, where farmers claimed that external food intervention hardly trickles down to the grassroots due to bureaucratic constraints and political screening.

This gap between policy-level coordination and ground-level implementation is a structural flaw in the design and administration of food diplomacy programs across several West African countries. Several focus group respondents in Kebbi and northern Côte d’Ivoire confirmed that local voices are hardly heard, even when aid is intended for them.

Empirical evidence corroborates these worries. The 2018 ECOWAS Food and Nutrition Security Programme sought to domesticate the ECOWAS Regional Agricultural Policy (ECOWAP) but was hampered by donor agencies, regional institutions, and national ministries’ coordination deficits. The Niger and Burkina Faso audits found late distribution, mixed reporting requirements, and exclusion of beneficiary voice. In spite of being financed externally by the EU and IFAD, its implementation was compromised by excessive planning centralization and minimal transparency levels in the fund release (ECOWAS 2019).

The same problems were felt in Nigeria in the 2020 National Food Security Response Plan, which was launched during the COVID-19 pandemic. While the program attracted robust global support, particularly from the World Bank's NG CARES

TABLE 4. Major Food Security Aid Flows and Diplomatic Instruments in West Africa (2015-2024)

Instrument / Initiative	Implementing Body	Timeframe	Financial Commitment	Description
ECOWAS Regional Food Security Reserve (RFSR)	ECOWAS	2017–2024	Not specific	Distributed over 55,000 metric tons of cereals to Sierra Leone. For instance, in 2024, Nigeria received approximately 7,000 metric tons to address acute food insecurity affecting over 31 million people.
Food Systems Resilience Program (FSRP)	World Bank, ECOWAS, CILSS, CORAF	2021–2024	\$645 million	A multi-phase program aimed at increasing agricultural productivity through climate-smart agriculture, promoting intraregional value chains and trade, and building regional capacity to manage agricultural risks.
REWARD-ECOWAS Rice Value Chain Initiative	African Development Bank (AfDB), ECOWAS	2025	\$12 million	Aimed at strengthening regional rice production to ensure food security and reduce dependence on costly rice imports. The project focuses on supporting policy reforms, improving regulation of agricultural inputs, and enhancing regional digital monitoring systems.
EU–ECOWAS Trade and Food Security Agreements	European Union, ECOWAS	2023	€212.5 million	Agreements covering promotion of trade and regional integration, energy interconnectivity, renewable energy, sustainable food systems, and food security.
IMF Emergency Financing for Mali	International Monetary Fund (IMF)	2024	\$120 million	Emergency financing to address rising food insecurity in Mali, covering costs related to food provision, clean water access, sanitation facilities, and shelter for displaced individuals.
AfDB Support for Nigeria's Agriculture	African Development Bank (AfDB)	2022–2025	\$2.2 billion	Mobilizing funds to establish agricultural processing zones in 28 Nigerian states, aiming to enhance food security and generate employment.

Source: Researchers compilation.

initiative, field reports of Benue, Taraba, and Niger States reported that food assistance distribution was informed by local patron networks. This is reminiscent of the report by KII 9, a local CSO actor resident in Plateau, that *“The paperwork is neat at the top, but we don’t see that neatness in delivery”*. It is politics all the way down.

Barrett (2020) warns that food diplomacy is weakened in weak institutional environments where donor-local coordination has unstructured backlinks. His evidence indicates that effectiveness in aid depends less on the volume of assistance and more on aid chain management, especially in weak state institution countries like Guinea-Bissau, Chad, and Northern Nigeria.

Even within donor communities, there have been criticisms. The 2021 WFP Post-Distribution Monitoring Reports for Niger and Mali indicated logistical coordination issues, including unverified recipient lists and the absence of real-time auditing systems, which undermined confidence in both international and domestic food diplomacy systems.

Conclusion and Policy Implications

This study examined the nexus between food security, economic diplomacy, and national security in West Africa within the institutional context of the Economic Community of West African States and broader international partnerships. Drawing on both quantitative and qualitative evidence, the findings indicate that while food security diplomacy has generated measurable interventions, its overall effectiveness remains structurally constrained.

Empirically, the study finds that food security initiatives have produced uneven outcomes across spatial and institutional contexts. Urban and politically visible areas tend to benefit more from emergency food interventions and donor-supported programmes, whereas rural and conflict-affected regions remain persistently vulnerable. This uneven distribution reflects deeper governance and coordination challenges rather than mere resource scarcity. These findings align with existing literature highlighting the implementation gap between policy commitments and actual food security outcomes (Nwozor and Olanrewaju 2020; European Commission 2022).

From a regime-related perspective, the results suggest that West Africa’s food security architecture constitutes an incomplete and weakly institutionalized regime. While multiple actors, including the African Union, World Bank, and International Monetary Fund, contribute to a shared framework of cooperation, the effectiveness of this regime is undermined by low compliance, fragmented implementation, and asymmetries in state capacity. Consequently, food security diplomacy operates more as a coordination mechanism for short-term crisis response than as a transformative system capable of ensuring long-term resilience.

Furthermore, the study establishes a clear linkage between food insecurity and national security vulnerabilities. Persistent food shortages, particularly in fragile regions, interact with conflict dynamics, displacement, and weak institutional presence to produce conditions conducive to instability. In this sense, food insecurity is not only a developmental concern but also a strategic security issue, reinforcing the need for integrated policy approaches.

Comparatively, the analysis reveals that countries with relatively stronger institutional coordination and policy coherence demonstrate better food security outcomes, even when resource constraints are similar. This suggests that governance quality and regime effectiveness are more decisive than the volume of external support received. On the basis of these findings, the study advances the following policy implications. First, there is a need to strengthen institutional coherence within the regional food security regime, particularly by improving coordination between regional bodies and national governments. Second, food security interventions must be more deliberately integrated with conflict-sensitive frameworks, especially in high-risk areas where insecurity directly disrupts agricultural production and distribution systems.

Third, enhancing transparency and accountability in aid delivery mechanisms is critical to restoring trust and improving programme effectiveness. Finally, sustained investment in context-appropriate agricultural modernisation, including accessible mechanisation and climate-resilient practices, is essential for reducing long-term dependency on food imports.

In sum, the study concludes that while food security diplomacy in West Africa has established a foundation for cooperation, its current configuration lacks the institutional depth and coherence required to achieve sustainable outcomes. Addressing these structural limitations is essential not only for improving food security but also for enhancing regional stability and security.

Recommendations

Based on the empirical findings and the analytical insights derived from Regime Theory, this study advances the following recommendations:

First, there is a need to strengthen institutional coordination within the regional food security architecture. Existing frameworks under the Economic Community of West African States and the African Union should be better harmonised with national-level policies to reduce duplication, policy fragmentation, and implementation gaps. Effective regime performance depends not merely on the existence of institutions, but on their coherence and enforcement capacity ([Keohane 1984](#)).

Second, governments and regional bodies should prioritise context-specific, rural-focused interventions. The findings demonstrate a persistent rural-urban disparity in

food security outcomes. Targeted investment in rural infrastructure, storage systems, and market access is essential to ensure that food security initiatives reach the most vulnerable populations rather than remaining concentrated in urban centres.

Third, there is an urgent need to integrate food security strategies with conflict-sensitive and security frameworks. Given the established linkage between food insecurity and instability, interventions must be designed in tandem with peacebuilding and local security mechanisms, particularly in conflict-prone areas. This aligns with evidence that conflict significantly undermines food production and distribution systems (Ujunwa, Okoyeuzu, and Kalu 2019).

Fourth, transparency and accountability in aid and programme implementation must be strengthened. Regional governments and international partners such as the World Bank and the International Monetary Fund should adopt stricter monitoring and evaluation frameworks to ensure that allocated resources translate into measurable outcomes. This includes improving data systems and reducing opacity in fund disbursement.

Fifth, there is a need to promote inclusive and accessible agricultural modernisation. Mechanisation and climate-smart agriculture should be scaled in a manner that is affordable and adaptable to smallholder farmers, who constitute the majority of agricultural producers in West Africa. Evidence suggests that technological adoption, when properly implemented, enhances productivity and resilience (Osabohien et al. 2022; Gold 2024).

Finally, regional actors should deepen intra-regional trade integration in agricultural commodities. Reducing trade barriers, formalising informal trade networks, and improving cross-border logistics will enhance food availability and price stability across the region. This is particularly important given that informal trade currently dominates food exchange in West Africa, limiting policy effectiveness (Isah 2023).

References

- Adebayo, A.A. 2020. "Food security governance and rural development challenges in Nigeria." *African Journal of Agricultural Research and Policy* 15(3): 210-224.
- African Development Bank (AfDB). 2022. "African economic outlook 2022."
- _____. 2023. "Africa macroeconomic performance and outlook 2023".
- Barrett, C.B. 2020. "Food systems and the economics of food security: What we know and what we need to know." *American Journal of Agricultural Economics* 102(3): 1-20. <https://doi.org/10.1111/ajae.12081>.
- Breisinger, C., O. Ecker and J.F. Trinh Tan. 2014. Conflict and food insecurity. *IFPRI Discussion Paper*.
- Bryceson, D.F. 2017. *Food security, urbanization and agrarian transformation in Africa*. In S. Devereux (Ed.), *Food security in Sub-Saharan Africa* (pp. 45-67). Oxford University Press.
- Cadre Harmonisé. 2024. "Food security analysis for West Africa – March 2024 cycle". <https://www.food-security.net>.

- Clapp, J.** (2017). "Food self-sufficiency and international trade." *Global Environmental Politics* 17(1): 1-18.
- Cochrane, L.** 2019. "Aid, food security, and peacebuilding: Rethinking humanitarian food interventions in conflict settings." *Global Food Security* 21: 1-8. <https://doi.org/10.1016/j.gfs.2019.03.004>.
- Creswell, J. W., and V.L. Plano.** 2018. *Designing and conducting mixed methods research* (3rd ed.). Sage.
- ECOWAS.** 2018. "Annual report on agriculture and food security implementation in West Africa." Economic Community of West African States Commission. Abuja: ECOWAS Commission.
- _____. 2021. "ECOWAS agricultural policy (ECOWAP) at 15: Achievements and prospects". Abuja: ECOWAS Commission.
- ECOWAS Commission.** 2019. "ECOWAS regional agricultural policy (ECOWAP) implementation review report." Abuja: ECOWAS.
- European Commission.** 2022. "Safeguarding food security and reinforcing the resilience of food systems. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions (COM(2022) 133 final)". Publications Office of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0133>.
- European Union External Action.** 2023. "EU Global Gateway strategy: Partnerships for sustainable food systems in Africa". European Commission.
- FAO.** 2023. *The state of food security and nutrition in the world*. Food and Agriculture Organization.
- Food and Agriculture Organization (FAO).** 2022. "The state of food security and nutrition in the world 2022". <https://openknowledge.fao.org/server/api/core/bitstreams/67b1e9c7-1a7f-4dc6-a19e-f6472a4ea83a/content>.
- Gold, K.L.** 2024. "Food insecurity in West Africa: Is global warming the driver? *World Agricultural Economy* 5(4): 403-419. <https://doi.org/10.36956/rwae.v5i4.1186>.
- Hendrix, C.S., and H.J. Brinkman.** 2013. "Food insecurity and conflict dynamics: Causal linkages and complex feedbacks." *Stability: International Journal of Security and Development* 2(2): Art. 26. <https://doi.org/10.5334/sta.bm>.
- Ibrahim O. Salawu, and E.O. Lambe.** 2024. "An Impact Assessment of Insecurity on Nigeria's Socio-political Development." *Jigawa Journal of Politics (JJIP)* 4(1).
- Isah, M.B.** 2023. "Food insecurity in West Africa: Governance failures, structural constraints and historical legacies." *African Journal of Food, Agriculture, Nutrition and Development* 23(2): 145-162.
- Intergovernmental Panel on Climate Change (IPCC).** 2022. *Sixth assessment report: Impacts, adaptation and vulnerability*. IPCC.
- Keohane, R.O.** 1984. *After hegemony: Cooperation and discord in the world political economy*. Princeton University Press.
- Krasner, S. D.** 1983. International regimes. *International Organization*, 36(2): 185-205.
- Laborde, D., W. Martin, and R. Vos.** 2020. *Poverty and food insecurity could grow dramatically as COVID-19 spreads*. International Food Policy Research Institute (IFPRI) Blog. <https://www.ifpri.org/blog/poverty-and-food-insecurity-could-grow-dramatically-covid-19-spreads>.
- Lambe, E.O.** 2025. "Hybrid security and the erosion of state monopoly: Vigilantism, informal security and political order in the Lake Chad Basin." *Bulletin of "Carol I" National Defence University* 14(3): 101-123. <https://doi.org/10.53477/2284-9378-25-38>.

- Lambe, E.O., and I.O. Lambe.** 2026. "The impact of insecurity on sustainable development drive in Nigeria's Fourth Republic: An analysis of state-driven peace initiatives." *UNIOFFA Journal of Interdisciplinary Studies (OJIS)*.
- Lambe, E. O., et al.** 2024. "An assessment of the effect of active and passive political behaviour of citizens on governance and development in Nigeria." *Wukari International Studies Journal* 8(8).
- Lipton, M.** 1977. *Why poor people stay poor*. Harvard University Press.
- Muhammad, K.A., and O.O. Babatunde.** 2023. "Food insecurity and structural constraints in Sub-Saharan Africa: Trade barriers and regional integration challenges." *Journal of International Development and Cooperation* 29(3): 201-219.
- NEPAD.** 2021. "Comprehensive Africa Agriculture Development Programme (CAADP) review report". AU-NEPAD Planning and Coordinating Agency.
- Nwoko, K.C.** 2023. "Environmental change and farmer-herder conflicts in Nigeria's Middle Belt". *African Security Review* 32(1): 45-61. <https://doi.org/10.1080/10246029.2023.2166221>.
- Nwozor, A., and J.S. Olanrewaju.** 2020. "The ECOWAS agricultural policy and the quest for food security: Assessing Nigeria's implementation strategies". *Development Studies Research* 7(1): 59-71. <https://doi.org/10.1080/21665095.2020.1785904>.
- Okoli, A.C., and G.A. Atelhe.** 2020. "Nomads against natives: A political ecology of herder-farmer conflicts in Nigeria". *African Journal on Conflict Resolution* 20(1): 23-45. <https://doi.org/10.4314/ajcr.v20i1.2>.
- Okoyeuzu, C.R., and U. Kalu.** 2019. "Conflict, agricultural disruption and food security in ECOWAS states." *African Development Review* 31(4): 512-526.
- Olomola, A.S.** 2015. *Agricultural policy and food security in Nigeria*. IFPRI Working Paper.
- Osabohien, R., A.A. Karakara, J. Ashraf, and M.A.S. Al-Faryan.** 2022. "Green environment-social protection interaction and food security in Africa." *Environmental Management* 71(4): 835-846. <https://doi.org/10.1007/s00267-022-01737-1>.
- Raleigh, C., A. Linke, and J. O'Loughlin.** 2015. "Climate change and conflict risk." *PNAS* 112(45): 14333-14338.
- Schneider, M., C. Béné, T. Evans, and K. Tilker.** 2018. "Policy coherence in food systems and rural development: Donor-driven agendas and local realities." *World Development* 109: 1-14.
- Schneider, M., et al.** 2011. "Donor-driven agricultural policy." *World Development* 39(3): 1-12.
- Ujunwa, A., C.R. Okoyeuzu, and E.U. Kalu.** 2019. "Armed conflict and food security in West Africa: Socioeconomic perspective." *International Journal of Social Economics* 46(2): 182-198. <https://doi.org/10.1108/IJSE-11-2017-0538>.
- United Nations Development Programme (UNDP).** 1994. *Human development report 1994: Human security*.
- World Bank.** 2020. *ECOWAS trade and integration report*.
- _____. 2022. "World Bank scales up its financing for food security to strengthen the resilience of food systems across West Africa". <https://www.worldbank.org/en/news/press-release/2022/07/29/world-bank-scales-up-its-financing-for-food-security-to-strengthen-the-resilience-of-food-systems-across-west-africa>.
- World Food Programme & Food and Agriculture Organization (WFP&FAO).** 2024. "Hunger hotspots: FAO-WFP early warning report on acute food insecurity – March 2024 edition".
- Yamane, T.** 1967. *Statistics: An introductory analysis*. Harper & Row.

Multilateralism and National Development: An Assessment of Nigeria's Roles in the Development of International Organizations (IO) in Africa (1960-2025)

Basheer Olalere USAMOTU, PhD*

Young Kenneth IRHUE***

Musediq Olufemi LAWAL**

Oluwatoyin Adijat OWOLEWA****

*Osun State University, Nigeria

e-mail: amobiolalere@gmail.com, basheer.usamotu@uniosun.edu.ng

 <https://orcid.org/0000-0002-5648-8063>

**Department of Sociology and Criminology, Osun State University, Osogbo, Nigeria

e-mail: flawal2005@gmail.com

 <https://orcid.org/0000-0002-3667-2533>

***Department of Political Science and International Relations,
Osun State University, Osogbo, Nigeria

 <https://orcid.org/0000-0003-4608-1304>

****Osun State University, Nigeria

Abstract

Nigeria's participation in international organizations (IOs) has been a cornerstone of its foreign policy since gaining independence. Despite being a founding member of various IOs, including the African Union (AU) and the Economic Community of West African States (ECOWAS), Nigeria's engagement has not yielded the expected benefits. Based on this backdrop, this research investigates Nigeria's participation in IOs and the role of Nigeria's multilateral foreign policy in the development of Nigeria. Qualitative methods and liberal institutionalism were used to investigate Nigeria's role in IOs in Africa. It has been revealed that despite Nigeria's active participation and contribution to these organizations, they do not benefit as they should. This study has demonstrated that Nigeria played a significant role as a regional leader within African multilateral organizations, particularly the African Union (AU) and Economic Community of West African States (ECOWAS). Nigeria had contributed to regional security and promoted trade and cooperation. The study recommends that Nigeria should be more conscious of its gains while pursuing its multifaceted foreign policy.

Keywords:

Multilateralism; Development; National Development; International Organizations; Africa.

Article info

Received: 24 March 2026; Revised: 2 April 2026; Accepted: 21 May 2026; Available online: 30 June 2026

Citation: Usamotu, B.O., M.O. Lawal, Y.K. Irhue, and O.A. Owolewa. 2026. "Multilateralism and National Development: An Assessment of Nigeria's Roles in the Development of International Organizations (IO) in Africa (1960-2025)." *Bulletin of "Carol I" National Defence University*, 15(2): 111-128. <https://doi.org/10.53477/2284-9378-26-21>

Bulletin of "Carol I" National Defence University, 15(2): 111-128. <https://doi.org/10.53477/2284-9378-26-21>



© „Carol I” National Defence University Publishing House

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC-SA) 111

Introduction

Nigeria, a country that is rich in diversity, culture, and resources, plays a significant role on the global stage, especially in Africa, through its multilateral foreign policy. Multilateralism is the practice of engaging multiple countries in collaborative efforts to address shared challenges and promote mutual interests, particularly in the areas of security, trade, and development ([Ayoob 1991](#)). Like other countries on other continents, multilateralism has become increasingly important for African nations to achieve their foreign policy objectives. Nigeria and many African countries are part of regional organizations like the African Union (AU) and Economic Community of West African States (ECOWAS), which promote cooperation and collective decision-making on political, economic, and social issues ([Anyaku 2012](#)). Scholars have argued that these multilateral efforts have helped to address challenges such as security threats, climate change, and economic development, allowing African nations to leverage their collective strength ([Barbara 2024](#)). By engaging in multilateralism, African countries have participated in fostering partnerships with other regions, attracting foreign investment, and promoting peace and stability ([Oduwole 2014](#)).

Historically, Nigeria, as one of the largest countries in Africa, has been a key player in several African countries, demonstrating commitment to regional cooperation and integration. Nigeria participated in various organizations, some of which include the United Nations (UN), where Nigeria actively participates in peacekeeping missions and discussions on global issues like climate change and human rights ([Adebajo 2008](#)). Additionally, Nigeria is a member of the African Union (AU), the Economic Community of West African States (ECOWAS), and the Commonwealth of Nations, among others ([Obi 2021](#)). This membership enables Nigeria to engage with other countries. However, despite being a founding member of various international organizations (IOs), Nigeria's engagement has not yielded the expected benefits for the country. Efforts have been made by scholars and policymakers to address this issue, yet the problem persists. It is manifested in many ways. The economy remains vulnerable, and infrastructure and human development indicators continue to lag. The country's participation in IOs could only be explained as ineffective and inefficient ([Oshewolo et al. 2023](#)).

Thus, this paper aims to investigate the level of Nigeria's participation in IOs and to assess the impact of its engagement on national development. This introduction is followed by a chapter on methodology, literature review, and theoretical framework. The next chapter is focused on determining the level of Nigeria's participation in IOs in Africa since obtaining independence and the impact of this participation on the development of the country. The last segment consists of the conclusion and recommendations.

Methods and materials

In order to investigate the intricate relationship among multilateralism, national development, and Nigeria's contributions to the growth of international organizations (IOs) in Africa, this study uses qualitative research methods and a case study approach. Because it makes it easier to gather comprehensive, nuanced, and contextual insights about social phenomena, such as behaviors, attitudes, and experiences pertinent to Nigeria's involvement with IOs, qualitative research is especially useful for this study. A multifaceted data collection technique has been used to accomplish the study's goals. The study mostly uses secondary data from a wide range of sources, such as official publications, scholarly works, policy documents, and credible media sources. A thorough grasp of Nigeria's history and current roles within various international institutions, such as the African Union (AU) and the Economic Community of West African States (ECOWAS), is made possible by this extensive compilation of information.

Content analysis has been adopted as the main method for the analysis of the gathered data. This analytical technique enables a methodical analysis of textual data to find trends, themes, and patterns pertaining to Nigeria's involvement in and contributions to international organizations. The study examines the effects of Nigeria's international participation on national development results and challenges prevailing narratives by examining the substance of documents and literature. Furthermore, the case study method allows for a concentrated investigation of particular examples of Nigeria's engagement with different IOs, placing the results in the larger context of Africa's political and developmental environment. This method makes it easier to identify important players, their motivations, and the way internal and foreign issues interact to influence Nigeria's foreign policy choices.

Thus, the approach described here offers a solid framework for analyzing the complex dynamics of multilateralism in Africa, especially as they relate to Nigeria's goals for regional leadership and national development. This study aims to shed light on Nigeria's successes and difficulties in using the potential of international organizations for its development objectives through a methodical collection and analysis of qualitative data.

Theoretical Framework

This paper adopts the approach of liberal institutionalism. This tool of analysis is quite relevant here because it focuses on specialized international agencies as the main actors in international politics. Also, liberalism, a subset of international relations, posits that morality, law, and IOs can indeed set the basis for relations between states ([Moravcsik 1997](#)). It was asserted that cooperation among states is possible and there is a possibility of states acting as a community rather than an autonomous unit ([Keohane 1984](#)). Even though realism argues that the international

system is anarchical in nature and states pursue self-interests, Neo-liberalism, a critique that emerged in the 1980s, debunked this view held by the realists, as it rather lays emphasis on international institutions as a means of reducing conflicts (Goldstein and Pevehouse 2007). This school of thought believes that human beings are not only rational but also cooperative to seek mutual and long-term gains rather than maximizing short-term gains, hence the term liberal institutionalism.

Formal institutions, such as neo-liberalism, promote international cooperation through rules, regulations, and decision-making procedures. Neo-liberalism focuses on economic and environmental cooperation, analyzing state behavior and the international system (Keohane 1984). It posits that increased economic contacts between states lead to dependence for national goals like growth, employment, and price stability. ECOWAS, from a neo-liberal perspective, can act as a regional ally for states to achieve economic objectives. Liberal institutionalism promotes economic cooperation, integration, trade barriers, and peace. AU and ECOWAS are responsible for ensuring free movement of people and goods, smooth trade relations, and peace and security within the region (Moravcsik 1997). The theory is used to justify Nigeria's involvement in IOs in Africa, especially the AU and ECOWAS. The theory is also used to explain what Nigeria has gained from these multilateral relations.

The Theory Employed and the Empirical Analysis

The theory of Liberal Institutionalism employed in the study provides a fundamental framework for comprehending Nigeria's interactions with international organizations (IOs) in Africa. According to liberal institutionalism, international organizations and institutions are essential for fostering state cooperation, peace, stability, and reciprocal economic gains. This theory highlights the importance of group action and the notion that states can work together to accomplish shared objectives through common frameworks, regulations, and standards rather than being purely self-interested actors.

Nigeria's active involvement in the establishment and administration of important African IOs, such as the African Union (AU) and the Economic Community of West African States (ECOWAS), is evaluated in the empirical analysis in light of its foreign policy aims and national development goals. By identifying particular instances when Nigeria has used its participation in these organizations so as to achieve regional stability, economic integration, and collective security, the analysis supports the argument. The paper, for example, highlights Nigeria's crucial role in setting up the OAU and ECOWAS, demonstrating how its ideological dedication to African growth and unity is consistent with the principles of liberal institutionalism. The practical implementation of liberal institutionalism is demonstrated by Nigeria's financial contributions and diplomatic interactions with these organizations, which have sought to promote cooperative projects that tackle urgent regional problems and increase Nigeria's influence on the continent.

Furthermore, the empirical findings highlight an area where the principles of liberal institutionalism may need to be reevaluated because, despite Nigeria's substantial contributions to these multilateral institutions, the anticipated developmental gains for Nigeria have not been completely realized. According to the theory, institutional cooperation can benefit both parties, but the precise results rely on the internal and external difficulties that member nations confront, such as corruption, poor governance, and regional instability, all of which Nigeria still faces.

Deductively, liberal institutionalism and the empirical analysis are related in that the theory offers the analytical framework for understanding Nigeria's participation in international organizations, and the empirical results show how these interactions affect both Nigeria's domestic development and its larger regional goals.

Literature Review

This part reviews some related literature on relevant concepts in this paper, which include multilateralism, development, national interest, and national development.

Multilateralism: Multilateralism, according to Ruggie (1992), is the coordination of interactions among three or more nations, based on common values and norms such as diffuse reciprocity, generalized behavior, and indivisibility. It places a strong emphasis on using shared frameworks to promote international cooperation in the political, economic, and security spheres. According to Bayne and Woolcock (2017), multilateralism plays a significant role in Africa, especially in advancing sustainable development, peacekeeping, and regional integration through institutions like the African Union (AU) and ECOWAS. They also highlight how trade and financial cooperation help to maintain economic stability.

Ikenberry (2011) argues that multilateralism strengthens global governance by promoting inclusivity, accountability, and legality in international decision-making, setting it apart from bilateralism and unilateralism. Dauda, Ahmad, and Keling (2019) highlight the peacekeeping and conflict-resolution functions of multilateralism, especially through institutions like the UN, AU, and ECOWAS, which lessen the possibility of violence and encourage diplomatic interaction. Through organizations like the WTO, ECOWAS Free Trade Area, and ACFTA that promote investment, employment, and technical advancement, Bhagwati (2008) links multilateralism to economic development and trade liberalization.

As demonstrated by the Paris Agreement and the WHO's cooperation during COVID-19, Kickbusch (2020) emphasizes its significance in tackling global issues like pandemics and climate change by facilitating resource sharing and collaborative action. Lastly, Abdel-Latif (2023) argues that through organizations like the UN Human Rights Council and the ICC, multilateralism upholds international law and a rules-based global order, guaranteeing justice, human rights, and predictability in international relations.

Development: According to the different experts, development is a multifaceted, collaborative process that includes moral, social, and human improvement in addition to economic success. According to Oguonu (2012), development entails collaboration between the governed and the government, whereby both work to raise social well-being and living standards. While acknowledging the traditional economic indicators of progress, such as national income and per capita growth, Onah (2010) contends that true development should go beyond economic growth to include advancements in human welfare and quality of life.

In a similar vein, Todaro and Smith (2011) define development as a process that combines social change and economic growth with the goal of lowering poverty and inequality while improving freedom, health, and education. Sen (1999) broadens this concept by characterizing progress as the growth of individuals' liberties and the elimination of limitations such as social deprivation and poverty. A normative dimension is added by Goulet (1971), who contends that genuine growth must ensure freedom, self-worth, and life-sustenance to demonstrate respect for human dignity. According to Seers (1969), progress should not just be evaluated based on economic indicators but also on the way it affects poverty, unemployment, and inequality. In order to guarantee inclusion and sustainability, Chambers (1997) argues that development must be led by the people, particularly the excluded.

The ability of a society to use resources to improve human situations and achieve structural transformation is the final way that Rodney (1972) places development within a historical-materialist framework. Together, these academics see development as a comprehensive, people-centered, and transformational process that aims to improve the well-being of individuals and society as a whole.

National Interest: Scholars generally agree that a country's national interest serves as the foundation for both its foreign and domestic policies. According to Ukhamsi and Kumapayi (2023), it is the tenet that directs governmental acts, which are influenced by a nation's domestic requirements and constitution, which in turn affect its interactions with other countries. Agaba and Ukhamsi (2015) show how many governments struggle to articulate their national interests, pointing out that a country loses focus in both its foreign and domestic policies when its national interests are not properly defined.

According to Nester (2001), national interest includes both broad aims like peace, security, and economic expansion, as well as particular purposes exclusive to each state that are frequently achieved by the use of force. From a realist perspective, Morgenthau (1948) claims that the quest for power is a fundamental aspect of international politics and defines national interest only in terms of survival and power. Rosenau (1969), on the other hand, broadens the idea to encompass both tangible and intangible components, such as culture, ideology, and leadership views, which influence the definition and pursuit of national interests.

For Holsti (1967), national interest is multifaceted, encompassing short-term security requirements, medium-term objectives like economic cooperation, and long-term ambitions like world peace. According to Schwarzenberger (1951), the idea of national interest is dynamic and ever-changing, responding to shifts in both internal and external circumstances. As governments put their own growth and survival first in their interactions with others, Ebegbulem (2019) emphasizes its crucial significance in foreign policy.

All things considered, the writers agree that national interest is a dynamic, multifaceted, and context-driven idea that integrates aspects of welfare, security, power, and values to influence how nations behave and engage with one another in the international system.

National Development: According to the experts, national development is a thorough and multifaceted process that aims to enhance residents' general well-being and quality of life. According to Bhawna (2016), it is the overall progress of a country in all areas – economic, social, political, and cultural – with a focus on lowering inequality, raising living standards, and ensuring the safety of people and property. It is defined by Adagbabiri and Okolie (2016) as the long-term enhancement of the material and spiritual facets of national life, as evidenced by improved housing, food, education, transportation, and general happiness, all accomplished in a manner that upholds human dignity. According to Todaro and Smith (2006), growth is a transforming process that involves raising society via freedom, self-worth, and sustenance, three essential components that propel human-centered advancement.

National development in Nigeria is defined as the government's endeavor to improve the welfare of its people via economic diversification, infrastructure, healthcare, and education. This devotion is demonstrated by programs such as the National Economic Empowerment and Development Strategy (NEEDS), which places a high priority on institutional reform, human capital development, and poverty reduction.

All of the academics agree that national development is a wide, inclusive, and people-centered process that combines economic expansion with social advancement, human dignity, and long-term enhancement of the standard of living for the populace.

Results and Discussion

Nigeria's roles in the development of IOs in Africa

Nigeria's role in the development of IOs in Africa cannot be overemphasized because, since the attainment of independence, it has made Africa its centerpiece. It makes its foreign policy towards the development of Africa a *sine qua non*. Nigeria's commitments are majorly felt in its active participation in the establishment of major IOs and the management of those organizations in Africa.

a. Establishment of IOs in Africa

Nigeria has participated substantially and proactively in the establishment and

development of major African international organizations. Its participation is both ideological and practical, shaped by its post-independence foreign policy, population size, geographical positioning, and aspiration to provide leadership on the African continent. Nigeria's engagement has been guided by principles of African unity, regional stability, and economic integration. Over the decades, this engagement has manifested in leadership roles, founding memberships, and consistent diplomatic activity across the continent ([Adebajo 2008](#)).

One of the earliest and most significant examples of Nigeria's contribution to the establishment of IOs in Africa was its involvement in the creation of the Organization of African Unity (OAU) in 1963. Nigeria was among the 32 independent African countries that signed the OAU Charter in Addis Ababa, Ethiopia, a foundational moment in the continent's post-colonial history. This marked not only Nigeria's early commitment to continental solidarity but also demonstrated its willingness to take a leadership role in Africa's collective efforts to safeguard independence, resist neo-colonialism, and promote integration. The establishment of the OAU came at a time when African countries were deeply divided along ideological lines, with two major blocs: the radical Casablanca Group, which supported rapid political integration, and the more cautious Monrovia Group, which favored gradual cooperation while preserving national sovereignty. Nigeria, under the leadership of Prime Minister Abubakar Tafawa Balewa, strategically aligned with the Monrovia Group, advocating a more moderate and pragmatic approach to unity that emphasized functional cooperation in key areas such as education, trade, culture, and diplomacy, rather than immediate political federation ([Adebajo 2022](#)).

Balewa's position was grounded in Nigeria's broader foreign policy outlook, which prioritized non-alignment, respect for state sovereignty, and peaceful coexistence. He believed that unity should emerge organically through mutual respect and shared interests, rather than through political pressure or ideological compulsion. In his address during the Addis Ababa Conference, Balewa emphasized that while political unity was desirable, the diversity of Africa's colonial experiences and political systems necessitated a cautious, cooperative approach to integration. This moderate vision was key in bridging the ideological gap between the two rival blocs and helped create a broad consensus that enabled the adoption of the OAU Charter ([Akinyeye 2017](#)).

General Yakubu Gowon played a decisive role in the establishment of the Economic Community of West African States (ECOWAS). Following the Nigerian Civil War, Gowon sought ways to foster regional cooperation and prevent future conflict by promoting economic integration. He initiated high-level discussions with President Gnassingbé Eyadéma of Togo in the early 1970s to lay the groundwork for a regional economic bloc ([Arise 2022](#)). These discussions culminated in the signing of the Treaty of Lagos on 28 May 1975, officially establishing ECOWAS, with Nigeria as a founding and leading member. Gowon's leadership was critical in garnering regional consensus, and Nigeria under his administration provided

both political and material support to ensure the successful establishment of the organization ([Nnoli 1980](#)).

Olusegun Obasanjo, who succeeded Gowon after the 1975 coup, continued Nigeria's strong engagement in regional and continental diplomacy. As a military head of state (1976–1979) and later as a civilian president (1999–2007), Obasanjo was deeply committed to African integration. During his military tenure, he reinforced Nigeria's role in ECOWAS and promoted liberation movements across Southern Africa, including the ANC in South Africa and MPLA in Angola. He also hosted the 1977 FESTAC (Second World Black and African Festival of Arts and Culture), symbolizing Nigeria's commitment to pan-African cultural and political solidarity ([Nwanegbo 2008](#)).

In his civilian presidency, Obasanjo was central to the transformation of the Organization of African Unity (OAU) into the African Union (AU). Nigeria was among the first countries to ratify the Constitutive Act of the African Union on 26 April 2001, an action that brought the AU into full legal existence. Obasanjo also led peace mediation efforts across the continent, including in Liberia, Sudan, and Côte d'Ivoire, and proposed the establishment of an African standby force to deal with conflicts, reinforcing Nigeria's role in institutionalizing African solutions to African problems. Through the initiatives of Gowon in establishing ECOWAS and Obasanjo's efforts in strengthening both ECOWAS and the African Union, Nigeria not only helped form these key organizations but also provided leadership, funding, and strategic direction. Their efforts positioned Nigeria as a central force in Africa's multilateral development and integration ([Adebajo 2002](#)). In accordance with liberal institutionalism, this paper concludes that Nigeria has contributed immensely to the emergence and development of international organizations. These contributions relate to the Nigerian belief that human beings are rational and cooperative, seeking mutual and long-term gains, rather than maximizing short-term gains.

b. Management of IOs in Africa

Nigeria has played a significant and influential role in the management of IOs across Africa. It has contributed financially and diplomatically to IOs to foster regional and continental development. As the continent's most populous country and one of its largest economies, Nigeria's influence is felt in various international bodies, reflecting its commitment to Africa's political stability, economic development, and global representation. Nigeria has provided key leadership within major African organizations, such as the African Union (AU) and the Economic Community of West African States (ECOWAS). Nigerian diplomats have taken on prominent roles, shaping policies that address peacekeeping, conflict resolution, and regional integration. Nigeria's commitment to peace is evident in its leading role in ECOWAS-led peacekeeping missions in Liberia, Mali, Sierra Leone, and the Central African Republic, where it has deployed troops and offered financial resources to stabilize conflict-affected areas ([Onuoha 2013](#)).

Nigeria is one of the largest contributors to African IOs, playing a crucial role in supporting the continent's political stability and development. The country provides substantial funding to key bodies such as the Economic Community of West African States (ECOWAS), the African Union (AU), and various peacekeeping and humanitarian initiatives. These financial contributions help ensure that these organizations can operate effectively, respond quickly to regional crises, and sustain long-term development programs. Its funding is vital in supporting peacekeeping missions across Africa, particularly in conflict zones within West Africa. By underwriting the costs associated with deploying troops, logistics, and humanitarian aid, Nigeria strengthens the capacity of organizations like ECOWAS to maintain peace and security (KFF 2022). This financial backing not only facilitates immediate conflict resolution but also supports post-conflict reconstruction efforts, enabling affected countries to rebuild infrastructure and institutions. Nigeria's financial commitments contribute to regional economic integration projects (Congressional Research Service 2020). These include infrastructure development, such as roads, energy, and trade facilitation initiatives that aim to boost intra-African trade and economic growth. Nigerian leaders like Olu Femi Adeniran have held chairmanship roles in financial committees within ECOWAS and the African Development Bank, helping to shape policies that promote regional economic integration and financial stability. Despite challenges such as political instability and corruption, Nigeria's geopolitical importance and economic strength keep it central to Africa's international cooperation and governance efforts (Nwankwo 2021; Adeniran 2023). Table 1 and Figure 1 depict the level of Nigeria's financial commitments to international organizations.

TABLE 1. Financial Contributions of Member States of ECOWAS S

No.	Member Country	Financial Contributions for ECOWAS Sustenance
1	Benin	3.9%
2	Burkina Faso	2.6%
3	Cape Verde	1.5%
4	Cote D' Ivoire	13%
5	The Gambia	6%
6	Ghana	12.9%
7	Guinea Bissau	1.5%
8	Liberia	6.7%
9	Mali	1.9%
10	Mauritania	2.6%
11	Niger	2.1%
12	Nigeria	32.8%
13	Senegal	5.4%
14	Sierra Leone	4.4%
15	Togo	3.6%

Source: ECOWAS Secretariat, Lagos (Library document on member's contributions), 2013

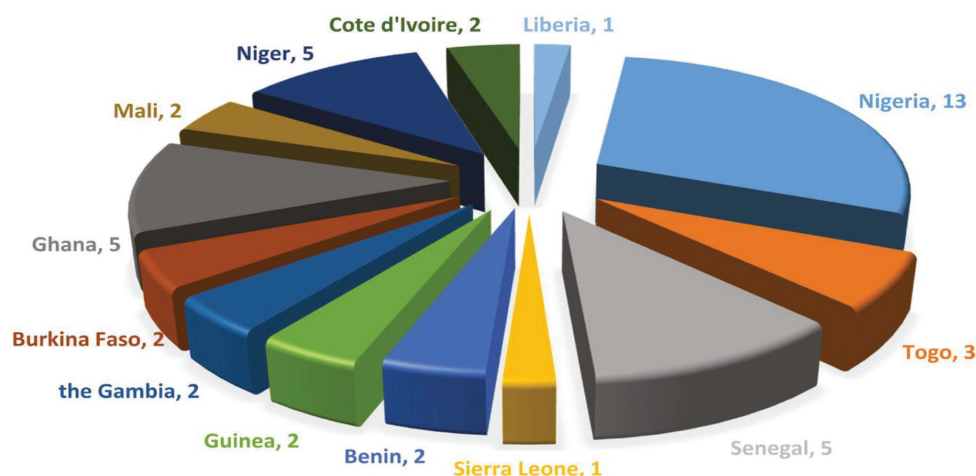


Figure 1 Years Spent by Member-countries as Chair of ECOWAS.

Source: Oshewolo et al. (2023) Nigeria in ECOWAS Politics: Major Contributions, Dividends and Setbacks.

Following the analysis above, this paper argues that Nigeria is not only the major financial hub of ECOWAS but also a force behind the successes of the union. Nigeria has demonstrated its commitment and belief in cooperation with other states to attain greater happiness for Africans in general and Nigerians in particular.

Multilateralism policy and Nigeria's development

The position of Nigeria in Africa, resulting from human and natural resource endowment, made Nigeria pursue an Africa-centered foreign policy, which is also in line with liberal institutionalism. In this quest, the only viable option available was multilateral diplomacy. Therefore, the Commonwealth of Nations, the Nonaligned Movement, the United Nations (UN), and the Organization of African Unity (OAU) became the earliest medium with which Nigeria pursued its national and African interests (Agaba and Ukhani 2015). The fundamental tenets of Nigeria's foreign policy are "non-alignment, African solidarity, economic diplomacy, peacekeeping, international cooperation, national interest, regional integration, multilateralism, cultural diplomacy, and national sovereignty (Danyaya 2025). These tenets influenced Nigeria's relations with the international community, fostering economic growth, peace, and cooperation while safeguarding national interests. Nigeria's involvement in international organizations, participation in global governance, and bilateral and multilateral interactions with other nations all clearly reflect the aforementioned ideals.

On many occasions, Nigeria had cooperated with other states to fight against insurgent groups in Sub-Saharan regions. Nigeria played a significant role in regional peacekeeping operations in Sierra Leone and Liberia between 1990 and 2002, mainly to bring peace and stability to these two nations. Nigeria has benefited from this policy by ensuring peaceful coexistence in the world, which, in turn, brings about peace to Nigeria. The image of Nigeria is boosted through multilateral policy, even

though, on many occasions, official activities by Nigerian peacekeeping forces have raised ethical concerns ([Danyaya 2025](#)).

The African Continental Free Trade Area (AfCFTA), ratified by Nigeria in December 2020, remains a cornerstone of regional integration. The agreement aims to eliminate tariffs on 90 percent of goods, promoting a freer exchange of goods and services across Africa. This paper is of the view that the full implementation of AfCFTA has boosted Nigeria's exports significantly, provided greater market access, and reduced reliance on crude oil exports. The benefits of AfCFTA to the Nigerian economy equally include larger market access, free movement of labour, goods, services, and capital. The AfCFTA agreement has also motivated Nigerian SMEs to expand their businesses to other African countries.

Before the enactment of the AfCFTA agreement, ECOWAS was in place to manage the African economy. Nigeria was not only an active member when it was first established, but also continues to be active since its formation in 1975. Like AfCFTA, Nigeria benefited from the free trade policy of ECOWAS. This policy has favored Nigeria in exporting its goods to West African states. Nigeria also benefited, through its multilateral policy, from ECOWAS, through increased trade opportunities, access to a larger regional market, and the free movement of labor, visa facilitation for our businessmen and women, and students. Nigeria earned \$823.06 million from exports to ECOWAS countries and \$2.72 billion from shipping out products to Africa in the first quarter of 2020. In the second quarter of 2020, exports to the whole of Africa were estimated at N401.4 billion, while goods worth N149.3billion were exported to ECOWAS. This, according to analysts, is set to expand owing to the AfCFTA. In 2018, Nigeria equally benefited from \$5bn in projects from China through its visit to ECOWAS members at the Forum on China – Africa Cooperation (FOCAC) ([Akinyemi, Okoli, and Chidozie 2021](#)). Nigeria has also managed to achieve its vision in prompting the commitment of ECOWAS Member States to deepening and strengthening institutions in the sub-region, through good governance, the fight against corruption, combating terrorism, violent extremism, and organized crime.

The influence of Nigeria in the AU and its participation in the union equally improved Nigeria's development. Though Nigeria expended its oil boom funds on the liberation of some African countries like Sierra Leone, Liberia, and South Africa. It is on record that the High Commissioner of Sierra Leone to Nigeria, Dr. Solomon Gembah, says that Nigeria spent over \$13bn on the liberation of his country and Liberia ([Adebajo 2022](#)). Despite this humongous amount spent on achieving multilateralism of Nigeria's foreign policy, it equally benefited from the policy because this action projected the image and prestige of Nigeria among member states in the entire continent of Africa. Another benefit is security and support from African member states during the Nigerian civil war. Nigeria, for instance, benefited from the loyalty of Niger to the extent that the Nigerian president, Ahmadu Diori, was quoted to have said that he could abandon it at its challenging time ([Dele 2017](#)). Justifying his position, Diori said that given how extensively Niger depends on

Nigeria for economic survival, he could not support Biafra, because according to him, “when Nigeria sneezes, Niger not only catches a cold, it is already on admission in the hospital” (Dele 2017).

Moreover, Nigeria is a member of OPEC, which regulates the price and export of oil. Being a member of this organization has assisted Nigeria in maximizing opportunities from crude oil export. In 2021, the then Minister of State Petroleum Resources, Chief Timipre Sylva, highlighted the critical benefits of Nigeria’s 50-year membership in OPEC, which began in 1971 (Leadership 2021). He stated that OPEC has enabled Nigeria to coordinate oil policies, secure stable oil prices, and influence the global oil market. Sylva emphasized that this membership has fostered the development of Nigeria’s oil industry and has been mutually beneficial, facilitating policy harmonization and the sharing of expertise among member countries (Leadership 2021). Nigeria has significantly benefited from OPEC’s efforts to stabilize the oil market, due to its reliance on oil revenue. The country has played a crucial role in OPEC’s success, producing six Presidents of OPEC conferences and four Secretaries-General.

Multilateralism has propelled and showcased Nigerian values among the committee of nations. Since 1960, when it attained its independence, it has extended its influence to other parts of the world. This is done by joining the United Nations Organization (UNO), now known as the UN, and being active in the activities of the Union. It maximized the opportunity to the extent Nigeria tops the list of African countries to have been on the United Nations Security Council as a non-permanent seat member with a record of five times from 1966 – 1967, 1978 – 1979, 1994 – 1995, 2010 – 2011, and 2014 – 2015.

Systematic Analysis of the Impact of Nigeria’s Multilateral Foreign Policy on National Development

Nigeria’s foreign policy emphasizes multilateral diplomacy to enhance African-centered initiatives, leveraging its strategic location and resources. Key organizations aiding this pursuit include the OAU, UN, Commonwealth of Nations, and Non-Aligned Movement. The following systematic analysis of the impacts of these multilateral initiatives on Nigeria’s national development is quite essential:

1. Economic Growth: Nigeria’s involvement in multilateral trade agreements such as ECOWAS and the AfCFTA has significantly enhanced its economic growth. The ratification of AfCFTA in December 2020 facilitated free trade across Africa by eliminating tariffs on 90% of goods, allowing Nigerian companies better market access and promoting economic diversification away from crude oil dependence. Nigeria’s longstanding participation in ECOWAS since 1975 has also provided its products access to a broader West African market, with exports to ECOWAS nations generating approximately \$823 million in the first half of 2020. This economic integration supports the growth and resilience of Nigerian SMEs in other African

markets by providing them with increased opportunities for trade, access to larger consumer bases, and the ability to compete more effectively against larger firms.

2. Security and Reputation: Nigeria's contributions to regional peacekeeping, especially in Sierra Leone and Liberia from 1990 to 2002, have significantly enhanced its national security and international reputation. By fostering a stable environment in West Africa, Nigeria's actions have indirectly benefited its own security and positioned it as a regional leader, earning respect from neighboring countries despite some ethical issues associated with its peacekeeping operations.

3. International Standing and Political Leverage: Nigeria's political clout in international fora has been strengthened by its proactive diplomacy. Nigeria's 50-year membership in OPEC has been essential to maintaining oil price stability and boosting the nation's oil-dependent economy. Nigeria has been able to boost its export revenue, which is essential to its national growth, and influence global oil policies thanks to the strategic advantages of OPEC membership. Participation in the UN: Nigeria's dedication to global governance has been highlighted by its history as a non-permanent member of the UN Security Council. Nigeria has actively participated in international debates over its five periods in this position, which has improved its reputation internationally and given it the opportunity to promote African concerns on a global scale.

4. National Sovereignty and Security Cooperation: Nigeria has strengthened its security arrangements by pursuing multilateral collaborations. Collaborative Security Efforts: Nigeria has improved regional security cooperation in the fight against organized crime and terrorism by cultivating alliances within ECOWAS and the African Union (AU). This strategy has been crucial for resolving internal security issues and bolstering Nigeria's influence in the region. Assistance in Times of Crisis: A spirit of solidarity that further strengthens national stability and sovereignty is fostered by Nigeria's established links with other African states, as demonstrated by historical circumstances such as the Nigerian Civil War.

5. Cultural diplomacy and image: Nigeria's image in the world has been greatly influenced by its multilateral foreign policy, which promotes international collaboration and cultural interchange. Cultural diplomacy: Nigeria's foreign policy is based on the principles of African solidarity and cultural diplomacy, which have enabled the nation to showcase its rich cultural legacy internationally and gain soft power that facilitates international interactions and cooperation. International Aid and Cooperation: Despite being expensive, Nigeria's financial contributions to the liberation of nations like Sierra Leone and Liberia have improved its reputation as a pan-African leader. As a result, neighboring nations have offered Nigeria reciprocal support, which could be crucial for Nigeria's international relations.

Conclusion and Recommendations

Nigeria's historical dedication to African unity, regional stability, and collective prosperity is demonstrated by its long-standing participation in multilateral organizations, including the United Nations, the African Union, and the Economic Community of West African States. This paper has demonstrated that Nigeria has continuously asserted itself as a key player in Africa's multilateral architecture, from its groundbreaking role in the creation of the Organization of African Unity (OAU) to its leadership in peacekeeping, crisis resolution, and regional integration. These contributions, which are based on the ideas of liberal institutionalism, show how Nigeria views collaboration, common standards, and institutional frameworks as means of achieving mutual advancement.

This paper, however, highlights a glaring paradox: despite Nigeria's massive financial, military, and diplomatic investments in the growth and maintenance of international organizations in Africa, the country's own progress has been unequal and limited. The main contribution is that the expected benefits of global participation, including improved governance, infrastructure development, economic change, and human development, have not yet materialized. This disconnect is not primarily the result of multilateralism's failure; rather, it is a reflection of enduring domestic obstacles that make it difficult to effectively translate external engagements into internal development outcomes, such as governance deficiencies, corruption, weak institutions, and inconsistent policy ([Chidozie 2021](#)).

Furthermore, the paper has shown that rather than a well-defined and deliberately pursued national interest, Nigeria's multilateral involvement has frequently been motivated more by ideological commitments to African solidarity and leadership aspirations. Although this has increased Nigeria's stature and power throughout the continent, it has also resulted in a trend of disproportionate contributions in comparison to observable national gains. As a result, Nigeria's participation in international organizations might be described as having an impact on the region but not being the best at achieving its own development goals.

All things considered, Nigeria's experience from 1960 to 2025 shows that, despite its importance, multilateralism is not intrinsically sufficient for national growth. Strong institutional frameworks, cogent national interest articulation, and alignment of external engagements with internal capabilities are all necessary for its efficacy. Suffice it to say that Nigeria participates extensively but does not benefit sufficiently.

This article proposes that Nigeria must change from broad, ideology-driven global involvement to a strategic, interest-based strategy. In its interactions with institutions like the United Nations, the African Union, and the Economic Community of West African States, Nigeria should prioritize and clearly define its national interests, making sure that involvement results in quantifiable national advantages. Aligning global commitments with domestic development objectives is a top issue, especially

by making use of frameworks like the African Continental Free Trade Area to support industrialization, trade expansion, and economic diversification. To successfully convert foreign activities into observable development achievements, it is also crucial to strengthen domestic institutions, enhance governance, and combat corruption. Nigeria could also improve economic diplomacy, take on a more strategic and selected leadership role, and set up robust monitoring systems to assess the advantages of its global engagement. The nation's ability to gain from multilateralism will be further enhanced by investing in human resources and supporting the private sector, particularly SMEs. In order to ensure that its involvement in regional security, diplomacy, and cultural influence translates into tangible economic, political, and developmental gains at home, Nigeria must finally align its financial and military contributions with anticipated rewards.

References

- Abdel-Latif, J.** 2023. "Egypt and Nigeria: Complementary roles in African Union leadership." *African Affairs* 122(486): 1-22.
- Adagbabiri, M.M., and A.M. Okolie.** 2016. "The challenges of national development in Nigeria in the 21st century." *International Journal of Advanced Academic Research* 2(7): 45-58.
- Adebajo, A.** 2008. *The curse of Berlin: Africa after the Cold War*. Columbia University Press.
- _____. 2021. *The curse of Berlin: Africa after the Cold War*. Oxford University Press.
- _____. 2022. "Nigeria and South Africa in the African Union: Cooperation and competition in continental leadership." *International Affairs* 98(3): 1045-1063.
- Adeniran, T.** 2023. *Nigeria's domestic challenges and regional leadership in Africa*. Centre for Strategic Studies Press.
- Agaba, J., and U. Ukhami.** 2015. "Defining national interest in contemporary foreign policy." *Journal of International Relations* 12(3): 45-58.
- Akinyemi, A., N. Okoli, and F. Chidozie.** 2021. *Corruption and governance in Nigeria: Issues and perspectives*. Spectrum Books.
- Akinyeye, Y.** 2017. "Nigeria and the African Union: A study of Nigeria's role in the development of the African Union." *African Journal of International Affairs* 20(1-2): 1-20.
- Anyaoku, E.** 2012. *Nigeria's foreign policy and leadership in Africa: Challenges and prospects*. Nigerian Institute of International Affairs.
- Arise, O.** 2022. "Economic decline and Nigeria's regional influence in Africa." *Nigerian Economic Review Journal* 8(2): 45-63.
- Ayoob, M.** 1991. "The security problematic of the Third World. *World Politics* 43(2): 257-283. <https://doi.org/10.2307/2010473>."
- Barbara, K.** 2024. Africa's multilateral engagement in global governance. *Global Policy Journal* 15(1): 78-92.

- Bayne, N., and S. Woolcock.** 2017. *The new economic diplomacy: Decision-making and negotiation in international economic relations* (4th ed.). Routledge.
- Bhagwati, J.** 2008. *Termites in the trading system: How preferential agreements undermine free trade*. Oxford University Press.
- Bhawna, S.** 2016. "National development and its indicators." *International Journal of Research in Social Sciences* 6(8): 22-29.
- Chambers, R.** 1997. *Whose reality counts? Putting the first last*. Intermediate Technology Publications.
- Chidozie, F.** 2021. "Civil society and the anti-corruption struggle in Nigeria." *African Journal of Political Studies* 15(1): 22-39.
- Congressional Research Service.** 2020. *Nigeria: Current issues and U.S. policy* (CRS Report No. R43836). U.S. Library of Congress. <https://crsreports.congress.gov>.
- Danyaya, M.S.** 2025. "The fundamental principles of Nigerian foreign policy in international relations. *Mediterranean Publications and Research International Journal of Humanities, Literature and Art Research*.
- Dauda, M., M.Z. Ahmad, and M.F. Keling.** 2019. Nigeria's role and its peacekeeping challenges in Africa: An assessment. *European Journal of Social Sciences Studies* 3(4): 186-208.
- Dele, I.** 2017. "Over-dependence on oil and its implication for development in Nigeria." *HUMASS: McU Journal of Humanities, Management, Applied & Social Sciences* 1(2): 25-33. <https://www.researchgate.net/publication/330662159> Over-Dependence on Oil and its Implication for Development in Nigeria.
- Ebegbulem, J.C.** 2019. "The dynamics of Nigeria's foreign policy and national interest." *African Journal of Political Science and International Relations* 13(4): 57-68.
- Goldstein, J.S., and J.C. Pevehouse.** (2008). *International relations* (8th ed.). Pearson.
- Goulet, D.** 1971. *The cruel choice: A new concept in the theory of development*. Atheneum Press.
- Holsti, K.J.** 1967. "National role conceptions in the study of foreign policy." *International Studies Quarterly* 14(3): 233-309. <https://doi.org/10.2307/3013584>.
- Ikenberry, G.J.** 2011. *Liberal leviathan: The origins, crisis, and transformation of the American world order*. Princeton University Press.
- Keohane, R.O.** 1984. *After hegemony: Cooperation and discord in the world political economy*. Princeton University Press.
- KFF.** 2022. PEPFAR: The U.S. President's Emergency Plan for AIDS Relief. *Kaiser Family Foundation*.
- Kickbusch, I.** 2020. "The COVID-19 pandemic: Shaping the health diplomacy of the future." *Global Health Diplomacy Journal* 1(1): 5-12.
- Leadership.** 2021. Public service person of the year 2021: Chief Timipre Sylva. *Leadership Conferences*.
- Moravcsik, A.** 1997. "Taking preferences seriously: A liberal theory of international politics." *International Organization* 51(4): 513-553. <https://www.princeton.edu/~amoravcs/library/preferences.pdf>.

- Morgenthau, H.J.** 1948. *Politics among nations: The struggle for power and peace*. Alfred A. Knopf.
- Ndlovu-Gatsheni, S.J.** 2020. *Decolonization, development and knowledge in Africa: Turning over a new leaf*. Routledge.
- Nester, W.R.** 2001. *The foundations of American power: The United States in the global arena, 1789–1990*. St. Martin's Press.
- Nnoli, O.** 1980. *Ethnic politics in Nigeria*. Fourth Dimension Publishing.
- Nwanegbo, C.** 2008. "Obasanjo's role in the development of ECOWAS." *Journal of West African Studies* 15(2): 120-135.
- Nwankwo, C.O.** 2021. "Nigeria's financial contributions to regional organizations: Implications for African stability and integration." *African Journal of International Relations* 12(1): 28-49.
- Obi, C.** 2021. "Evolution of Nigeria's peacekeeping doctrine: From reactive to proactive engagement." *Journal of Modern African Studies* 59(3): 389-412.
- Oduwole, J.** 2014. "International trade dispute remedies: How equitable for Africa?" *Journal of Private and Property Law* 32: 92-105.
- Oguonu, C.N.** 2012. *Public administration: A Nigerian and comparative perspective*. Great AP Express Publishers.
- Onah, F.O.** 2010. *Managing public programmes and projects*. Great AP Express Publishers.
- Onuoha, F.** 2013. "Nigeria's role in peacekeeping and conflict resolution in Africa: A critical assessment." *Nigerian Journal of International Studies* 39(1): 15-34.
- Oshewolo, S., A. Azeez, O. Adesanya, T. Oladipo, O. Olaleye, and O. Ade-Ibijola.** 2023. Nigeria in ECOWAS politics: Major contributions, dividends and setbacks. *African Studies Association of India*.
- Rodney, W.** 1972. *How Europe underdeveloped Africa*. Bogle-L'Ouverture Publications.
- Rosenau, J.N.** 1969. *Linkage politics: Essays on the convergence of national and international systems*. Free Press.
- Ruggie, J.G.** 1992. "Multilateralism: The anatomy of an institution." *International Organization* 46(3): 561-598. <https://doi.org/10.1017/S0020818300027831>.
- Schwarzenberger, G.** 1951. *Power politics: A study of international society*. Stevens & Sons.
- Seers, D.** 1969. The meaning of development. *International Development Review* 11(4): 2-6.
- Sen, A.** 1999. *Development as freedom*. Oxford University Press.
- Todaro, M.P., and S.C. Smith.** 2006. *Economic development* (9th ed.). Addison-Wesley.
- _____. (2011). *Economic development* (11th ed.). Addison-Wesley.
- Ukhami, I., and S. Kumapayi.** 2023. "National interest and foreign policy in contemporary Africa." *African Journal of International Affairs* 9(1): 17-29.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

<https://buletinul.unap.ro/index.php/en/>

The Romanian Army's Confrontation with the Realities of Modern War: Lessons Learned from the Campaigns of 1913, 1916, and 1917

Ovidiu PĂDURARIU, PhD

*Doctoral School of Social and Human Sciences,
"Ștefan cel Mare" University of Suceava, Romania
e-mail: ovidiu.padurariu@yahoo.com

 <https://orcid.org/0009-0007-9174-6471>

Abstract

The article examines the Romanian Army's confrontation with the profound transformations of modern warfare during the period 1913-1917, focusing on the experiences acquired during the Second Balkan War and the campaigns of the First World War. The study explores the manner in which the Romanian army understood, assimilated, and attempted to apply the lessons learned from contemporary conflicts, emphasizing the complex relationship between the French-inspired military tradition that shaped Romanian doctrine and the emerging demands of industrialized warfare. Particular attention is devoted to the evolution of military organization, command structures, mobilization capacity, logistic support, operational doctrine, and the adaptation of tactical methods to the new realities of the modern battlefield, characterized by trench warfare, heavy artillery, machine guns, and increasingly sophisticated systems of communication and coordination. The analysis also highlights the limits of pre-war military thinking, the difficulties encountered during the 1916 campaign, and the process of institutional and operational adaptation that contributed to the Romanian Army's recovery and reorganization during the 1917 campaign.

Keywords:

Romanian Army; Modern Warfare; the 1913 Military Campaign; the 1916 Military Campaign; the 1917 Military Campaign; Military Doctrine; Learned Lessons.

Article info

Received: 11 April 2026; Revised: 30 April 2026; Accepted: 4 June 2026; Available online: 30 June 2026

Citation: Pădurariu, O. 2026. "The Romanian Army's Confrontation with the Realities of Modern War: Lessons Learned from the Campaigns of 1913, 1916, and 1917." *Bulletin of "Carol I" National Defence University*, 15(2): 129-160. <https://doi.org/10.53477/2284-9378-26-22>



© „Carol I” National Defence University Publishing House

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution ([CC BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/))

Introduction

The beginning of the twentieth century represented a period of accelerated transition for European armies, marked by technological, doctrinal, and organizational transformations that profoundly altered the character of warfare. The development of automatic weapons, the expansion of railway networks, the emergence of aviation, the growing importance of artillery, and the widespread use of field fortifications were among the key factors that transformed armed conflict into an industrialized form of warfare, characterized by total mobilization, attrition, and complex coordination.

In this context, the Romanian Army faced the challenge of adapting a military structure shaped by nineteenth-century models of warfare to the realities of modern conflict. The experiences gained during the campaigns of 1913, 1916, and 1917 constituted crucial stages in the process of doctrinal and operational maturation of the Romanian military institution.

The issue of the Romanian Army's adaptation to the demands of modern warfare constitutes one of the central themes in military historiography devoted to the early twentieth century. The technological and doctrinal transformations that took place in Europe following the Franco-Prussian War of 1870-1871 profoundly altered the nature of armed conflict, leading to the emergence of a new form of warfare characterized by mass mobilization, the extensive employment of artillery and machine guns, the increasing importance of logistics, and the integration of national economies into the military effort (Keegan 1999, 54-61). Within this context, European armies were compelled to redefine their command structures, operational doctrines, and systems of military training.

For Romania, the beginning of the twentieth century coincided with a period of regional affirmation and the consolidation of the institutions of the modern state. The Romanian Army, regarded as one of the principal pillars of national independence and sovereignty following the military campaign of 1877-1878, underwent an extensive process of reorganization and modernization. The military reforms initiated at the end of the nineteenth century sought to adapt the Romanian military system to Western models, particularly the French one, which was perceived as the most advanced expression of contemporary military art (Otu 2014, 27-31). Nevertheless, the modernization of the army progressed unevenly, constrained by insufficient economic resources, underdeveloped infrastructure, and administrative shortcomings. In 1907, General Alexandru Iarca addressed a letter to Ion I. C. Brătianu, requesting his intervention with King Carol I to remedy several serious deficiencies within the Romanian Army. In his memorandum, Iarca criticized the excessive allocation of resources to the fortification system at the expense of the field army, the inadequate defense of the Danube in comparison with that of Bulgaria, the insufficient preparation of the General Staff, shortcomings in command and training, the continued use of the Mannlicher Model 1893 rifle, which he considered

obsolete, as well as significant shortages of equipment and transportation assets. ([Iarca 1922](#), 95-97).

The 1913 campaign during the Second Balkan War constituted the first major test of general mobilization for the Romanian Army since the War of Independence. Romania's intervention against Bulgaria took place within a favorable strategic context, and military operations did not involve large-scale combat engagements. Nevertheless, the campaign revealed numerous logistical shortcomings, particularly in the field of medical services, as well as organizational deficiencies, demonstrating that the military institution was not yet fully prepared to meet the demands of modern warfare ([AMNR, General Staff Collection](#), file 45/1913). The cholera epidemic, supply difficulties, and coordination problems among military formations represented the first serious indications of the vulnerabilities affecting the Romanian military system. These shortcomings highlighted the gap between the army's formal organizational structure and its actual operational capabilities, emphasizing the need for comprehensive reforms in preparation, administration, and logistical support.

Despite the conclusions drawn after 1913, many of the lessons of the campaign were only partially implemented. Romania's political and military leadership continued to display considerable optimism regarding the army's ability to cope with a large-scale European conflict. Furthermore, the influence of French military doctrine, particularly its emphasis on the decisive offensive, contributed to the persistence of tactical concepts that were insufficiently adapted to the new realities of the battlefield ([Fuller 1961](#), 143-149).

Romania's entry into the First World War on 27 August/9 September 1916 marked the decisive confrontation between traditional military concepts and the realities of modern industrial warfare. The military campaign of 1916 dramatically exposed the limitations of the Romanian Army's operational and logistical preparedness. Although the initial offensive in Transylvania achieved a number of local successes, the rapid response of the Central Powers and the inability of the Romanian leadership to manage a war on two fronts resulted in a series of defeats and ultimately forced the army and the state administration to retreat to Moldavia ([Torrey 1998](#), 112-118). The events of 1916 demonstrated that modern warfare required far more than courage and high morale. Success depended on strategic coordination, technological superiority, efficient infrastructure, and effective cooperation among different branches of the armed forces. Deficiencies within the command structure, the shortage of heavy artillery, inadequate ammunition supplies, and logistic vulnerabilities all contributed decisively to the failure of the campaign. Moreover, the experience revealed the growing importance of industrial capacity and sustained resource mobilization, factors that increasingly determined military effectiveness in the age of total war. The setbacks of 1916 thus underscored the urgent need for comprehensive military reform and adaptation to the operational demands of twentieth-century warfare.

However, the defeat of 1916 did not signify the complete collapse of the Romanian Army. During the winter of 1916-1917, under the influence of the French Military Mission led by General Henri Mathias Berthelot, the army underwent an extensive process of reorganization and modernization ([Berthelot 1920](#), 301-317). Reforms in military training, improvements in infantry-artillery cooperation, the introduction of modern defensive methods, and the restoration of troop morale enabled the transformation of the army into a force capable of withstanding the offensives of the Central Powers.

The 1917 campaign, embodied in the battles of Mărăști, Mărășești, and Oituz, represented the culmination of the Romanian Army's adaptation to modern warfare. The Romanian Army demonstrated that the dramatic experiences of the previous year had been assimilated and transformed into valuable operational and tactical lessons ([Torrey 2011](#), 156-172). The resistance displayed during the summer of 1917 carried not only military significance but also profound political and moral importance, contributing to the survival of the Romanian state and reinforcing the ideal of national unity.

The experiences of the campaigns of 1913, 1916, and 1917 represented successive stages in the Romanian Army's confrontation with the realities of modern warfare. Although differing in scale and strategic context, these campaigns highlighted both the persistence of structural shortcomings and the army's capacity to learn and adapt. Therefore, a comparative analysis of these three campaigns makes it possible to trace the transformation of the Romanian Army into a military institution capable of operating under the conditions of industrialized and total warfare.

The present study is based on the premise that the issue of the Romanian Army's adaptation to the realities of modern warfare during the period 1913-1917 has been addressed only fragmentarily in historiography, primarily through separate analyses of individual military campaigns or of the political and diplomatic context of the era. In most studies, the 1913 campaign is treated as a secondary episode within the history of the Balkan Wars, the 1916 campaign is examined predominantly from the perspective of military defeat, while the year 1917 is associated almost exclusively with the heroic resistance displayed at Mărășești, Mărăști, and Oituz.

The absence of a comparative and integrated approach to these military experiences creates a significant gap in understanding the process of transformation undergone by the Romanian Army in the context of modern industrial warfare. From this perspective, the present research seeks to highlight the vulnerabilities as well as the doctrinal and organizational changes that characterized the Romanian Army between 1913 and 1917.

The main objective of this study is to analyze how the Romanian Army confronted the challenges of modern warfare and succeeded in adapting to the military transformations that shaped the early twentieth century.

In order to achieve the proposed aim, the following objectives were established: identifying the prime characteristics of modern warfare; analyzing the structural

vulnerabilities of the Romanian Army during the 1913 campaign; assessing the impact of the 1916 campaign on the Romanian military system; highlighting the doctrinal and operational transformations manifested during the 1917 campaign; and conducting a comparative analysis of the three military campaigns.

The study seeks to examine the relationship between military modernization, the administrative and logistic capacity of the state, the evolution of military doctrine, and the operational and tactical experiences of the battlefield. At the same time, the research analyzes the way how the transformations of European warfare influenced Romanian military structures and their capacity for adaptation.

The study employs a predominantly qualitative approach, characteristic of historical and military-historical research. The qualitative nature of the research derives from the analysis and critical interpretation of historical sources, archival documents, memoirs, operational journals, and specialized scholarly works. The investigation seeks to understand historical processes, institutional mechanisms, and the relationship among doctrine, organization, and the experience of modern warfare. Quantitative elements relating to troop strength, casualties, or military organization are used only as complementary evidence to support historical interpretation.

The research primarily employs an inductive line of reasoning. By examining specific military experiences – the campaigns of 1913, 1916, and 1917 – the study formulates broader conclusions regarding the Romanian Army's capacity to adapt to modern warfare. At the same time, the analysis makes selective use of deductive reasoning by relating the Romanian experience to the general characteristics of European warfare and to the doctrinal transformations of the period.

The research is structured around the following fundamental questions: To what extent was the Romanian Army prepared to meet the demands of modern warfare prior to the First World War? What structural vulnerabilities were revealed by the 1913 campaign? What were the main causes of the difficulties encountered during the 1916 campaign? Which doctrinal and operational transformations made it possible to achieve the defensive success in 1917? And to what extent do the campaigns under examination reflect the broader process of military and institutional modernization undertaken by the Romanian state?

The research is based on the critical analysis of historical sources and the application of the comparative method. The study draws upon archival documents, reports of the General Headquarters, military correspondence and memoirs, personal accounts, as well as scholarly studies and specialized works in the field of military history. The comparative method has enabled the identification of similarities and differences among the three campaigns, while also highlighting the evolution of Romanian military doctrine and organization. Furthermore, the historical and interpretative analysis seeks to place the experience of the Romanian Army within the broader context of the transformations that reshaped European warfare during the first decades of the twentieth century.

Modern Warfare and the Challenges of the Early Twentieth Century

The transformations that occurred in the military sphere during the late nineteenth and early twentieth centuries fundamentally altered the nature of armed conflict. Technological advancement, the industrialization of European economies, and the introduction of new combat equipment brought about a transition from the maneuver warfare characteristic of the nineteenth century to industrialized warfare of attrition, marked by total mobilization, massive resource consumption, and the involvement of entire societies in supporting the war effort ([Keegan 1999](#), 45-63).

For small and medium-sized states such as Romania, these developments posed a major challenge. Adaptation to modern warfare required not only the modernization of weaponry but also the development of infrastructure, the reorganization of military institutions, and the integration of the national economy into the system of national defense ([Stone 1998](#), 12-18).

Following the Franco-Prussian War of 1870-1871, the major European powers initiated extensive military reform programs. Prussia's victory demonstrated the importance of rapid mobilization, the effective use of railway networks, and close coordination between the general staff and operational units ([Dupuy 1977](#), 55-68). As a result, the German model of military organization became a significant point of reference for many European armies.

At the same time, technological progress transformed the conditions under which military operations were conducted. The introduction of repeating rifles, machine guns, and quick-firing artillery significantly increased the firepower of defensive positions ([Fuller 1961](#), 140-156). Under these circumstances, traditional frontal assaults became increasingly costly in terms of both manpower and resources.

The Russo-Japanese War of 1904-1905 represented another decisive moment in the evolution of modern military art. The conflict demonstrated the effectiveness of field fortifications, the importance of heavy artillery, and the critical role of logistics in sustaining a prolonged war ([Stevenson 2005](#), 35-42). European military observers noted that the success of military operations depended increasingly on the state's capacity to provide material support and organizational efficiency for its armed forces. The Balkan Wars of 1912-1913 offered a realistic preview of the character of the future European conflict. The intensive use of artillery, the high casualty rates, and the persistent difficulties of supply demonstrated that modern warfare had surpassed the limitations of the traditional conflicts of the nineteenth century ([Hall 2000](#), 119-138). These experiences underscored the growing importance of industrial resources, logistic planning, and operational coordination in determining military effectiveness on the battlefield.

Despite these lessons, many European states failed to fully implement the conclusions drawn from these conflicts. Military doctrines continued to place excessive emphasis

on offensive action and troop morale, while underestimating the strength of defensive positions and the growing importance of positional warfare. In France, the doctrine of the offensive à outrance ("offensive at all costs") promoted the belief that offensive spirit and determination could compensate for the technical superiority of defensive firepower (Strachan 2001, 162-170). This concept also exerted a significant influence on the Romanian Army.

Prior to 1914, most European states developed mobilization systems based on compulsory military service. Standing armies were reinforced by large reserve forces, enabling the mobilization of substantial numbers of troops (van Creveld 1977, 201-214). However, this expansion of military manpower generated new logistic and administrative challenges. At the same time, the growth of the armaments industry and the increasing consumption of ammunition highlighted the dependence of modern warfare on the economic capacity of the state. Military conflict thus became not merely a confrontation between armies, but also a contest between industrial and administrative systems.

The Romanian military system was organized based on compulsory military service and general mobilization. The model adopted closely followed the structure of the French Army, both in terms of unit organization and in its tactical concepts and officer training system (Otu 2014, 27-35). Nevertheless, the modernization of the military institution progressed unevenly. Romania possessed limited economic resources, while its domestic armaments industry remained underdeveloped. Consequently, the army relied heavily on imports of weapons and ammunition (Hitchins 2013, 255-263).

One of the main weaknesses of the Romanian military system was its insufficiently developed infrastructure. The railway network was relatively sparse compared to those of Western European states, and modern roads were limited in number, particularly in frontier regions. These deficiencies adversely affected the army's capacity for mobilization and supply (Torrey 1998, 51-57). Furthermore, both the logistic and medical support systems exhibited numerous vulnerabilities. Military exercises and maneuvers conducted before 1914 revealed significant difficulties related to troop transportation, ammunition distribution, and the organization of medical services (RNMA, Ministry of War Collection, file 212/1912).

The Focșani-Nămoloasa-Galați (F.N.G.) fortification system represented one of the most important components of Romania's defensive strategy at the end of the nineteenth century. Conceived in the context of the geopolitical transformations that followed the achievement of independence, this defensive complex was intended to block the main strategic corridor linking Eastern Europe with the interior of Romanian territory, commonly known as the "Focșani Gate." The construction of the fortifications reflected the concern of Romania's political and military leadership to adapt the army to the requirements of modern warfare and to strengthen the

state's defensive capabilities. Through the scale of the works, the complexity of its infrastructure, and the integration of artillery into the defensive system, the F.N.G. line corresponded to the broader European trends of the period regarding the organization of permanent defenses. At the same time, the rapid evolution of military technology and the development of heavy artillery reduced the strategic effectiveness of permanent fortifications at the beginning of the twentieth century (Pascu et al. 1988, 214-222). General Alexandru Iarca, in his capacity as Deputy Inspector General of the Romanian Army, argued – contrary to the views of King Carol I – that the fortification systems around Bucharest and along the F.N.G. line were of limited military value. In his opinion, these works required enormous financial expenditures, exceeding 100 million lei, without providing a genuine strategic advantage in relation to the most probable war scenarios facing Romania (Iarca 1922, 10-11).

At the doctrinal level, the Romanian Army was strongly influenced by French concepts emphasizing offensive action. Military regulations placed considerable emphasis on rapid attacks and troop morale, while assigning relatively limited importance to defensive organization and combined-arms cooperation (Ionescu 2002, 71-84). This doctrinal orientation would later have a negative impact on the conduct of the 1916 campaign. The officer corps was characterized by significant disparities in professional training and military education. A number of officers had pursued studies in France, Germany, or Austria-Hungary and were therefore familiar with the latest developments in European military doctrine (Rosetti 1926, 94-103). At the same time, however, many commanders had been shaped by a conservative military culture marked by formalism, rigidity, and adherence to traditional concepts of warfare. This coexistence of progressive and conservative tendencies within the officer corps limited the army's ability to develop a coherent and fully modern operational doctrine.

In 1903, there was a significant gap between Romania and the major European powers with regard to investments allocated to the maintenance and training of individual soldiers. The relatively low level of military expenditure reflected both the limited economic capabilities of the Romanian state and the difficulty of sustaining a comprehensive modernization process within a European environment increasingly characterized by military competition and an intensifying arms race. In countries such as Germany and France, the funds allocated per soldier were substantially higher, allowing for the development of modern military infrastructure, more effective training systems, and superior technical equipment. By contrast, the Romanian Army was compelled to operate under severe budgetary constraints, a situation that affected the pace of weapons procurement, the quality of military equipment, and the logistic capabilities of its forces. Although the political and military leadership initiated important reforms following the War of Independence, insufficient financial resources limited their overall effectiveness. Consequently, the disparity in financial expenditure per soldier reflected not only an economic imbalance but also

Romania's strategic vulnerability in comparison with the highly industrialized states of Europe. The problem of modernizing the Romanian Army cannot be interpreted solely from a military perspective; rather, it must be understood in relation to the general level of Romania's economic development at the beginning of the twentieth century. The limited capacity to finance the armed forces reflected the constraints of the national economy and the dependence of military reforms on the budgetary resources available to the state ([Pascu et al. 1988](#), 223-224).

Despite these limitations, the Romanian Army possessed several important advantages. Troop morale was high, and the military institution enjoyed considerable social prestige as well as strong political support. Moreover, the experiences of the Balkan Wars and observations of contemporary conflicts contributed to a growing awareness of the need for reform. The fundamental problem, however, lay in the insufficient pace of modernization. A significant gap existed between the technological evolution of European warfare and the capacity of Romanian institutions to adapt to these changes. The campaigns of 1913 and 1916 would later demonstrate, in dramatic fashion, the consequences of this disparity.

The 1913 Campaign: Between Political Success and Military Limitations

Romania's participation in the Second Balkan War constituted the first major test of the Romanian Army in the context of the military transformations taking place at the beginning of the twentieth century. Although the 1913 campaign unfolded within a favorable strategic environment and did not involve large-scale engagements with the Bulgarian Army, the experience nevertheless revealed significant shortcomings within the Romanian military system, particularly in the fields of logistics, medical services, and organization ([Torrey 1998](#), 44-49).

From a political perspective, Romania's intervention aimed to preserve the balance of power in the Balkan Peninsula and to prevent Bulgaria from emerging as the dominant regional power. Following the victory of the Balkan League over the Ottoman Empire in the First Balkan War (1912-1913), tensions among the former allies regarding the partition of Macedonia led to the outbreak of a new conflict during the summer of 1913 ([Hall 2000](#), 97-115). Romania took advantage of Bulgaria's diplomatic isolation and decided to intervene militarily in order to strengthen its strategic position and secure the acquisition of Southern Dobruja (the Quadrilateral) ([Hitchins 2013](#), 269-273).

The general mobilization of June 1913 represented the largest Romanian military concentration since the War of Independence. Within a relatively short period, approximately 400,000 soldiers were mobilized, demonstrating the administrative capacity of the Romanian state to rapidly organize substantial military forces ([Scurtu 2004](#), 60-64). The success of the mobilization was largely attributable to the

widespread popular enthusiasm and patriotic spirit displayed by the population in the context of Romania's participation in the Second Balkan War. At the same time, the mobilization served as a confirmation of the military reforms undertaken after the War of Independence and of the effectiveness of the army's recruitment and territorial organization system. However, the experience of 1913 also created the impression that the Romanian Army possessed a high degree of operational responsiveness and command efficiency. This perception significantly influenced both political and military assessments in the years preceding Romania's entry into the First World War, fostering a confidence that was not always fully supported by the army's actual operational and logistic capabilities (Pascu et al. 1988, 331-333).

Despite its apparent success, the mobilization revealed numerous structural deficiencies. The railway transportation capacity was insufficient, and the concentration of military units was carried out with considerable difficulty. The lack of a modern transportation infrastructure adversely affected both the pace of troop movements and the supply of military formations (RNMA, General Staff Collection, file 45/1913). Documents of the General Staff reveal significant problems related to the organization of transport convoys, the distribution of ammunition, and the coordination of transportation networks (RNMA, General Staff Collection, file 45/1913). In many cases, units lacked adequate means for transporting food supplies and equipment, while provisioning efforts were delayed by the poor condition of roads and the limited capacity of the railway system. These shortcomings highlighted the gap between the army's ability to mobilize large numbers of troops and its capacity to sustain them effectively in the field, a vulnerability that would become even more evident during the campaigns of the First World War.

Military operations commenced with the crossing of the Danube and the rapid advance into Bulgarian territory. The absence of organized Bulgarian resistance enabled Romanian troops to advance to the vicinity of Sofia without engaging in any major battles (Kirițescu 1989, 39-41). From a strategic perspective, the campaign was a success, contributing to the enhancement of Romania's regional prestige and facilitating the conclusion of the Treaty of Bucharest in August 1913 (Brătianu 1940, 22-27). At the same time, the military communications system remained insufficiently developed. The transmission of orders was often slow, adversely affecting coordination between units and limiting the command's ability to exercise effective control over military operations (Otu 2014, 31-36). These shortcomings highlighted the gap between the evolving requirements of modern warfare and the level of development of Romania's military infrastructure. In the context of a large-scale European conflict, such vulnerabilities could have had serious operational consequences.

The rapid success of operations created the impression that the Romanian Army possessed a high degree of efficiency. In reality, the absence of major engagements concealed numerous dysfunctions that would become far more apparent in

subsequent campaigns. The 1913 campaign demonstrated that the Romanian Army encountered serious difficulties in sustaining operations in the field. Even under conditions of limited enemy resistance, the supply of troops proved problematic ([Ionescu 2002](#), 82-89).

The most serious problem of the 1913 campaign was the cholera epidemic that broke out among Romanian troops. Poor sanitary conditions, the lack of potable water, and inadequate hygiene measures facilitated the rapid spread of the disease ([RNMA, Ministry of War Collection](#), file 212/1913).

The losses caused by the epidemic far exceeded those resulting from military engagements. This situation revealed the vulnerability of the military medical system and the inadequacy of logistic preparations for a large-scale campaign ([Hitchins 2013](#), 274-276).

Medical reports drafted after the campaign highlighted the shortage of medical personnel, the lack of medical supplies, the inefficient organization of the evacuation of sick soldiers, and the inadequate conditions prevailing in military camps ([RNMA, Army Medical Service Collection](#), file 18/1913). These findings underscored the fact that the Romanian Army's preparedness for modern warfare depended not only on combat capabilities but also on the effectiveness of its medical and logistic support systems, areas in which significant deficiencies remained evident.

General Alexandru Averescu emphasized in a report submitted to the Ministry of War that, although the army possessed substantial manpower and maintained a high level of morale, its infrastructure and the organization of its auxiliary services did not meet the requirements of a modern conflict ([Averescu 1991](#), 43-45).

Constantin Hârjeu, Minister of War between 1912 and 1914, was regarded as one of the principal figures responsible for the dysfunctions manifested during the 1913 campaign. General Alexandru Iarca highlighted the inadequacies of the Romanian Army's medical service, stressing the shortage of medication and the absence of effective measures to combat cholera during the Bulgarian campaign, despite the fact that the danger of an epidemic had been recognized before the commencement of military operations. Although sufficient time had been available for preparation, the necessary preventive measures were not implemented adequately. Furthermore, Hârjeu was criticized for advocating the practice of retaining the most capable officers in troop command positions rather than integrating them into staff structures, a policy that ran counter to the modern practices adopted by the leading European armies of the period ([Iarca 1922](#), 73-75). This approach limited the development of a highly professional General Staff and hindered the army's ability to improve operational planning and command efficiency, areas that would prove crucial in the conflicts that followed.

The 1913 campaign also exposed the limitations of the Romanian military command system. Although mobilization was carried out relatively rapidly, coordination between major formations and command structures was frequently deficient ([Ionescu 2002](#), 86-91). The absence of modern communications systems hindered

the transmission of orders and the exchange of information between headquarters. Moreover, the military exercises conducted prior to 1913 had not adequately prepared the army for large-scale operations ([Otu 2014](#), 34-36).

At the doctrinal level, the Romanian Army continued to be strongly influenced by French concepts emphasizing rapid offensive action and the offensive spirit of troops. Military regulations devoted relatively limited attention to logistic issues and combined-arms cooperation ([Fuller 1961](#), 149-153).

Differences in the professional training of officers were also evident. While part of the officer corps was familiar with the latest developments in modern European military doctrine, many commanders remained attached to traditional concepts characterized by formalism and rigidity ([Rosetti 1926](#), 94-103).

The absence of decisive military engagements contributed to the emergence of an overly optimistic perception of the Romanian Army's ability to cope with a major European conflict. In reality, the 1913 campaign had already revealed the existence of significant structural weaknesses. The apparent success of the operation tended to obscure these deficiencies, leading both political and military leaders to overestimate the army's level of preparedness. As subsequent events would demonstrate, many of the vulnerabilities identified in 1913 remained unresolved and would have serious consequences during the First World War.

Following the conclusion of military operations and the signing of the Treaty of Bucharest, the Romanian military leadership produced several reports assessing the experience of the campaign ([RNMA, Ministry of War Collection](#), file 212/1913). These documents emphasized the need for the accelerated modernization of the army and put forward recommendations concerning the development of railway infrastructure, the modernization of the military medical service, improvements in logistics, the expansion of modern artillery, the reorganization of the command system, and the enhancement of military communications ([RNMA, Ministry of War Collection](#), file 212/1913).

Nevertheless, many of the proposed reforms were implemented only partially. The rapid success of the campaign contributed to the persistence of a favorable perception regarding the overall effectiveness of the Romanian Army ([Torrey 1998](#), 49-52). Moreover, economic constraints and the absence of a modern domestic armaments industry limited the pace of modernization. A particularly significant issue was the continued adherence to a predominantly offensive doctrine inspired by the French model. The lessons concerning the importance of defense, artillery firepower, and logistics were insufficiently incorporated into Romanian military regulations and doctrine ([Fuller 1961](#), 154-158).

From a historical perspective, the 1913 campaign may be regarded as a transitional stage between the traditional wars of the nineteenth century and the total industrial

conflict of the 1914-1918 period. For the Romanian Army, the Balkan experience represented both a confirmation of Romania's regional status and a warning regarding the necessity of modernizing the military institution.

Paradoxically, it was precisely the absence of decisive military engagements that contributed to an underestimation of the true challenges posed by modern warfare. The logistic, medical, and organizational vulnerabilities observed in 1913 would reappear in a much more severe form during the 1916 campaign.

The 1916 Campaign: Confrontation with Industrial Warfare

Romania's entry into the First World War on 27 August/9 September 1916 marked the decisive moment of confrontation between the Romanian Army and the realities of modern industrial warfare. While the experience of the 1913 campaign had provided only limited indications of the vulnerabilities within the Romanian military system, the campaign of 1916 dramatically demonstrated the incompatibility between the traditional concepts embraced by the military leadership and the total character of the European conflict ([Torrey 1998](#), 112-118).

Modern warfare required economic mobilization, technological superiority, combined-arms coordination, and extensive logistic capabilities. Under these conditions, the Romanian Army, still undergoing an incomplete process of modernization, faced major difficulties in conducting large-scale operations against opponents who were more experienced, better organized, and more effectively equipped ([Keegan 1999](#), 198-205).

The 1916 campaign exposed structural weaknesses at the levels of command, logistics, equipment, and operational doctrine. At the same time, the dramatic experience of the retreat into Moldavia created the conditions for the subsequent reorganization of the army and its adaptation to the new realities of industrial warfare.

Romania's neutrality between 1914 and 1916 was determined by the complexity of the international situation and by the need for military and diplomatic preparation on the part of the state ([Hitchins 2013](#), 280-287). Within political and military circles, divergent opinions existed regarding both the desirability of entering the war and the strategic orientation that Romania should adopt.

General Alexandru Iarca argued that Romania lacked the material and human resources necessary to sustain a prolonged conflict and to replace the inevitable losses that such a war would entail. In light of the country's financial and geographical limitations, he believed that Romania's entry into the First World War should be postponed for as long as possible in order to avoid strategic isolation and the concentration of superior enemy forces against the country. In support of this assessment, Iarca referred to plans developed by the Central Powers for potential attacks against Romania during 1915-1916. At the same time, he maintained that he had consistently advised Ion I. C. Brătianu to avoid premature intervention until the

launch of a general Allied offensive. Nevertheless, Iarca considered that once such an Allied offensive had begun, Romania was obliged to enter the war regardless of its own level of preparedness, accepting even the possibility of major sacrifices in pursuit of its national objectives (Iarca 1922, 140-141).

The political and military convention signed with the Entente in August 1916 formalized Romania's entry into the war against Austria-Hungary in exchange for the recognition of Romanian claims to Transylvania, the Banat, and Bukovina (Brătianu 1940, 45-59). The Romanian political leadership considered the moment favorable, given the difficulties encountered by the Central Powers on other fronts.

The campaign plan developed by the Romanian General Headquarters envisaged a main offensive in Transylvania while maintaining a defensive posture on the southern front (Kirițescu 1989, 126-141). Romanian strategy was based on the concept of a rapid advance through the Carpathian passes and the occupation of key objectives before the Central Powers could concentrate sufficient forces for a counteroffensive. Romanian strategic thinking was strongly influenced by the French doctrine of the decisive offensive. It was believed that the offensive spirit of the troops and the speed of operations could compensate for material and organizational shortcomings (Fuller 1961, 149-163). In reality, however, the European war had already demonstrated the effectiveness of organized defense, artillery firepower, and modern defensive systems. The experience of the Western and Eastern Fronts showed that success increasingly depended on sustained logistic support, coordination among different arms of service, and the ability to concentrate overwhelming firepower rather than on offensive determination alone. Consequently, some of the assumptions underlying Romanian strategic planning in 1916 were already out of step with the evolving realities of industrial warfare.

The Romanian plan failed to fully take into account the challenges of fighting a war on two fronts and underestimated the Central Powers' capacity for rapid reaction and force concentration. Furthermore, cooperation with the Russian Army was constrained by divergent strategic objectives and persistent difficulties in achieving effective coordination between the allied commands (Stone 1998, 217-225).

The 1916 campaign exposed numerous structural vulnerabilities within the Romanian Army, stemming from the incomplete modernization of the military institution and the limited resources available to the Romanian state (Ionescu 2002, 98-112). These weaknesses became evident at every level of military activity, from strategic planning and command organization to logistics, communications, and battlefield support. The campaign demonstrated that, despite the reforms undertaken in previous decades, the Romanian military system remained insufficiently prepared to meet the demands of a large-scale industrial war against well-equipped and experienced opponents.

- **Insufficient Equipment.** One of the most serious problems was the shortage of modern weaponry. The Romanian Army possessed a relatively small number of

machine guns and heavy artillery pieces compared to the armies of the Central Powers (Stroea and Băjenaru 2010, 92-103). Ammunition stocks were inadequate for sustaining a prolonged conflict, while domestic arms production was incapable of meeting the requirements of military operations. Numerous units entered combat with incomplete equipment and limited ammunition reserves (AMNR, General Headquarters Collection, file 178/1916). Furthermore, Romanian military aviation was still at an early stage of development, and modern communications equipment remained insufficient. In the context of industrial warfare, these deficiencies significantly reduced operational effectiveness and limited the army's capacity for coordination and command. The costs associated with the reorganization and re-equipment of the Romanian Army for the 1917 campaign, estimated at approximately 1.6 billion lei, exceeded by more than three times Romania's total annual state budget for the years 1913-1914, which amounted to roughly 500 million lei (Pascu et al. 1988, 500-502). This disparity illustrates the economic limitations of the Romanian state and helps explain the major difficulties encountered during the 1916 campaign. Under these circumstances, the deficiencies in armaments, ammunition, equipment, and logistics cannot be interpreted solely as the result of command failures. They must also be understood as manifestations of the Romanian state's limited capacity to sustain the material and financial demands of modern industrial warfare.

- **Logistic Vulnerability.** Logistics constituted one of the most significant weaknesses of the Romanian Army. The inadequately developed railway network and the poor state of road infrastructure severely hindered both the supply system and the rapid movement of troops (van Creveld 1977, 201-214). The transportation of artillery and ammunition was carried out with considerable difficulty, while the absence of modern storage facilities disrupted the continuity of supply operations. In many instances, frontline units did not receive ammunition, food, or equipment in a timely manner (RNMA, General Staff Collection, file 221/1916). These logistical deficiencies became even more pronounced in the context of simultaneous military operations conducted in Transylvania and Dobruja. The Romanian Army lacked the resources necessary to sustain an effective war effort on two fronts.

- **Command and Coordination Problems.** The command structure proved insufficiently adapted to the conditions of modern warfare. Coordination between armies and army corps was frequently deficient, while the transmission of orders was often slow and inefficient (Otu 2017, 74-83). The absence of an effective unity of command and the difficulties associated with the flow of information reduced the operational leadership's ability to respond rapidly to changes in the tactical situation. Furthermore, disparities in the professional competence and training of commanders negatively affected the coherence of military operations. Differences in experience, doctrinal outlook, and decision-making often resulted in inconsistent execution of operational plans and hindered effective cooperation between formations. General Constantin Prezan later observed that one of the main weaknesses of the Romanian Army in 1916 was the inability of its command structure to adapt initial plans to the rapidly evolving operational situation (Prezan 1995, 74-79).

• **The Limitations of Offensive Doctrine.** The Romanian military leadership continued to be strongly influenced by French doctrinal concepts emphasizing rapid offensive action and the morale of troops (Strachan 2001, 162-170). Military regulations devoted insufficient attention to organized defense, combined-arms cooperation, and the systematic employment of artillery fire. The experience of the Western Front had already demonstrated that frontal assaults against well-prepared defensive positions resulted in enormous casualties. The growing effectiveness of machine guns, heavy artillery, and entrenched defensive systems had fundamentally altered the balance between offense and defense. Nevertheless, the Romanian Army failed to fully incorporate the lessons of modern warfare into its doctrine, training, and operational planning.

During the first weeks of the campaign, Romanian troops achieved a number of local successes in Transylvania. The advance through the Carpathian passes proceeded relatively rapidly, and the Romanian population of the province welcomed the army favorably (Torrey 2011, 71-86). However, the Romanian offensive was gradually slowed down by logistic difficulties and the lack of sufficient reserves to sustain continued operations. At the same time, the German High Command reacted swiftly by transferring experienced troops under the command of General Erich von Falkenhayn (Dupuy 1977, 187-194). Simultaneously, Field Marshal August von Mackensen organized the German-Bulgarian offensive in Dobruja. The attack on Turtucaia resulted in a severe defeat for the Romanian Army and had a profound impact on both troop morale and public opinion (Kirilescu 1989, 214-223). The defeat at Turtucaia demonstrated the vulnerability of the Romanian defensive system and the absence of effective coordination between the different fronts. Moreover, it compelled the Romanian military leadership to transfer substantial forces from Transylvania to the southern front, thereby reducing the strength and momentum of the main offensive. This strategic diversion of resources contributed significantly to the loss of the initiative and facilitated the subsequent counteroffensives launched by the Central Powers.

General Alexandru Iarca argued that the fortified positions at Turtucaia and Silistra should not have been defended during the 1916 campaign, maintaining that the preservation of such fortifications could not justify weakening the field army. In his view, these positions possessed limited strategic value and, because of their exposed and peripheral location, could not be effectively integrated into the army's overall operational maneuver. Iarca further contended that the relatively small garrisons stationed there lacked the capacity to conduct significant offensive actions against enemy lines of communication. Drawing upon military experience, he emphasized that troops confined within fortifications risked being surrounded and destroyed, as had occurred at Turtucaia. He also believed that subordinating the maneuver of the field army to the defense of fixed positions restricted the freedom of action of the high command and imposed rigidity upon the operational deployment of forces. According to Iarca, the supply and transportation of troops across the Danube could

have been organized through alternative logistic centers, such as Cernavodă, without the need to maintain these bridgeheads. Given that Romania's main strategic effort was concentrated in Transylvania, he argued that the forces deployed in Dobruja should have been reduced to the minimum necessary level. In his assessment, the immobilization of substantial numbers of troops in the garrisons of Turtucaia and Silistra contributed directly to the weakening of the Romanian field army. Iarca ultimately concluded that the abandonment of the original plan to withdraw from Dobruja and the adoption of a predominantly defensive strategy facilitated the disaster at Turtucaia. The defeat resulted in considerable human and material losses, undermined the morale of the army, and diminished Romania's military prestige (Iarca 1922, 153-157).

In the autumn of 1916, the offensive launched by the Central Powers forced the gradual withdrawal of the Romanian Army from Transylvania and Wallachia (Hitchins 2013, 288-295). The enemy's technical and organizational superiority, combined with the Romanian Army's logistic and command deficiencies, contributed to the rapid deterioration of the strategic situation. Bucharest was occupied on 6 December 1916, and the government, the royal family, and a large part of the state administration withdrew to Moldavia (Scurtu 2004, 71-79). The situation of the Romanian state had become critical, while the army faced heavy losses, material shortages, and declining morale.

The retreat highlighted the difficulties of conducting a modern war in a state with insufficiently developed infrastructure. Congested roads, the shortage of transportation assets, and adverse weather conditions severely affected the movement of both troops and civilians (AMNR, General Headquarters Collection, file 245/1916). These challenges demonstrated the extent to which military operations in the age of industrial warfare depended upon efficient transportation networks and administrative capacity. Nevertheless, the Romanian Army did not collapse completely. The core of its combat forces succeeded in withdrawing to Moldavia and preserving the continuity of military resistance. This capacity for institutional survival proved crucial, as it created the conditions necessary for the subsequent reorganization of the army in 1917. Despite the severity of the defeats suffered during the campaign, the preservation of a functioning military structure enabled Romania to remain in the war and laid the foundation for the military recovery that would follow.

General Alexandru Iarca explained the disaster of the 1916 campaign through a series of structural deficiencies within the Romanian Army, placing at the center of his analysis the absence of clear strategic foresight and a coherent war objective. In his view, this fundamental weakness was reflected in a flawed military organization and in a command structure incapable of effectively coordinating military operations. Iarca also criticized the unrealistic character of Romania's war plans and the inadequate level of troop training, particularly among reserve formations,

which were insufficiently prepared for the demands of modern warfare. In his assessment, tactical factors and material shortages were of secondary importance when compared to deficiencies in military strategy and leadership. Referring, among others, to views associated with General Alexandru Averescu, Iarca argued that the “new tactics” of modern warfare had not yet been fully defined and that shortages of modern equipment alone could not explain the scale of the defeat. He therefore concluded that the failure of the Romanian Campaign of 1916 resulted primarily from fundamental shortcomings in organization, training, and command. These deficiencies severely undermined the Romanian Army’s ability to conduct effective operations and to respond adequately to the challenges posed by industrial warfare (Iarca 1922, 230).

The 1916 campaign represented the most dramatic military experience in Romania’s history up to that point. It demonstrated that modern warfare required not only military mobilization but also economic capacity, administrative organization, and doctrinal adaptation (Stevenson 2005, 421-429).

The defeats suffered during the campaign exposed the limitations of the Romanian state’s incomplete modernization and highlighted the incompatibility between traditional military concepts and the realities of industrial warfare. At the same time, however, the experience of 1916 created the conditions necessary for the subsequent transformation of the Romanian Army.

From a historiographical perspective, the 1916 campaign should be interpreted not merely as a sequence of military defeats, but also as the decisive moment in the confrontation between the institutions of the Romanian state and the demands of modern warfare. The lessons derived from this experience would profoundly influence the reorganization of the army and the evolution of Romanian military doctrine in the following year.

The Reorganization of the Romanian Army and the 1917 Campaign

The defeats suffered by the Romanian Army during the 1916 campaign revealed the limitations of the Romanian military system when confronted with the realities of modern industrial warfare. Nevertheless, the retreat into Moldavia and the preservation of the army’s principal combat nucleus created the conditions for an extensive military reorganization carried out during the winter of 1916-1917 (Torrey 2011, 145-156).

The process of rebuilding the Romanian Army took place under extremely difficult circumstances. A large portion of the national territory was occupied by the Central Powers, the economy was in a critical condition, and the civilian population was affected by displacement, famine, and epidemics (Hitchins 2013, 295-302). Despite these challenges, the political and military leadership, with the support of the Western Allies, succeeded in reorganizing the army and transforming it into

a force capable of resisting the German and Austro-Hungarian offensives of the summer of 1917.

The 1917 campaign represented the culmination of the Romanian Army's adaptation to the realities of modern warfare. The defensive victories at Mărăști, Mărășești, and Oituz demonstrated that the painful lessons of 1916 had been assimilated and transformed into valuable doctrinal and operational experience ([Kirițescu 1989](#), 233-267). These successes reflected not only improvements in military organization and training but also a broader institutional capacity to learn from defeat and adapt to the demands of industrialized conflict.

Following the occupation of Bucharest and the retreat into Moldavia, the Romanian state faced one of the most severe crises in its modern history. Approximately two-thirds of the national territory was under enemy occupation, while the administration, industry, and economic resources had been profoundly disrupted ([Scurtu 2004](#), 80-85). Under these circumstances, the reconstruction of the army became an essential prerequisite for the survival of the Romanian state. The process of military reorganization was coordinated by the Romanian General Headquarters under the leadership of General Constantin Prezan and benefited from the direct support of the French Military Mission headed by General Henri Mathias Berthelot ([Prezan 1995](#), 91-102).

The main objectives of the reorganization were the restoration of combat strength, the modernization of military training, the restructuring of the command system, the improvement of cooperation among the different branches of the armed forces, the re-equipment of the army with modern weaponry, and the enhancement of the defensive capabilities of the Moldavian front ([Otu 2017](#), 104-119). These measures sought not merely to replace the losses suffered in 1916 but to create a more effective and adaptable military force capable of meeting the operational requirements of modern industrial warfare.

The reorganization process was carried out simultaneously with efforts to restore troop morale and to rebuild the army's logistic and medical support systems. A decisive role in the reorganization of the Romanian Army was played by the French Military Mission, which arrived in Romania at the end of 1916. General Henri Berthelot and his collaborators contributed significantly to the modernization of military training and to the adaptation of Romanian doctrine in accordance with the lessons of the Western Front. French officers participated in the reorganization of major formations, the development of new training programs, the instruction of Romanian officers, the restructuring of the artillery arm, and the improvement of medical and logistic services ([Cristescu 2010](#), 201-219).

The French Military Mission placed particular emphasis on cooperation between infantry and artillery, the organization of defense in depth, and the effective employment of artillery fire. These principles represented a significant departure

from the predominantly offensive doctrine that had influenced the Romanian Army before 1916. At the same time, France and the other Allied powers supplied Romania with modern weapons, ammunition, and equipment, thereby contributing to the restoration of the army's combat effectiveness ([RNMA, General Headquarters Collection](#), file 312/1917). General Henri Berthelot later observed that one of the major strengths of the Romanian soldier was his remarkable capacity for endurance and adaptation under difficult conditions ([Berthelot 1920](#), 328-331). This resilience, combined with the organizational and doctrinal reforms implemented during the winter of 1916-1917, became a crucial factor in the recovery of the Romanian Army and its subsequent performance during the campaigns of 1917.

The experiences of the 1916 campaign brought about significant changes in the doctrine and training system of the Romanian Army. The lessons of modern warfare highlighted the necessity of abandoning concepts based exclusively on frontal offensives and the offensive spirit of the troops ([Strachan 2001](#), 241-248). The new regulations and training programs emphasized combined-arms cooperation, the effective employment of artillery, the defensive organization of terrain, the construction of field fortifications, the use of concentrated firepower, and the tactical flexibility of military units ([Ionescu 2002](#), 121-133).

The training of both soldiers and officers became more realistic and better adapted to the conditions of the modern battlefield. Tactical exercises focused on coordination among different branches of the armed forces and on preparing troops for the defense of fortified positions. Greater attention was also devoted to communications and military intelligence systems. The Romanian command increasingly recognized that the success of military operations depended to a large extent on the speed of information transmission and on effective coordination between units ([RNMA, General Staff Collection](#), file 355/1917).

The reorganization of the army was not limited to technical and organizational measures; it also possessed an important moral and psychological dimension. The defeats of 1916 had profoundly affected the morale of both the troops and the civilian population ([Torrey 1998](#), 173-181). Consequently, the military and political leadership sought to restore the fighting spirit of the nation through improved supply conditions, strengthened discipline, intensified patriotic propaganda, and the promotion of the ideals of national defense and state survival ([Hitchins 2013](#), 303-307).

The presence of King Ferdinand I and Queen Marie near the front lines had a significant positive impact on the morale of the army. Their visible commitment to the national cause served as a source of encouragement for both soldiers and civilians during one of the most critical periods in Romania's history. Furthermore, promises concerning agrarian reform and the extension of political rights contributed to strengthening the loyalty and motivation of the soldiers, many of whom viewed the war not only as a struggle for national survival, but also as a means of achieving important social and political reforms ([Marie, Queen of Romania 2014](#), 92-105).

The Mărăști Offensive, conducted in July 1917, represented the first major success of the reorganized Romanian Army ([Kirițescu 1989](#), 268-289). The operation, coordinated by General Alexandru Averescu, aimed to break through the Austro-Hungarian front and improve the strategic position of the Romanian and Russian forces. The preparation of the offensive demonstrated the progress achieved in operational planning and combined-arms cooperation. Artillery was employed systematically to destroy enemy positions and to support the advance of the infantry, reflecting the doctrinal and tactical lessons learned from the previous year's campaign ([Averescu 1991](#), 167-182). Careful coordination between different branches of the armed forces and the concentration of firepower played a crucial role in the success of the operation. The victory at Mărăști possessed both significant military and psychological importance. It demonstrated that the Romanian Army had become capable of conducting modern military operations and of effectively applying the experience gained during the difficult campaign of 1916. Moreover, the success strengthened the confidence of both the troops and the military leadership, providing tangible evidence that the reforms implemented during the winter of 1916-1917 had substantially improved the army's combat effectiveness.

The Battle of Mărășești, fought between July and August 1917, was the most important military engagement undertaken by the Romanian Army during the First World War ([Torrey 2011](#), 187-209). The offensive launched by the Central Powers aimed at destroying the Romanian and Russian forces in Moldavia and permanently eliminating Romania from the war. Under these circumstances, the defense of the Mărășești front acquired decisive strategic importance ([Stone 1998](#), 287-296). The Romanian Army made effective use of defense in depth, field fortifications, infantry-artillery cooperation, local counterattacks, and the mobility of tactical reserves ([Otu 2017](#), 132-141).

Simultaneously with the fighting at Mărășești, Romanian troops repelled the Austro-Hungarian offensive in the Oituz sector. The mountainous terrain and difficult combat conditions tested the army's capacity for endurance and adaptation. The defense at Oituz highlighted the importance of the initiative displayed by local commanders and the effectiveness of defensive organization. Romanian troops utilized fortified positions and rugged terrain to block the enemy's advance ([RNMA, Second Army Collection](#), file 88/1917). The resistance at Oituz contributed decisively to the preservation of the Moldavian front and prevented the occupation of the last unoccupied part of Romanian territory.

Despite these defensive successes, the reorganization of the Romanian Army did not eliminate all the structural problems that had existed before the war. Romania continued to depend on Allied support for weapons and ammunition, while the national economy remained severely affected by the occupation of much of the country by the Central Powers ([Hitchins 2013](#), 308-312). At the same time, the international situation became increasingly difficult following the Russian Revolution of 1917 and the collapse of the Eastern Front. Under these circumstances, Romania found itself strategically isolated ([Stevenson 2005](#), 501-514).

Nevertheless, the 1917 campaign demonstrated the Romanian Army's capacity to learn from experience and adapt to the realities of industrial warfare. The contrast between the army's performance in 1916 and its achievements in 1917 highlighted the importance of doctrinal, logistic, and operational reorganization.

From a historical perspective, the 1917 campaign represents the moment at which the Romanian Army succeeded, at least partially, in overcoming the structural limitations that had been revealed in 1913 and 1916. The resistance in Moldavia possessed fundamental military, political, and symbolic significance for the survival of the Romanian state and for the subsequent realization of Greater Romania. It demonstrated that, despite severe setbacks and material constraints, the Romanian military institution was capable of adapting to the demands of modern warfare and preserving the conditions necessary for the achievement of the nation's political objectives.

The Armistice of Focșani, signed on 26 November/9 December 1917, must be understood within the context of the radical transformations that occurred on the Eastern Front following the Bolshevik coup in Petrograd on 25 October/7 November 1917. The seizure of power by the Bolsheviks under the leadership of Vladimir Lenin, together with the new regime's determination to conclude a separate peace with the Central Powers, led to the disintegration of the Russian Front and the strategic isolation of Romania. Under these circumstances, the continuation of the war became extremely difficult from both a military and a logistic perspective. In his memoirs, General Alexandru Averescu recounted that, following the Crown Council of 18 February 1918, during which King Ferdinand I read the declaration accepting peace, he convened a meeting with the Council of Ministers attended by Generals Constantin Prezan, Artur Văitoianu, Eremia Grigorescu, and Constantin Zaharia to examine the possibility of resuming military operations. Although Generals Eremia Grigorescu and Artur Văitoianu argued in favor of continuing armed resistance, the decisive assessment was provided by General Constantin Zaharia, who, after evaluating the logistic situation, concluded that "resistance is a utopia" (Averescu 1937, 298-299). This assessment highlights the decisive role played by logistics in shaping the political and military decisions of the Romanian leadership. Consequently, Romania's temporary withdrawal from the war cannot be interpreted solely as a consequence of the operational situation on the battlefield. Rather, it must be understood in relation to the collapse of the Allied system in the East and the material impossibility for the Romanian Army to sustain a prolonged conflict under conditions of strategic isolation.

The armistice with the Central Powers, signed at Focșani on 26 November/9 December 1917, generated mixed reactions among the Entente powers, many of which refused to accept the arguments advanced by Romania to justify the suspension of hostilities. Although the decision of the Romanian authorities was dictated by the extremely difficult military and political circumstances created by the disintegration of the Russian Army and Romania's isolation on the Eastern Front, the Western Allies viewed the armistice with considerable reservation, regarding it as a weakening of the common front against the Central Powers.

Comparative Analysis of the Military Campaigns of 1913, 1916, and 1917

The comparative analysis of the military campaigns conducted by the Romanian Army in 1913, 1916, and 1917 makes it possible to highlight the transformations that occurred in the structure, doctrine, and operational capabilities of the Romanian military institution in the context of modern warfare. Although these campaigns took place under different political and military circumstances, they reveal both elements of continuity and significant differences with regard to army organization, the conduct of operations, and the degree of adaptation to the realities of industrial warfare (Torrey 1998, 41-52).

The 1913 campaign constituted the first major test of the Romanian military system since the War of Independence; however, the absence of decisive military engagements limited the operational significance of the experience. While the campaign exposed the structural vulnerabilities of the Romanian Army, the events of 1917 demonstrated the institution's capacity for reorganization and adaptation (Otu 2017, 65-83).

A comparison of these three military experiences allows for a deeper understanding of the gradual process through which the Romanian Army evolved from the traditional concepts of nineteenth-century warfare toward forms of organization and military action more characteristic of modern industrial conflict.

- **Persistence of Logistic Problems.** One of the most significant continuities among the three campaigns was the logistic vulnerability of the Romanian Army. In each case, the inadequately developed infrastructure and the limited capacity of the railway network adversely affected mobilization, troop movements, and supply operations (van Creveld 1977, 201-214). In 1913, difficulties related to transportation and the organization of supply convoys hampered operations in Bulgaria, even in the absence of major combat engagements (RNMA, General Staff Collection, file 45/1913). In 1916, these problems manifested themselves in a far more severe form, undermining the army's ability to sustain simultaneous operations in Transylvania and Dobruja (Kirițescu 1989, 214-223). Although the reorganization of 1917 brought partial improvements to the logistic system, difficulties concerning the supply of ammunition, equipment, and food continued to exist. Romania remained dependent on Allied assistance and on the limited infrastructure available in Moldavia (Hitchins 2013, 303-307). The persistence of these logistic shortcomings demonstrates that military modernization could not be separated from the broader economic and administrative development of the Romanian state.

- **The Influence of Political Factors on Military Decision-Making.** In all three campaigns, military decisions were strongly influenced by political and diplomatic considerations (Brătianu 1940, 22-59). In 1913, Romania's intervention against Bulgaria was primarily intended to strengthen the country's regional position and

secure the acquisition of Southern Dobruja (the Quadrilateral) (Hall 2000, 119-138). As a result, the campaign possessed a predominantly political and strategic character rather than a purely military one. In 1916, Romania's entry into the war on the side of the Entente was determined both by national objectives related to the unification of Transylvania with Romania and by the pressures of the international context (Torrey 2011, 71-86). The Romanian political leadership considered the moment favorable for achieving the national ideal, despite the fact that the army was not fully prepared for a large-scale conflict. In 1917, the resistance in Moldavia carried not only military significance but also profound political and symbolic importance. The preservation of the front was essential for the survival of the Romanian state and for maintaining the political legitimacy of both the government and the monarchy (Scurtu 2004, 80-92). Thus, in all three campaigns, political considerations exerted a substantial influence on the planning and conduct of military operations.

• **Command and Coordination Deficiencies.** Problems related to command and coordination constituted another recurring feature of the Romanian military experience between 1913 and 1917 (Ionescu 2002, 82-133). During the 1913 campaign, the absence of modern communications systems and the difficulties encountered in coordinating major formations revealed significant limitations in operational leadership (RNMA, Ministry of War Collection, file 212/1913). In 1916, these deficiencies produced far more serious consequences. The lack of effective coordination among Romanian armies and the inability of the command structure to adapt rapidly to the changing operational situation contributed significantly to the failure of the campaign (Prezan 1995, 74-79). Weaknesses in planning, communication, and decision-making reduced the army's capacity to respond effectively to the initiatives of the Central Powers. Although Romanian military leadership improved considerably in 1917, problems concerning the transmission of orders and inter-service coordination did not disappear entirely (RNMA, General Headquarters Collection, file 312/1917). Nevertheless, the experience accumulated during the previous campaigns, together with the assistance provided by the French Military Mission, enabled the Romanian Army to mitigate many of these vulnerabilities.

• **Morale and Endurance.** Throughout all three campaigns, the morale and endurance of the Romanian soldier constituted essential factors in military effectiveness. In 1913, the army demonstrated discipline and a capacity for rapid mobilization. In 1916, although the campaign ended in retreat and substantial losses, the army did not collapse completely and succeeded in preserving the continuity of military resistance. In 1917, the morale of the reorganized troops became one of the principal factors behind the defensive successes achieved at Mărășești and Oituz (Averescu 1991, 167-182). This continuity highlights the fact that, despite the structural deficiencies of the military institution, the Romanian soldier possessed a remarkable capacity for adaptation and endurance under difficult conditions.

- **Intensity of the Conflict.** The most evident difference among the three campaigns lies in the scale and intensity of the conflict. The 1913 campaign took place in a strategic environment favorable to Romania and did not involve major military engagements. Operations were limited in scope, and success was achieved rapidly with relatively modest military effort. By contrast, the campaigns of 1916 and 1917 were conducted within the broader context of the First World War, a conflict characterized by total mobilization, the massive employment of artillery, and extremely high human losses ([Stevenson 2005](#), 421-429). The operational environment was considerably more complex, requiring sustained logistic support, large-scale coordination, and the effective integration of modern weapons systems. If 1916 represented Romania's first direct confrontation with the realities of industrial warfare, 1917 demonstrated the Romanian Army's capacity to operate effectively within a modern, high-intensity conflict.

- **Doctrinal Adaptation.** The differences among the three campaigns also reflect the evolution of Romanian military doctrine. In 1913, the army remained strongly influenced by the traditional concepts of maneuver warfare and rapid offensive action. The absence of decisive engagements prevented a full understanding of the lessons of modern warfare ([Otu 2014](#), 31-36). In 1916, the predominantly offensive doctrine proved insufficiently adapted to the conditions of industrial warfare. The Romanian Army had not yet fully incorporated the lessons emerging from the Western Front concerning the importance of artillery, field fortifications, and defense in depth. As a result, many operational concepts remained rooted in pre-war assumptions that underestimated the growing significance of firepower and defensive organization. By contrast, 1917 witnessed a significant doctrinal transformation. The reorganization of the army and the influence of the French Military Mission encouraged the development of combined-arms cooperation and the adaptation of defensive tactics to the realities of modern conflict ([Cristescu 2010](#), 201-219).

- **Quality of Command.** Another important point of differentiation is the evolution of the army's operational leadership. In 1913, the limitations of the command structure did not produce serious consequences because of the limited nature of the military engagements. In 1916, however, difficulties in operational coordination and the inability to adapt rapidly to enemy initiatives contributed decisively to Romania's defeat ([Kirițescu 1989](#), 214-223). By 1917, the experience gained during the previous campaign and the reorganization of the command system had enabled a far more effective form of military leadership. Generals Constantin Prezan, Alexandru Averescu, and Eremia Grigorescu demonstrated a superior capacity for coordination, decision-making, and adaptation to the evolving conditions of the battlefield.

- **The Army and Society.** The campaigns under analysis also highlight the evolution of the relationship between the army and Romanian society. In 1913, the war had only a limited impact on the civilian population, and military operations were

perceived primarily as an affirmation of Romania's regional prestige (Scurtu 2004, 60-64). The conflict remained largely confined to the military sphere and did not fundamentally alter the everyday life of most citizens. In contrast, the campaigns of 1916 and 1917 involved the mobilization of society as a whole. The occupation of a large part of the country, the withdrawal of the government and administration to Moldavia, the economic crisis, and the heavy human losses transformed the war into a profound collective experience (Marie, *Queen of Romania* 2014, 92-105). The distinction between the military and civilian spheres became increasingly blurred as the demands of total war affected every aspect of national life. At the same time, the army emerged as the principal symbol of national resistance and of the hope for achieving political and territorial unity.

Viewed comparatively, the campaigns of 1913, 1916, and 1917 illustrate the broader process through which the Romanian Army adapted to the requirements of modern warfare. The 1913 campaign served as a warning – insufficiently understood at the time – regarding the logistic and organizational vulnerabilities of the Romanian military system. The campaign of 1916 exposed the limitations of incomplete modernization and the shortcomings of traditional military doctrine. By contrast, the experience of 1917 confirmed the capacity of the Romanian military institution to learn, adapt, and transform itself in response to the challenges of industrial warfare. Accordingly, these three campaigns should be analyzed as interdependent stages in the process of military modernization and Romania's integration into the paradigm of European industrial warfare. Taken together, they reveal a gradual evolution from a military system shaped by nineteenth-century assumptions toward one increasingly capable of operating within the complex realities of twentieth-century total war.

The analysis of the Romanian Army's confrontation with the realities of modern warfare between 1913 and 1917 extends beyond a strictly historical dimension and offers a number of conclusions relevant to the understanding of contemporary operational challenges. The military transformations that occurred during the period under examination present numerous parallels with the changes currently generated by technological innovation, new forms of conflict, and the multidimensional character of modern warfare.

At the beginning of the twentieth century, the emergence of modern artillery, machine guns, and the mobilization of industrial resources fundamentally transformed the character of armed conflict. Similarly, today's strategic environment is shaped by the development of drones, cyber warfare, autonomous systems, and artificial intelligence, all of which are profoundly changing the conduct of military operations (Freedman 2017, 311-340).

The experience of the Romanian Army between 1913 and 1917 demonstrates that one of the greatest vulnerabilities of a military institution arises when doctrine, organization, and infrastructure fail to evolve at the same pace as the changing nature

of warfare. In 1916, the Romanian Army entered a modern industrial conflict while still relying on structures and tactical concepts largely influenced by nineteenth-century models of warfare. In a similar manner, contemporary armed forces may encounter significant difficulties if technological modernization is not accompanied by corresponding doctrinal and organizational adaptation. Technological superiority alone does not automatically guarantee military success in the absence of a flexible doctrine and a rapid capacity for operational learning. The Romanian experience illustrates that effective adaptation requires not only the acquisition of new technologies but also the development of institutional mechanisms capable of integrating innovation into military planning, training, and operational practice.

The campaigns of 1913 and 1916 demonstrated that logistic deficiencies can decisively affect military effectiveness, regardless of troop morale or the level of preparation of military structures. Difficulties related to supply, mobility, and transportation infrastructure had a negative impact on the Romanian Army's ability to sustain large-scale operations. The realities of contemporary conflicts confirm this conclusion. The war in Ukraine has highlighted the importance of logistics, the protection of lines of communication, and the resilience of both military and civilian infrastructure (Strachan 2013, 97-114). Operational success depends not only on the performance of military equipment, but also on the capacity of the state to sustain a prolonged military effort.

Consequently, one of the fundamental lessons derived from this experience is that the adaptation of armed forces must include the development of logistic infrastructure, the enhancement of mobilization capacity, the protection of critical infrastructure, and the strengthening of institutional and economic resilience (Kilcullen 2020, 184-201).

Contemporary conflicts also demonstrate that armed forces must be prepared for hybrid warfare, multidomain operations, information and cyber confrontations, and the simultaneous employment of conventional and unconventional means (Hoffman 2009, 34-39). In this respect, the experience of the Romanian Army between 1916 and 1917 underscores the importance of an institution's ability to adapt rapidly to changes in the character of warfare.

The 1917 campaign highlighted the decisive role of cooperation between infantry and artillery, as well as the importance of effective coordination between command structures and combat units (Otu 2017, 132-141). Today, this lesson is reflected in the concept of multidomain operations, which requires the integration of land, air, maritime, cyber, and information activities within a unified command-and-control system (U.S. Army Training and Doctrine Command 2018, 7-18).

Historical experience has demonstrated that military success depends on the interoperability of force structures, the integration of modern technologies, the speed of information flow, and the capacity for operational coordination (Stevenson 2005, 421-429). The Romanian Army's performance in 1917 showed how improvements in coordination, communication, and combined-arms cooperation could significantly enhance combat effectiveness, even under conditions of limited resources.

The experiences of the period 1913-1917 underscored the fact that military effectiveness depends directly on the capacity of the state and society to sustain the war effort. During the First World War, Romania's ability to resist was influenced not only by the performance of its armed forces but also by the mobilization of the economic, administrative, and moral resources of society. In this context, the present research highlights the fact that the adaptation of armed forces cannot be separated from the strengthening of the state's overall resilience.

The contrast between the performance of the Romanian Army in 1916 and that of 1917 demonstrates the importance of institutional learning and adaptive capacity. The rapid reorganization of the army, the modernization of training, and the incorporation of lessons derived from battlefield experience enabled the transformation of a military force in crisis into one capable of resisting the offensives of the Central Powers. This conclusion carries significant relevance for contemporary armed forces. In a strategic environment characterized by rapid change and uncertainty, the capacity for organizational learning becomes one of the most important prerequisites for operational effectiveness ([Farrell, Osinga, and Russell 2013, 11-27](#)).

The comparative analysis between the experiences of the Romanian Army during the period 1913-1917 and contemporary operational realities highlights the enduring nature of several fundamental problems of warfare: the importance of logistics, the necessity of doctrinal adaptation, the role of combined-arms cooperation, and the relationship between military capability and the state's capacity to sustain military operations.

Historical experience accentuates that military success depends not exclusively on technology or numerical superiority, but also on institutional adaptability, doctrinal flexibility, and societal resilience. The Romanian Army's evolution from the setbacks of 1916 to the defensive successes of 1917 illustrates how the ability to learn, reorganize, and adapt can significantly influence the outcome of military operations.

Consequently, the lessons derived from the Romanian Army's confrontation with modern industrial warfare can provide valuable insights for understanding contemporary challenges and supporting the ongoing process of military transformation and adaptation. These lessons remain relevant in an era characterized by rapid technological change, multidomain operations, and increasingly complex security environments, reaffirming the importance of organizational learning, operational flexibility, and the integration of military capabilities within the broader framework of national resilience.

Conclusions

The analysis of the Romanian Army's confrontation with the realities of modern warfare during the campaigns of 1913, 1916, and 1917 highlights the complex nature of the Romanian state's process of military adaptation at the beginning of the

twentieth century. The evolution of the military institution during this period reflects both the limitations of Romania's political and economic modernization and the army's capacity to learn from the dramatic experiences of contemporary conflicts.

The findings of this research demonstrate that, between 1913 and 1917, the Romanian Army underwent an accelerated and often contradictory process of adaptation to modern warfare. The 1913 campaign revealed the existence of significant logistic, medical, and organizational vulnerabilities; however, the lessons derived from this experience were only partially implemented before Romania's entry into the First World War. The cholera epidemic, supply difficulties, and infrastructural shortcomings demonstrated that the army was not fully prepared for the demands of a large-scale modern conflict. The political and military leadership continued to display excessive optimism regarding the Romanian Army's ability to cope with a major European war. The influence of the French doctrine of the decisive offensive, combined with an underestimation of the importance of logistics and positional warfare, contributed to the persistence of tactical concepts that were insufficiently adapted to the new realities of the battlefield.

The 1916 campaign revealed the limitations of the incomplete modernization of the military institution and the difficulties involved in adapting to modern industrial warfare. Romania entered the First World War with a military establishment that remained only partially modernized, dependent on external resources, and burdened by logistic and organizational deficiencies. The defeats suffered in Transylvania, Dobruja, and Wallachia demonstrated the limitations of the Romanian military system when compared with the modern armies of the Central Powers. The lack of heavy artillery, insufficient ammunition supplies, difficulties in operational coordination, and the vulnerability of the country's infrastructure all contributed decisively to the failure of the campaign. At the same time, the experience of 1916 highlighted the inability of a predominantly offensive doctrine to respond effectively to the conditions of attritional warfare and the realities of the industrialized battlefield.

Nevertheless, the 1916 campaign should not be viewed merely as a succession of military defeats. It also marked the beginning of an accelerated process of institutional transformation. The retreat into Moldavia and the preservation of the army's principal combat nucleus created the conditions necessary for the subsequent reorganization of the Romanian armed forces.

At the same time, the research demonstrates that the reorganization of 1917 represented a decisive moment in the transformation of the Romanian Army. Under the influence of the French Military Mission led by General Henri Berthelot, the army underwent an extensive process of doctrinal, organizational, and technical reconstruction. The reform of military training, the development of combined-arms cooperation, the modernization of artillery employment, and the reorganization of the defensive system enabled the army to adapt to the conditions of modern warfare. The victories at Mărăști, Mărășești, and Oituz demonstrated the effectiveness of the

transformations implemented in 1917. The reorganized Romanian Army succeeded in offering effective resistance to the offensives of the Central Powers and in preserving the existence of the Romanian state under extremely difficult strategic circumstances.

The analysis of the campaigns of 1913, 1916, and 1917 also highlights the existence of important structural continuities. Logistic problems, the influence of political factors on military decision-making, and deficiencies within the command system persisted throughout the entire period under examination. At the same time, however, the successive experiences of war generated significant doctrinal and organizational changes. The Romanian Army gradually evolved from a force largely shaped by nineteenth-century military concepts into an institution increasingly capable of operating under the conditions of modern industrial warfare.

The difference between the army's performance in 1916 and that of 1917 demonstrates the capacity of the Romanian military institution to learn and adapt within a relatively short period of time. In this respect, the experience of war played an essential role in accelerating doctrinal modernization and in the professionalization of operational leadership.

From a historical perspective, the Romanian Army's confrontation with modern warfare must be analyzed in close connection with the broader process of modernization of the Romanian state. The limitations of the army largely reflected the economic, administrative, and industrial constraints of Romania at the beginning of the twentieth century. Modern warfare required the comprehensive mobilization of society's resources, and military capability became inseparable from the economic and institutional infrastructure of the state. Consequently, the effectiveness of the armed forces depended not only on military organization and combat readiness but also on the state's capacity to generate, sustain, and coordinate the resources necessary for prolonged military operations.

At the same time, the experiences of the period 1913-1917 had important consequences for the subsequent development of the Romanian Army. The lessons concerning the role of logistics, artillery, combined-arms cooperation, and operational command significantly influenced the process of military reorganization during the interwar period.

Furthermore, the campaigns under examination contributed to strengthening the role of the army within Romanian society and to legitimizing it as the principal instrument for the achievement of national unity. The resistance of 1917 became a central element of collective memory and of the broader narrative concerning the Romanian Army's contribution to the creation of Greater Romania.

The Romanian Army's confrontation with the realities of modern warfare between 1913 and 1917 represents a process of transition from the traditional nineteenth-century military model to the demands of European industrial warfare. The experiences of these campaigns demonstrate that adaptation to modern warfare

depended not exclusively on the courage of soldiers or the competence of military commanders, but also on the capacity of the state to integrate technological, organizational, and doctrinal progress into its military and administrative structures. Therefore, this study confirms that the military experiences of the period 1913-1917 should be interpreted as successive stages in the process of Romania's military and institutional modernization within the broader context of European industrial warfare. These campaigns collectively illustrate the challenges, limitations, and achievements of a state and military institution undergoing profound transformation in response to the rapidly changing nature of modern conflict.

References

- Romanian National Military Archives (RNMA)**, Ministry of War collection, file 212/1912.
- _____. Ministry of War collection, file 212/1913.
- _____. General Headquarters collection, file 45/1913.
- _____. General Headquarters collection, file 221/1916.
- _____. General Headquarters collection, file 355/1917.
- _____. Great General Staff collection, file 178/1916.
- _____. Great General Staff collection, file 245/1916.
- _____. Great General Staff collection, file 312/1917.
- _____. Army Health Service collection, file 18/1913.
- _____. The 2nd Army collection, file 88/1917.
- Averescu Alexandru**. 1937. *Daily Notes from the War (1916-1918)*. 3rd Edition. Bucharest: National Culture Publishing.
- _____. 1991. *Daily Notes from the War*. Bucharest: Military Publishing.
- Berthelot Henri**. 1920. *Mémoires et correspondance militaire*. Paris: Plon.
- Brătianu, Gheorghe I.** 1940. *The political and military action of Romania in 1916*. Bucharest: The Romanian Book Publishing.
- Cristescu, Sorin**. 2010. *The Berthelot Mission and the Reorganization of the Romanian Army*. *Yearbook of the Institute of History*, no. 47. Bucharest.
- Dupuy, Trevor N.** 1977. *A Genius for War: The German Army and General Staff*. New Jersey: Prentice Hall.
- Farrell, Theo; Osinga, Frans; Russell, James A.** 2013. *Military Adaptation in Afghanistan*, Stanford: University Press.
- Fuller, J.F.C.** 1961. *The Conduct of War*. London: Eyre & Spottiswoode.
- Freedman, Lawrence**. 2017. *The Future of War: A History*. New York: Public Affairs.
- Hall, Richard C.** 2000. *The Balkan Wars 1912-1913*. London: Routledge.
- Hitchins, Keith**. 2013. *Romania 1866-1947*. Bucharest: Humanitas Publishing.

- Hoffman, Frank G.** 2009. *Hybrid Warfare and Challenges*. Joint Force Quarterly, nr. 52.
- Iarca, Alexandru.** 1922. *My memorial*. Buzău: Ioan Călinescu Publishing.
- Ionescu, Mihail E.** 2002. *The modern Romanian army*. Bucharest: Military Publishing.
- Keegan, John.** 1999. *The First World War*. London: Pimlico.
- Kilcullen, David.** 2020. *The Dragons and the Snakes*. New York: Oxford University Press.
- Kirițescu, Constantin.** 1989. *The History of the War for the Unification of Romania 1916-1919, vol. I*. Bucharest: Scientific and Encyclopedic Publishing House.
- Maria, Queen of Romania.** 2014. *The story of my life*, vol. III. Bucharest: Humanitas Publishing.
- Otu, Petre.** 2014. *The Modernization of the Romanian Army before the First World War*. *Military History Press*, no. 3-4. Bucharest.
- _____. 2017. *The Romanian Army in the First World War*. Bucharest: Military Publishing.
- Pascu, Ștefan et al.** 1988. *The military history of the Romania, vol. V*. Bucharest: Military Publishing.
- Prezan, Constantin.** 1995. *Memories*. Bucharest: Military Publishing.
- Rosetti, Radu.** 1926. *Confessions*. Bucharest: National Culture Publishing.
- Scurtu, Ioan.** 2004. *The history of the Romanians during the four kings*. vol. II. Bucharest: Encyclopedic Publishing House.
- Stevenson, David.** 2005. *1914-1918: The History of the First World War*. London: Penguin Books.
- Stone, Norman.** 1998. *The Eastern Front 1914-1917*. London: Penguin Books.
- Strachan, Hew.** 2013. *The Direction of War*. Cambridge: University Press.
- Stroea, Adrian, and Gheorghe Băjenaru.** 2010. *Romanian Artillery in Data and Images*. Bucharest: Technical-Editorial Center of the Army.
- Torrey, Glenn E.** 1998. *The Romanian Battlefield in World War I*. **Lawrence: University Press of Kansas**.
- _____. 2011. *Romania and World War I: A Collection of Studies*. Rochester, NY: Center for Romanian Studies.
- U.S. Army Training and Doctrine Command.** 2018. *The U.S. Army in Multi-Domain Operations 2028*. TRADOC Pamphlet 525-3-1.
- van Creveld, Martin.** 1977. *Supplying War: Logistics from Wallenstein to Patton*. Cambridge: University Press.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

<https://buletinul.unap.ro/index.php/en/>

Decentralized Security and Crime Control: Assessing the Effectiveness of Forest Guards in Kwara State, Nigeria

Akeem Ayanda ARABA, PhD*
Tawakalitu Bola YUSUF, PhD***

Kafayat Toyin ARABA, PhD**
Taoheed Opeyemi MUHAMMED****

*Department of Politics & Governance, Faculty of Management and Social Sciences,
Kwara State University, Malete, Nigeria
e-mail: araba.akeem@kwasu.edu.ng

 <https://orcid.org/0000-0002-1517-1238>

**Department of Sociology, Faculty of Humanities and Social Sciences,
Al-Hikmah University, Ilorin, Kwara State
e-mail: arabatoyinkafayat@gmail.com

***Department of Social Justice and Security Studies, Faculty of Management
and Social Sciences, Kwara State University, Malete, Nigeria
e-mail: tawakalitu.yusuf@kwasu.edu.ng

****Department of Politics & Governance, Faculty of Management and Social Sciences,
Kwara State University, Malete, Nigeria
e-mail: muhammedtaoheed@gmail.com

Abstract

The persistence of insecurity and criminal activity in Nigeria has intensified debates over the limits of centralized policing and the need for decentralized, community-based security arrangements. In Kwara State, the establishment of Forest Guards represents a subnational response to forest-based crimes such as kidnapping, banditry, illegal logging, and illegal mining, which thrive in remote and weakly governed terrains. This study assesses the effectiveness of Forest Guards in enhancing crime control and local security governance in Ifelodun, Asa, and Kaiama LGAs. Anchored in decentralized security governance and routine activity theory, the study adopts a mixed-methods design, combining survey data from 362 respondents across key stakeholder groups with secondary sources. Findings reveal that Forest Guards play important roles in patrol, surveillance, intelligence gathering, and community engagement. Respondents report moderate reductions in forest-based crimes through deterrence and improved monitoring. However, effectiveness is constrained by logistical, institutional, and legal challenges, including inadequate equipment, poor welfare, and unclear statutory mandates. The study concludes that strengthening legal frameworks, coordination, and funding is essential for sustainable impact.

Keywords:

Decentralized Security; Crime Control; Forest Guards; Local Governance; Kwara State; Nigeria.

Article info

Received: 16 November 2025; Revised: 22 December 2025; Accepted: 27 May 2026; Available online: 30 June 2026

Citation: Araba, A.A., T.B. Yusuf, K.T. Araba, and T.O. Muhammed. 2026. "Decentralized Security and Crime Control: Assessing the Effectiveness of Forest Guards in Kwara State, Nigeria." *Bulletin of "Carol I" National Defence University*, 15(2): 161-184. <https://doi.org/10.53477/2284-9378-26-23>



© „Carol I” National Defence University Publishing House

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC-SA)

Introduction

Across the globe, security decentralization has emerged as a response to the limits of centralized policing. Rising insecurity and the growing complexity of crime have strained state security institutions, especially in the Global South, where challenges include limited resources, wide territorial coverage, weak intelligence, and poor responsiveness to local threats. This has led to the delegation of security functions to subnational and community actors such as vigilante groups, auxiliary forces, and community policing initiatives that rely on local knowledge and proximity for rapid response (Baker 2010; Abrahamsen and Williams 2011). While these arrangements can improve crime control, they also raise concerns about coordination, accountability, and effectiveness.

A critical dimension of this global shift is the growing importance of ungoverned and forested spaces as hubs of criminal activity. Across regions such as Latin America, Southeast Asia, and Africa, forests have become strategic operational environments for kidnapping syndicates, illegal logging networks, wildlife traffickers, and armed insurgent groups. These areas often combine difficult terrain with weak state presence and limited surveillance capacity, creating ideal conditions for illicit activities (UNODC 2021). Consequently, decentralized security actors such as forest guards have gained prominence as mechanisms for territorial control and localized crime management. Their emergence reflects an adaptive security process in which states attempt to extend authority into hard-to-reach areas through locally embedded structures.

In Nigeria, the dynamics of insecurity have intensified this shift toward decentralized security. Over the past two decades, the country has experienced a steady escalation of violent crime and organized criminality, including terrorism, banditry, kidnapping for ransom, armed robbery, farmer-herder conflicts, and environmental crimes such as illegal logging and wildlife trafficking. These challenges have not only undermined public safety but have also weakened state authority, disrupted economic activities, and eroded public trust in the government's capacity to provide security as a fundamental public good (Akinwale and Aderinto 2011; Okoli and Ugwu 2019). Despite reliance on a centralized policing system anchored by the Nigeria Police Force (NPF), insecurity continues to spread across both urban and rural areas, revealing deep structural deficiencies within the national security architecture.

Nigeria's centralized policing system, inherited from colonial administration, places primary responsibility for internal security on federal authorities. While intended to ensure uniformity and cohesion, it has become increasingly ineffective in addressing diverse local security challenges. Studies report persistent problems such as manpower shortages, inadequate funding, weak intelligence, corruption, poor community relations, and slow response times, especially in remote areas (Ajibade et al. 2025; Hills 2012). These gaps have led states and communities to adopt decentralized security approaches to complement formal policing.

This shift has produced various local security actors, including state-backed outfits, vigilante groups, and auxiliary forces. Examples include the Civilian Joint Task Force (CJTF) in the North-East, the Amotekun Corps in the South-West, neighborhood watch groups, and emerging forest guard systems in several states. These initiatives reflect a move toward community-based security, where local actors support surveillance, intelligence gathering, and crime prevention ([Abrahamsen and Williams 2011](#); [Baker 2010](#)). However, their growth has raised concerns about legal status, effectiveness, accountability, and human rights.

One of the most pressing security challenges in Nigeria is the increasing use of forested and ungoverned spaces as bases for criminal operations. Forest reserves and borderland areas have become critical sites for kidnapping camps, bandit hideouts, arms trafficking routes, and illegal resource extraction activities such as logging and charcoal production ([Okoli and Okpaleke 2014](#)). These forest-based crimes present multidimensional threats that combine conventional security risks with environmental degradation and economic losses. Moreover, the rugged and expansive nature of forest terrains makes them difficult to police using conventional methods, thereby necessitating alternative approaches rooted in localized surveillance and territorial control ([Rufai 2017](#)).

In North-Central Nigeria, particularly in Kwara State, these dynamics have become more pronounced. The state serves as a key transit corridor linking northern and southern Nigeria and shares boundaries with several states. Its extensive forest reserves have recently been linked to kidnapping, armed robbery, and other cross-border criminal activities, raising public concern and exposing the limits of relying solely on federal security agencies for forest protection. In response, the Kwara State Government introduced the Forest Guards initiative as a decentralized security strategy to monitor forests, prevent criminal infiltration, and support formal security agencies.

The establishment of Forest Guards represents a decentralization of security based on local knowledge and proximity. Recruited mainly from host communities, they patrol forest areas, gather intelligence, prevent illegal activities such as logging and poaching, and collaborate with law enforcement agencies. The initiative reflects a broader effort by subnational governments to address security gaps left by overstretched federal institutions. However, there is still limited empirical evidence on their effectiveness, capacity, and overall contribution to crime control. Existing literature on decentralized security in Nigeria has predominantly focused on high-profile actors such as vigilante groups and regional security outfits, with relatively little attention given to forest guards as specialized security actors. Similarly, studies on forest-based crimes often emphasize environmental and conservation perspectives while neglecting their security implications ([Osemeobo 2005](#); [Olaleru and Egonmwan 2014](#)). This creates a significant gap in understanding how forest guards operate within Nigeria's evolving security architecture and whether they meaningfully contribute to enhancing public safety.

The problem addressed in this study, therefore, centers on the limited scholarly and policy understanding of the effectiveness of forest guards as decentralized security actors in Nigeria, with specific reference to Kwara State. While recent developments, including the federal deployment of over 7,000 trained forest guards across frontline states and the recruitment of additional personnel in Kwara, indicate growing institutional commitment, critical questions remain regarding their legal mandate, training, coordination with formal security agencies, and overall impact on crime reduction. Against this backdrop, this study examines the effectiveness of Forest Guards in improving crime control and security governance in Kwara State. It focuses on their operational roles, contributions to reducing forest-based crimes, challenges affecting their performance, and relationships with formal security agencies and local communities. The study is guided by three research questions on roles, impact, and challenges. The study is significant to both academic and policy discourse. It contributes to existing literature by highlighting the role of decentralized security and providing insights into grassroots security practices. It also offers recommendations for strengthening decentralized security frameworks, improving accountability, and enhancing crime control strategies in Nigeria's forested and rural areas.

Justification for the case study

This study focuses on Kwara State for three analytically significant reasons: First, Kwara occupies a strategic geo-security position as a transit corridor between northern and southern Nigeria, making it vulnerable to cross-regional criminal flows. Second, the state has experienced a recent escalation in forest-based crimes, particularly in Ifelodun, Kaiama, and Asa LGAs, where kidnapping and banditry have been linked to forest reserves. Third, Kwara represents a policy-relevant case of active decentralization, having institutionalized the Forest Guards initiative with over 3,300 personnel (700 initial + 2,600 additional recruits). Thus, Kwara State is selected not as a random case but as a critical case study where decentralized forest security is both operationalized and evolving, making it ideal for empirical assessment.

Literature Review: Decentralized Security and Crime Control

The decentralization of security provides a compelling framework for understanding contemporary transformations in crime control, particularly in low-capacity, post-colonial states such as Nigeria. Rather than viewing security as the exclusive responsibility of the state, decentralization refers to the process through which security functions such as surveillance, intelligence gathering, and enforcement are redistributed across multiple actors at national, subnational, and community levels. In contexts where state institutions face fiscal, logistical, and institutional limitations, this process becomes not merely an option but a practical necessity. In Nigeria, the persistence of complex and localized security threats has exposed the limitations of centralized policing, thereby accelerating the shift toward decentralized and hybrid security arrangements ([Suleiman and Maiangwa 2017](#)).

This shift aligns with plural policing, which challenges the idea of the state as the sole provider of security. Instead, security is increasingly delivered through partnerships between state and non-state actors within broader policing networks (Mazerolle et al. 2024). Scholars such as Cooper-Knock et al. (2024) describe this as “security assemblages,” where the state acts as a coordinating hub among community groups, private security providers, and auxiliary forces. This is especially evident in developing countries, where complex threats and limited state capacity require shared responsibility in crime control. From a sociological perspective, collective efficacy explains the value of decentralized security, emphasizing community cohesion and participation in maintaining order. Local actors have better contextual knowledge, terrain familiarity, and social networks that improve detection and response, particularly in rural and forest areas where formal policing is weak. However, decentralization also carries risks such as vigilantism, exclusion, and abuse if not properly regulated (Okeke-Ogbuafor, Gray, and Stead 2017).

Recent studies argue that while state-backed vigilante groups have strong local intelligence and trust, they often lack the capacity to confront armed criminal networks. This makes stronger collaboration between federal and state governments essential for training, equipping, and regulating decentralized actors under standardized and human rights-based frameworks (Araba and Muhammed 2026). A key concern is accountability, as unclear mandates in decentralized systems create “accountability gaps” where responsibility for misconduct becomes difficult to assign. Scholars therefore stress the need for transparency and legal oversight (Lister and Jones 2015).

The literature increasingly supports a hybrid security model where the state remains a regulator and coordinator rather than the sole provider of security. This is particularly relevant in post-colonial states like Nigeria, where centralized policing coexists with demands for localized security responses (Cooper-Knock, Berg, and Diphhoorn 2024).

In Nigeria, decentralization is closely linked to the problem of “ungoverned spaces,” especially forests used by bandits, kidnappers, and illegal resource actors (Okoli and Okpaleke 2014). Forest guards are seen as useful due to their local knowledge and community embeddedness, making them effective for intelligence gathering and rapid response. However, they face major constraints, including poor funding, weak training, inadequate equipment, and a lack of clear legal backing (Crawford 2006). Coordination challenges with agencies like the Nigeria Police Force and the Nigeria Security and Civil Defence Corps also limit effectiveness due to overlapping mandates and weak communication (Cooper-Knock, Berg, and Diphhoorn 2024). Overall, decentralization offers an adaptive response to state capacity limits, and forest guards play a growing role in localized security in areas like Kwara State. However, their effectiveness depends on strong legal frameworks, adequate resources, professional training, and effective inter-agency coordination; without these, decentralization risks becoming fragmented and ineffective.

Empirical Review of Related Studies

Beyond conceptual debates, empirical studies have increasingly examined decentralized and community-based security arrangements in Nigeria. Ojieleze (2025), in the *Political and Security Studies Scholarly Journal*, investigated the motivations for establishing Amotekun in Southwestern Nigeria using a qualitative exploratory design grounded in situational crime prevention theory and 31 interviews with members in Ondo State. Findings showed that Amotekun emerged in response to perceived failures of Nigeria's centralized security system in tackling kidnapping, robbery, and farmer-herder conflicts. The study also noted ethnic exclusivity and Yoruba socio-political alignment, suggesting a dual role in security provision and regional identity formation. It concluded that Amotekun reflects both crime control needs and broader regional political dynamics.

Similarly, Akano (2024), in the *Global Scientific Journal*, assessed Amotekun's impact on crime reduction in Ibadan, Oyo State, using surveys and qualitative interviews with officials, community leaders, and residents in Akinyele and Ibadan North LGAs (351 questionnaires and 12 interviews). Findings indicated improved crime control through 24-hour patrols and faster response times, leading to public acceptance. However, challenges such as inadequate funding, limited personnel, and a lack of equipment were identified. The study concluded that Amotekun's sustainability depends on stronger government support and improved resources.

Onwuzuruigbo (2021), in *African Studies Review*, employed a qualitative case-study design supported by field interviews and conflict-event data analysis. The study examined "enclaves of banditry" in northern Nigeria, showing how forested spaces function as operational bases for armed groups and how local geography shapes insurgent survival strategies. Onuoha and Okolie-Osemene (2019), in the *Palgrave Handbook on Internal Security Management in Nigeria*, adopted a qualitative documentary and policy analysis approach, synthesizing secondary data, policy reports, and empirical case studies on kidnapping-for-ransom. The study traced the evolution of kidnapping networks and examined how forest environments structurally enable hostage-taking economies.

Agbiboa (2020), in *Small Wars & Insurgencies*, examined the emergence of the Civilian Joint Task Force (CJTF) in north-eastern Nigeria as a youth-led vigilante response to Boko Haram. Using a qualitative approach based on field observations and local accounts, the study showed that the CJTF developed from a collective duty to protect communities, with youths supporting military operations by identifying insurgents. It also found that participation cut across ethnic and religious lines, challenging identity-based explanations of vigilantism. The study concluded that the CJTF represents community-based counterinsurgency where civilians complement state security efforts.

Badiora (2019), in *Policing: An International Journal of Police Strategies & Management*, studied community perceptions of vigilantism in Lagos using survey data from 768 residents, with 386 valid responses from those with recent contact with vigilante groups. Findings showed that support for vigilantism was shaped less by perceived effectiveness and more by legitimacy, procedural justice, and communal values. Residents were more supportive when vigilante groups were seen as fair and respectful. The study concluded that legitimacy and fair treatment are key to sustaining community-based security groups.

These studies show that decentralized security groups in Nigeria contribute to crime reduction, but modestly. Their effectiveness is mainly limited by legal and logistical constraints, while legitimacy based on fairness and inclusion strongly influences success. They also highlight the need for place-based security in forest areas. This study extends the literature by empirically examining Forest Guards in north-central Nigeria using primary data.

Theoretical Frameworks

The effectiveness of Forest Guards is best understood through the lenses of Plural Policing and Collective Efficacy.

Plural Policing and Security Assemblages

Traditional security discourse, rooted in Weberian theory, posits that the state must maintain a monopoly on the legitimate use of force. However, recent scholarship by Bayley and Shearing (2001) suggests a move toward “multilateralization,” where security is co-produced by a network of state and non-state actors. In Kwara State, the Forest Guard initiative functions as a Security Assemblage, a fluid collaboration between the Office of the National Security Adviser (ONSA), the Kwara State Government, and local community recruits. This hybrid model allows the state to “anchor” security while leveraging the specialized skills of localized units.

Routine Activity Theory and Capable Guardianship

According to Routine Activity Theory (Cohen and Felson 1979), crime occurs when a motivated offender and a suitable target converge in the absence of a “capable guardian”. Historically, Nigerian forests lacked this guardianship, leading to their exploitation by criminal networks. The deployment of 1,000 newly trained Forest Guards in Kwara State (2025) represents the institutionalization of guardianship. By maintaining a constant presence in “deep forest” zones, these guards disrupt the “routine” of criminal elements that previously operated with impunity due to the absence of state presence.

Methodology

The research employed a descriptive survey approach, utilizing data gathered from both primary (questionnaires and interviews) and secondary (textbooks, journals, government documents, newspapers, and internet sources) sources.

Research Design

This study adopts a descriptive survey design using a mixed-methods approach. According to John W. Creswell and J. David Creswell (2018) mixed methods combine quantitative and qualitative data to provide a broader and deeper understanding. The quantitative aspect uses a structured Likert-scale questionnaire to assess perceptions of security effectiveness, while the qualitative aspect relies on secondary sources such as official reports and publications for contextual support. This design is suitable for security studies in Nigeria, where crime statistics are often underreported, making stakeholder perceptions and documented evidence important.

Study Area

The study is situated in Kwara State, North-Central Nigeria. Kwara is strategically significant due to its vast forest reserves, including the Kainji Lake National Park (partially extending into the state) and several designated forest reserves in the Kwara South and North senatorial districts. These forests have recently become flashpoints for banditry and communal clashes, prompting the state government to deploy over 1,000 Forest Guards in 2025. The geographical diversity of the state, ranging from savannah to dense forest patches, provides a robust landscape for assessing how decentralized guards manage varied terrains.

Justification of the Study Population

The study population includes security actors and community members for methodological balance. Community members provide perceptions of safety and effectiveness, while Forest Guards, Police, and NSCDC offer operational perspectives. Traditional rulers add governance and legitimacy insights. However, using only community respondents would create perception bias, while multiple stakeholders are included to ensure balanced and triangulated findings.

Population of the Study

The study population comprises residents and security stakeholders from the forest-prone LGAs of Ifelodun, Asa, and Kaiama in Kwara State, selected due to their large forest reserves and recurring forest-related crimes such as kidnapping, banditry, illegal logging, and farmer-herder conflicts (Okoli and Okpaleke 2014; Akinwale and Aderinto 2011). Based on 2022 projected figures, the populations of Ifelodun (307,700), Asa (187,200), and Kaiama (186,200) give a combined population of 681,100 (City Population, 2022). However, the total study population was estimated at 752,000 persons.

The population includes forest guards, rural residents and farmers in forest-adjacent communities, officers of the Nigeria Police Force and Nigeria Security and Civil Defence Corps, as well as traditional rulers. Including both security personnel and community members ensured balanced and triangulated findings, as community members provided perception-based assessments, while security agencies and traditional rulers contributed operational and governance perspectives.

Sample Size Determination

The sample size for the study was determined using the Taro Yamane (1967) formula, which is appropriate for large populations:

$$N = \frac{N}{1 + N(e)^2}$$

Where:

n = sample size

N = population size (752,000)

e = margin of error (0.05)

Substituting:

$$n = \frac{752,000}{1 + 752,000(0.05)^2}$$

$$n = \frac{752,000}{1 + 752,000(0.0025)}$$

$$n = \frac{752,000}{1 + 1,880}$$

$$n = \frac{752,000}{1,881}$$

$$n = 399.787, \quad n \approx 400$$

Therefore, the study adopts a sample size of 400 respondents, representing the selected LGAs at a 5% margin of error and 95% confidence level.

Sampling Technique

A multi-stage sampling technique was used to ensure representativeness across Kwara State's three senatorial districts (Kwara Central, North, and South). In the first stage, purposive sampling was used to select Local Government Areas such as Kaiama, Asa, and Ifelodun due to their high concentration of forest reserves and history of forest-related crimes. In the second stage, stratified random sampling divided respondents into four groups: Forest Guards, rural residents/farmers, formal security personnel, and traditional rulers. In the final stage, simple random sampling was used to select individual respondents from each group.

Sample Frame

Table 1 presents the proportionate allocation of the sample size across the selected LGAs and respondent categories. The distribution is based on population size, ensuring that

TABLE 1: Sample Frame Distribution Across Selected LGAs and Respondent Categories

LGA	Population	Total Sample	Residents/ Farmers	Forest Guards	Police/ NSCDC	Traditional Rulers
Ifelodun	307,700	181	127	27	18	9
Asa	187,200	110	77	17	11	5
Kaiama	186,200	109	76	16	11	6
Total	681,100	400	280	60	40	20

LGAs with larger populations, such as Ifelodun, receive a correspondingly larger share of the sample. Within each LGA, respondents are further distributed across four strata: rural residents/farmers, forest guards, Police/NSCDC officers, and traditional rulers, using proportional allocation. This approach ensures representativeness, minimizes sampling bias, and enhances the validity of findings by capturing perspectives from both community members and security stakeholders.

Research Instrumentation

The study employs the forest security effectiveness questionnaire (FSEQ) as the primary instrument. The FSEQ is a structured questionnaire divided into four sections aligned with the research objectives: Roles, Impact, Challenges, and Interactions. Items are measured on a 5-point Likert scale ranging from “Strongly Agree” to “Strongly Disagree”. In addition to the questionnaire, the study utilizes secondary data sources, including official reports, publications, and other documented materials, to provide context and support the analysis of the survey results. These sources help to validate findings and offer insights into legal frameworks, inter-agency collaboration, and operational challenges in forest security.

Validity and Reliability

To ensure content validity, the research instruments were reviewed by experts in Criminology and Security Studies at Kwara State University and Al-Hikmah University. For reliability, a pilot study was conducted in a neighboring state (e.g., Ekiti or Osun), and the data were analyzed using Cronbach’s Alpha, with a coefficient of 0.70 or higher considered acceptable for the main study.

Reliability Results

A pilot test was conducted with 30 respondents in Osun State (Ola-Oluwa LGA), a neighbouring state with similar forest-adjacent rural settlements, before the main fieldwork. Item analysis was performed on each construct of the Forest Security Effectiveness Questionnaire (FSEQ), and minor revisions were made to three items based on pilot feedback. For the main study (N = 362), Cronbach’s alpha coefficients were computed using SPSS v28.0. As shown in Table 2, all constructs and the overall scale exceeded the 0.70 threshold, indicating acceptable to excellent internal consistency.

TABLE 2. Reliability Analysis: Cronbach’s Alpha by Construct (N = 362)

Construct	No. of items	Cronbach’s α	Interpretation
Roles of Forest Guards	9	0.756	Acceptable
Impact on Crime Reduction	8	0.848	Good
Institutional, Operational & Legal Challenges	10	0.881	Good

Source: Authors’ computation from the survey data (SPSS v28.0).

The Cronbach's alpha coefficients in Table 2 indicate that all three constructs exceed the acceptable 0.70 threshold (Roles $\alpha = 0.756$; Impact $\alpha = 0.848$; Challenges $\alpha = 0.881$), while the overall 27-item scale shows excellent reliability ($\alpha = 0.939$). The Roles scale demonstrates acceptable reliability, whereas the Impact and Challenges scales show good reliability. The slightly lower Roles coefficient is linked to item R9 (training adequacy), which was retained for theoretical completeness. Overall, the results support the use of summative mean scores for further analysis.

Method of Data Collection

Data collection was conducted over six weeks. Due to the remote nature of the forest communities, Field Research Assistants were trained to administer questionnaires in local languages (Yoruba, Hausa, and Baruba), enabling non-literate respondents to participate through guided interviews. Ethical considerations, including informed consent and respondent anonymity, were strictly maintained because of the sensitive nature of the security-related discussions.

Method of Data Analysis

Quantitative data were analysed using SPSS version 28.0. Descriptive statistics, including frequencies, percentages, and mean scores, were used to summarize respondent demographics and Likert-scale responses, with a 3.0 mean score serving as the threshold for agreement. Secondary data from reports and official statistics were reviewed and integrated to support and validate the survey findings.

Ethical Considerations

Ethical approval for this study was obtained from the Kwara State University Postgraduate Research Ethics Committee, the Kwara State Ministry of Tertiary Education, and relevant Institutional Review Boards before fieldwork commenced. Informed consent was obtained from all participants, while confidentiality and anonymity were maintained throughout the study. Participants were protected from harm, and their privacy and dignity were respected at all stages. The dataset was anonymized before being deposited in the Open Science Framework (OSF).

Results

Out of the 400 questionnaires administered, 362 were properly completed and returned, representing a response rate of 90.5%. The remaining 38 questionnaires (9.5%) were either not returned or were excluded due to incomplete or invalid responses.

Demographic Profile of Respondents

Demographic data show that, out of the 362 respondents, rural residents and farmers make up the largest share of respondents (50.3%), followed by Forest Guards (23.2%), formal security personnel (18.2%), and traditional rulers (8.3%), ensuring a balance of perception, operational, institutional, and governance perspectives. Respondents

are drawn from Ifelodun (40.9%), Asa (31.2%), and Kaiama (27.9%), reflecting their relative population distribution. The age profile is mainly concentrated in the 30-49 years group (63.5%), while 60.0% of respondents have at least secondary education. In addition, 61.3% have lived in their LGAs for over ten years, indicating strong familiarity with local forest and security dynamics. Overall, the sample provides informed and contextually grounded responses.

Research Objectives 1: *What roles do Forest Guards play in crime control and security provision in Kwara State?*

TABLE 3.1.: Perception of the Roles of Forest Guards in Kwara State (N = 362)

Code	Item Statement	SA n(%)	A n(%)	N n(%)	D n(%)	SD n(%)	Mean (SD)
R1	Forest Guards provide critical intelligence on suspicious movements in forest areas	113 (31.2)	182 (50.3)	54 (14.9)	13 (3.6)	0 (0.0)	4.09 (0.77)
R2	Forest Guards are effective in navigating difficult forest terrains	132 (36.5)	163 (45.0)	47 (13.0)	18 (5.0)	2 (0.6)	4.12 (0.85)
R3	Regular patrols by Forest Guards reduce kidnappers' and bandits' hideouts	103 (28.5)	182 (50.3)	55 (15.2)	18 (5.0)	4 (1.1)	4.00 (0.86)
R4	Regular patrols discourage illegal mining activities in forest reserves	86 (23.8)	199 (55.0)	58 (16.0)	18 (5.0)	1 (0.3)	3.97 (0.79)
R5	Forest Guards strengthen security collaboration, particularly with the NSCDC	106 (29.3)	182 (50.3)	54 (14.9)	19 (5.2)	1 (0.3)	4.03 (0.82)
R6	Illegal logging and deforestation have reduced due to enforcement activities	85 (23.5)	199 (55.0)	58 (16.0)	19 (5.2)	1 (0.3)	3.96 (0.79)
R7	Recruiting local indigenes as Forest Guards improves community trust	109 (30.1)	182 (50.3)	55 (15.2)	16 (4.4)	0 (0.0)	4.06 (0.79)
R8	Communities feel safer engaging in forest-related activities	103 (28.5)	182 (50.3)	55 (15.2)	18 (5.0)	4 (1.1)	4.00 (0.86)
R9	Forest Guards have sufficient training to confront armed criminals in forests	32 (8.8)	110 (30.4)	126 (34.8)	65 (18.0)	29 (8.0)	3.14 (1.07)
Grand Mean							3.93

Source: Field Survey (2026). Note: SA = Strongly Agree, A = Agree, N = Neutral, D = Disagree, SD = Strongly Disagree. Decision rule: mean ≥ 3.00 indicates agreement.

Table 3.1 demonstrates a broad consensus that Forest Guards make a meaningful contribution across the operational functions assessed. Eight of the nine items return means above 3.95, with respondents most strongly affirming the Guards' navigational advantage in difficult forest terrain (R2, M = 4.12, SD = 0.85), the value of the intelligence they generate (R1, M = 4.09, SD = 0.77), and the legitimacy that flows from local recruitment (R7, M = 4.06, SD = 0.79). The grand mean of 3.93 sits comfortably above the 3.00 decision threshold, indicating that the role profile of Forest Guards is widely endorsed by all four stakeholder categories. The single departure from this pattern is item R9 (training adequacy, M = 3.14, SD = 1.07), where the distribution shifts toward neutrality and disagreement, with roughly

26% of respondents disagreeing or strongly disagreeing. The contrast between the affirmation of what Forest Guards do and the skepticism about whether they are adequately trained to do it against armed adversaries provides the first empirical signal in the dataset that operational ambition is outrunning institutional capacity, a tension developed further in the analysis of Table 3.3.

Research Objectives 2: *To what extent have Forest Guards contributed to reducing forest-based crimes such as kidnapping, banditry, and illegal logging?*

TABLE 3.2.: Perception of the Roles of Forest Guards in Kwara State (N = 362)

Code	Item Statement	SA n(%)	A n(%)	N n(%)	D n(%)	SD n(%)	Mean (SD)
I1	Forest Guards enhance vigilance and support arrests of suspected criminals	84 (23.2)	199 (55.0)	58 (16.0)	19 (5.2)	2 (0.6)	3.95 (0.81)
I2	Increased patrol activity discourages criminals from using forests as safe havens	88 (24.3)	199 (55.0)	58 (16.0)	17 (4.7)	0 (0.0)	3.99 (0.77)
I3	There is a noticeable decline in kidnapping incidents linked to forest zones	85 (23.5)	199 (55.0)	58 (16.0)	19 (5.2)	1 (0.3)	3.96 (0.79)
I4	Criminals find it more difficult to use forests as operational bases	87 (24.0)	199 (55.0)	58 (16.0)	18 (5.0)	0 (0.0)	3.98 (0.78)
I5	Forest Guards have helped dismantle temporary bandit camps in forest reserves	71 (19.6)	200 (55.2)	72 (19.9)	18 (5.0)	1 (0.3)	3.89 (0.78)
I6	Improved security presence has reduced farmer displacement in affected communities	79 (21.8)	200 (55.2)	58 (16.0)	18 (5.0)	7 (1.9)	3.90 (0.86)
I7	Illegal timber transportation through forest routes has been reduced	69 (19.1)	200 (55.2)	72 (19.9)	19 (5.2)	2 (0.6)	3.87 (0.80)
I8	Monitoring of forest entry and exit points has improved	64 (17.7)	201 (55.5)	72 (19.9)	18 (5.0)	7 (1.9)	3.82 (0.85)
Grand Mean							3.92

Source: Field Survey (2026). Note: SA = Strongly Agree, A = Agree, N = Neutral, D = Disagree, SD = Strongly Disagree. Decision rule: mean $\geq$ 3.00 indicates agreement.

Table 3.2 shows that respondents perceive a moderate but uniformly positive impact of Forest Guards on the major categories of forest-based crime. All eight items fall within the narrow band 3.82-3.99, producing a grand mean of 3.92. The most strongly endorsed effects relate to deterrence (I2, M = 3.99, SD = 0.77) and the operational disruption of criminal sanctuaries (I4, M = 3.98, SD = 0.78), while perceptions of upstream monitoring at entry and exit points (I8, M = 3.82, SD = 0.85) and downstream interdiction of illegal timber transportation (I7, M = 3.87, SD = 0.80) trail slightly. The salient feature of this distribution is its compression: standard deviations cluster tightly around 0.80, and no item drops below the 3.80 mark. This suggests a settled and broadly shared view that the Forest Guard deployment is delivering measurable, if incremental, reductions in forest-based crime rather than transformative ones. The pattern is consistent with the impact

profile typical of newly deployed decentralized security forces operating below their intended capacity and points to the importance of sustained institutional investment if these early gains are to be consolidated.

Research Objectives 3: *What institutional, operational, and legal challenges affect the effectiveness of Forest Guards in Kwara State?*

TABLE 3.3.: Perception of the Roles of Forest Guards in Kwara State (N = 362)

Code	Item Statement	SA n(%)	A n(%)	N n(%)	D n(%)	SD n(%)	Mean (SD)
C1	Forest Guards lack modern communication tools (radios, GPS, surveillance devices)	164 (45.3)	138 (38.1)	37 (10.2)	18 (5.0)	5 (1.4)	4.21 (0.91)
C2	Forest Guards lack adequate patrol logistics (vehicles, motorcycles, fuel)	166 (45.9)	138 (38.1)	36 (9.9)	19 (5.2)	3 (0.8)	4.23 (0.89)
C3	Rivalry and institutional competition hinder cooperation with formal security agencies	86 (23.8)	199 (55.0)	58 (16.0)	18 (5.0)	1 (0.3)	3.97 (0.79)
C4	There is insufficient specialized training in human rights and intelligence-led policing	133 (36.7)	163 (45.0)	47 (13.0)	18 (5.0)	1 (0.3)	4.13 (0.84)
C5	Forest Guards are less equipped than the criminal actors they confront	168 (46.4)	138 (38.1)	36 (9.9)	18 (5.0)	2 (0.6)	4.25 (0.87)
C6	Irregular payment of salaries and allowances undermines the motivation of Forest Guards	134 (37.0)	163 (45.0)	47 (13.0)	18 (5.0)	0 (0.0)	4.14 (0.83)
C7	There is no clear legal framework guiding Forest Guards' powers of arrest and prosecution	163 (45.0)	138 (38.1)	37 (10.2)	18 (5.0)	6 (1.7)	4.20 (0.93)
C8	Political interference and elite influence weaken the professional integrity of Forest Guards	110 (30.4)	182 (50.3)	55 (15.2)	15 (4.1)	0 (0.0)	4.07 (0.79)
C9	Political or elite interference may facilitate the release of arrested offenders	130 (35.9)	163 (45.0)	47 (13.0)	19 (5.2)	3 (0.8)	4.10 (0.88)
C10	Absence of permanent surveillance outposts restricts continuous presence in forest areas	140 (38.7)	163 (45.0)	47 (13.0)	12 (3.3)	0 (0.0)	4.19 (0.78)
Grand Mean							4.15

Source: Field Survey (2026). Note: SA = Strongly Agree, A = Agree, N = Neutral, D = Disagree, SD = Strongly Disagree. Decision rule: mean ≥ 3.00 indicates agreement.

Table 3.3 shows the strongest and most internally consistent agreement of the construct in the study. All ten items score above 3.97, and the grand mean of 4.15 is the highest recorded in this dataset. Respondents most agreed that Forest Guards are out-armed by the criminals they confront (C5, M = 4.25, SD = 0.87), that they lack adequate patrol logistics (C2, M = 4.23, SD = 0.89), and that they lack modern communication tools (C1, M = 4.21, SD = 0.91). The legal-mandate deficit (C7, M = 4.20) and the absence of permanent surveillance outposts (C10, M = 4.19) follow closely, while the lowest-ranked challenge, institutional rivalry with formal

agencies (C3, M = 3.97), still sits well above the threshold of agreement. The cluster, therefore, identifies a tightly coupled constraint system in which logistical under-provision, legal indeterminacy, and welfare deficits operate in the same direction and compound each other. The policy implication is that piecemeal intervention is unlikely to shift Forest Guard performance, because the binding constraints sit simultaneously across the equipment, legal, and welfare domains.

Discussions of Findings

Research Objective One: *Examining the Roles of Forest Guards in Crime Control and Security Provision in Kwara State*

This section addresses the first research objective, which examines the roles of Forest Guards in crime control and security provision in Kwara State, Nigeria. The discussion is grounded in the broader framework of decentralized security governance, which emphasizes the growing involvement of subnational and community-based actors in addressing public safety challenges. In Nigeria, rising insecurity manifested through banditry, kidnapping, armed robbery, illegal logging, and communal violence, particularly in rural and forested regions, has exposed the limitations of conventional policing and military responses ([Onuoha and Okolie-Osemene 2019](#)). These challenges have necessitated complementary security arrangements beyond centralized institutions. Within this context, Forest Guards have emerged as relevant actors in localized crime control and environmental protection. Survey findings support this position, with generally high mean scores (3.14-4.12), indicating broad agreement that Forest Guards make meaningful contributions to security provision in Kwara State.

Forest Guards in Kwara State were initially established to protect forest reserves from illegal activities such as unauthorized logging, poaching, and encroachment. However, their responsibilities have expanded significantly due to the increasing use of forests as operational bases for criminal groups. Forests in Nigeria now serve as hideouts for kidnappers, bandits, and other armed actors because of their remoteness and weak surveillance presence ([Okoli and Ogayi 2018](#)). As a result, Forest Guards perform hybrid roles that combine environmental protection with security enforcement. Their functions include surveillance and patrol operations, intelligence gathering, collaboration with formal security agencies, community engagement, and crime deterrence. Consistent with this classification, respondents strongly agreed that Forest Guards provide critical intelligence (Mean = 4.09) and are effective in navigating difficult forest terrains (Mean = 4.12), highlighting the advantage of localized knowledge in forest-based security operations.

A core responsibility of Forest Guards is routine surveillance and patrol of forest reserves and adjoining rural communities. Through continuous monitoring, they detect suspicious movements, illegal settlements, and potential criminal hideouts. Surveillance plays a central role in crime prevention, as visible security presence discourages offenders and reduces opportunities for criminal activity ([Clarke 2012](#)).

By patrolling forest corridors and access routes, Forest Guards help disrupt criminal operations before they escalate into violent incidents. This aligns with situational crime prevention theory, which emphasizes reducing crime opportunities through environmental monitoring and guardianship (Clarke 2012). Survey results reinforce this role, as respondents agreed that Forest Guards reduce kidnappers' and bandits' hideouts (Mean = 4.00) and that regular patrols discourage illegal mining activities (Mean = 3.97).

Forest Guards also play a significant role in intelligence gathering and early warning systems. Their proximity to local communities and familiarity with forest terrain enable them to identify unusual activities, track unfamiliar movements, and detect emerging threats. This locally generated intelligence is shared with agencies such as the Nigeria Police Force and the Nigeria Security and Civil Defence Corps (NSCDC), thereby improving inter-agency coordination and response times. Decentralized security frameworks are widely recognized for enhancing grassroots intelligence essential for addressing rural and asymmetric crimes (Baker 2010). Survey evidence supports this, as respondents agreed that Forest Guards strengthen security collaboration, particularly with the NSCDC (Mean = 4.03).

In addition, Forest Guards help prevent environmental crimes such as illegal logging, charcoal production, and unregulated mining, which degrade ecosystems and can finance criminal networks, worsening insecurity (Ikuomola, Okunola, and Akindutire 2016). By enforcing forestry regulations and protecting natural resources, they also support social stability and sustainable development. Environmental degradation has been linked to resource conflicts and rural poverty that can intensify insecurity (Homer-Dixon 1999). Survey results support this, as respondents agreed that illegal logging and deforestation have reduced due to enforcement (Mean = 3.96).

Forest Guards also improve community engagement and trust in security provision. In many rural areas of Kwara State, limited confidence in centralized law enforcement has created gaps in security reporting. As locally recruited personnel, Forest Guards are more accessible and often act as first responders. Their interaction with community members strengthens cooperation and vigilance. Community-based security literature highlights trust and legitimacy as key to effective crime control (Tankebe 2013). Accordingly, respondents agreed that local recruitment improves trust (Mean = 4.06) and that communities feel safer engaging in forest-related activities (Mean = 4.00).

Finally, Forest Guards contribute to deterrence and territorial control by maintaining presence in forest areas often considered "ungoverned spaces", which are vulnerable to criminal activity (Raleigh and Dowd 2013). By monitoring these areas, they extend state authority into previously under-policed regions, helping to counter kidnapping and banditry that rely on forest hideouts. However, a key limitation remains, as

the lowest mean score (3.14) indicates insufficient training for confronting armed criminals, reflecting limited confidence in their tactical capacity.

Research Objective Two: *Assessing the extent to which Forest Guards have contributed to reducing Forest-based Crimes in Kwara State*

This section addresses the second research objective, which evaluates the extent to which Forest Guards have contributed to reducing forest-based crimes such as kidnapping, banditry, and illegal logging in Kwara State, Nigeria. The analysis is situated within the broader framework of decentralized security governance, which emphasizes the role of subnational and community-based actors in addressing security threats that exceed the capacity of centralized policing systems. In Nigeria, the growing use of forested areas as operational bases for criminal activities has intensified insecurity, particularly in rural and peri-urban communities. Forests now serve as strategic hideouts for kidnappers, bandits, and illegal loggers due to weak surveillance and difficult terrain ([Onuoha and Okolie-Osemene 2019](#); [Onwuzuruigbo 2021](#)). Against this backdrop, Forest Guards were introduced as a localized security mechanism to strengthen monitoring, improve intelligence gathering, and enhance territorial control. Survey findings indicate generally positive but moderate perceptions of their impact, with mean scores ranging from 3.82 to 3.99, suggesting that respondents acknowledge noticeable, but still evolving, contributions to crime reduction.

From a theoretical and practical standpoint, Forest Guards operate within decentralized security systems, where non-central actors complement overstretched federal institutions in managing localized threats ([Baker 2010](#)). In Nigeria, weaknesses in centralized policing, especially in remote forest areas, create response gaps that delay intervention in criminal incidents ([Hills 2012](#)). Forest Guards help bridge these gaps through a continuous presence in vulnerable locations. Survey results support this, as respondents agreed that they enhance vigilance and support arrests (Mean = 3.95) and discourage criminals from using forests as safe havens (Mean = 3.99).

A key impact is the disruption of kidnapping operations. Forests in Kwara State have historically provided cover for kidnapping syndicates, enabling camps and ransom coordination. Forest Guards have introduced routine patrols and monitoring of entry and exit points, limiting criminal movement. This aligns with situational crime prevention theory, which emphasizes reducing opportunities for crime through environmental control ([Clarke 2012](#)). Respondents reported reduced kidnapping incidents linked to forest areas (Mean = 3.96) and increased difficulty for criminals using forests as bases (Mean = 3.98).

Forest Guards also help mitigate banditry in rural communities bordering forests. Bandits often use forest cover for attacks and escape routes, but local intelligence gathering and collaboration with residents improve early warning and coordination

with formal security agencies. Community-based security literature highlights that locally embedded actors generate more actionable intelligence due to their familiarity with terrain and social networks (Tankebe 2013). Findings show agreement that Forest Guards dismantle temporary bandit camps (Mean = 3.89) and reduce farmer displacement (Mean = 3.90).

In addition, they contribute to addressing environmental crimes such as illegal logging, which degrades ecosystems and funds criminal networks (Ikuomola, Okunola, and Akindutire 2016). Through monitoring timber movement and enforcing forestry regulations, they support both environmental protection and crime control. Environmental security literature also links resource degradation to conflict emergence (Homer-Dixon 1999). Respondents reported reduced illegal timber transport (Mean = 3.87) and improved monitoring of forest access points (Mean = 3.82).

Overall, the findings suggest that Forest Guards have produced a moderate but meaningful reduction in forest-based crimes in Kwara State. Their strongest contributions are improved surveillance, disruption of criminal hideouts, intelligence sharing, and environmental protection. However, effectiveness remains evolving, as reflected in mean scores clustered around 4.00, indicating the need for stronger institutional support, logistics, and integration with formal security agencies.

Research Objective Three: *Institutional, Operational, and Legal Challenges Affecting the Effectiveness of Forest Guards in Kwara State*

This section examines the institutional, operational, and legal challenges affecting the effectiveness of Forest Guards in Kwara State. Although decentralized security initiatives have emerged as important responses to rising insecurity in forested areas of Nigeria, their performance is constrained by structural weaknesses within governance and law enforcement systems. Understanding these limitations is critical for assessing the sustainability and overall impact of Forest Guards in crime control and environmental protection. Survey findings reveal strong consensus among respondents regarding these challenges, with high mean scores ranging from 3.97 to 4.25, indicating that institutional and operational deficiencies are widely perceived as significant.

At the institutional level, limited funding and inadequate resource allocation constitute major constraints. Decentralized security arrangements in Nigeria often operate under tight budgets, affecting recruitment, training, logistics, and personnel welfare. Insufficient financial support restricts access to essential tools such as modern surveillance equipment, communication devices, protective gear, and transportation facilities required for effective patrols. Given the vast and difficult terrain of forest environments, mobility resources such as motorcycles and patrol vehicles are indispensable. However, the lack of such logistics limits the operational reach of Forest Guards, thereby weakening their deterrence capacity and slowing

their response to criminal activities. This concern is strongly reflected in the survey, where respondents agreed that Forest Guards lack modern communication tools (Mean = 4.21) and adequate patrol logistics (Mean = 4.23).

A major institutional challenge is the weak coordination between Forest Guards and formal security agencies such as the Nigeria Police Force, the Nigeria Security and Civil Defence Corps, and the military. Although effective decentralized security requires clear roles, communication, and coordination, ambiguity in mandates often leads to overlap, gaps, and jurisdictional tensions. Survey results confirm that rivalry and institutional competition hinder collaboration (Mean = 3.97).

Operationally, inadequate training is a key limitation. While local recruitment improves knowledge of terrain and communities, it does not always provide the professional policing skills needed to address kidnapping and banditry. There are gaps in intelligence-led policing and human rights training, and guards are often seen as being less equipped than criminals (Mean = 4.13; 4.25). Poor remuneration and welfare conditions also reduce morale and increase vulnerability to corruption, with irregular payments affecting motivation (Mean = 4.14).

Legally, Forest Guards face uncertainty due to the absence of a clear statutory framework defining their powers, especially regarding arrest and prosecution. This limits their authority and weakens enforcement capacity (Mean = 4.20). Weak oversight and accountability further raise concerns about misconduct, abuse of power, and political interference, which can undermine professionalism and public trust (Mean = 4.07; 4.10).

In addition, poor intelligence systems and a lack of digital infrastructure hinder effective data collection, crime tracking, and evidence-based decision-making. The absence of permanent surveillance outposts also limits sustained monitoring (Mean = 4.19). Finally, difficult terrain and environmental conditions in forest areas restrict access and allow criminals to evade detection, highlighting the need for better logistics, technology, and training.

Conclusion

The investigation into the decentralization of security in Kwara State reveals that the deployment of forest guards represents a pivotal shift toward a more resilient, multi-layered crime control framework. By reclaiming “ungoverned” forest spaces and leveraging localized intelligence, these guards have successfully disrupted the operational cycles of kidnappers and illegal loggers that centralized agencies were previously ill-equipped to manage. However, the study concludes that for this decentralized model to remain sustainable and effective, it must be anchored in a robust legal framework that clarifies mandates and ensures professional accountability. Ultimately, the Kwara State experience suggests that while the state must remain the primary coordinator of security, the integration of specialized,

community-rooted units is indispensable for securing vast rural and ecological terrains in contemporary Nigeria.

Recommendations

Drawing from the empirical findings, this study advances three key recommendations to strengthen the effectiveness of Forest Guards in crime control and security governance in Kwara State, focusing on institutional capacity and role clarity, performance monitoring, and legal reform with accountability mechanisms.

- Firstly, there is a need to strengthen institutional capacity through clear role definition and continuous professional development. Given their wide-ranging duties – surveillance, intelligence gathering, environmental protection, and community engagement – the Kwara State Government should establish a clear policy and legal framework defining their mandate within the wider security structure. This will reduce role duplication and conflicts with agencies such as the Nigeria Police Force and the Nigeria Security and Civil Defence Corps. Regular training in intelligence analysis, human rights compliance, and tactical operations is also essential, alongside adequate provision of logistics such as communication tools, mobility equipment, surveillance technology, and protective gear through sustained budgetary allocation.
- Secondly, the study recommends a strong monitoring and evaluation (M&E) system for evidence-based crime control. This should include systematic data collection, incident reporting, and periodic performance audits to assess Forest Guards' impact on crimes such as kidnapping, banditry, and illegal logging. A centralized digital reporting system would improve data accuracy and support trend analysis over time. Integration with joint intelligence platforms involving formal security agencies would enhance coordination and early warning capacity. In addition, regular community surveys and stakeholder engagement should be conducted to measure public trust and improve participatory security governance. Targeted strategies, such as anti-kidnapping patrols and enforcement against illegal logging, should also be prioritized.
- Finally, comprehensive legal reforms and accountability mechanisms are essential for sustainability. The state government should enact or revise laws to clearly define Forest Guards' powers, including arrest, detention, and inter-agency collaboration. Independent oversight or internal disciplinary systems should be established to ensure transparency and prevent abuse of power. Improved welfare packages and timely remuneration are also necessary to enhance morale and reduce corruption risks. Strengthening formal collaboration agreements and joint training with other security agencies will further improve coordination and reduce operational conflicts.

References

- Aas, Katja Franko. 2013. *Globalization and Crime*. SAGE Publications.
- Abiodun, T.F., and F.C. Onuoha. 2025. *Securing the Hinterlands: The Evolution of Sub-National Security Outfits in Nigeria*. African Academic Press.
- Abrahamsen, Rita, and Michael C. Williams. 2011. *Security Beyond the State: Private Security in International Politics*. Cambridge University Press.
- Agbibo, Daniel E. 2020. "Vigilante Youths and Counterinsurgency in Northeastern Nigeria: The Civilian Joint Task Force." *Small Wars & Insurgencies*. <https://doi.org/10.1080/13600818.2020.1837093>.
- Akano, Oluwatobi Pelumi. 2024. "Assessing the Performance and Impact of Amotekun Security Network in Crime Mitigation and Reduction in Ibadan." *Global Scientific Journal* 12(7): 525-543. <https://www.globalscientificjournal.com>.
- Akinwale, Akeem Ayofe, and Adeyinka Abideen Aderinto. 2011. "Crisis of Governance and Urban Violence in Nigeria." *African Journal of Criminology and Justice Studies* 5(1): Article 5. <https://digitalscholarship.tsu.edu/ajcjs/vol5/iss1/5>.
- Albarka. (2025, September 28). Troops, forest guards repel bandits in fierce Oke-Ode gun battle. <https://albarka.ng/troops-forest-guards-repel-bandits-in-fierce-oke-ode-gun-battle/>.
- Ajibade, A.A., O. Akano, O.F. Idris, and S.O. Sanusi. 2025. "Comparative analysis of perceived effectiveness of the Nigeria Police Force (NPF) and Amotekun on crime control in Ondo State." *International Journal of Criminology and Security Studies (IJCSS)* 4(2). Federal University Oye-Ekiti, Nigeria.
- Alemika, E.E.O., and I.C. Chukwuma. 2005. *Crime and Policing in Nigeria: Challenges and Prospects*. Lagos: CLEEN Foundation.
- Ambali, A.R., and A.A. Araba. 2020. Community policing and human security in Nigeria: A study of Lagos State Neighbourhood Safety Corps (LNSC). *Journal of Administrative Science* 17(2): 72-91. <http://jas.uitm.edu.my>.
- Araba, A.A., and O.M. Taoheed. 2026. "Assessing the Crime Control and Regional Security Responses: An Analytical Study of Operation Fagge Yamma, Nigeria." *Bulletin of "Carol I" National Defence University* 15(1): 39-55. <https://doi.org/10.53477/2284-9378-26-03>.
- Badiora, Adewumi I. 2019. "Shaping Community Support for Vigilantism: A Nigerian Case Study." *Policing: An International Journal of Police Strategies & Management* 42(2): 240-254. <https://doi.org/10.1108/PIJPSM-08-2017-0101>.
- Baker, Bruce. 2010. *Security in Post-Conflict Africa: The Role of Non-State Policing*. CRC Press.
- Bayley, David H., and Clifford D. Shearing. 2001. *The New Structure of Policing: Description, Conceptualization, and Research Agenda*. National Institute of Justice.
- City Population. 2022. Nigeria: Local government area populations 2022. <https://www.citypopulation.de/en/nigeria/admin/>.

- Clarke, Ronald V.** 2012. *Situational Crime Prevention: Successful Case Studies*. 2nd ed. Harrow and Heston.
- Cooper-Knock, S.J., J. Berg, and T. Diphooorn.** 2024. "Publics of Policing: Expanding Approaches to Nodal Policing." *Policing and Society* 34(1-2): 87-103. <https://doi.org/10.1080/10439463.2023.2255922>.
- Crawford, Adam.** 2006. "Networked Governance and the Post-modern Condition: The Case of Policing." *Theoretical Criminology* 10 (4): 449-479.
- Creswell, John W., and J. David Creswell.** 2018. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5th ed. SAGE Publications.
- De Filippi, Primavera, and Aaron Wright.** 2018. *Blockchain and the Law: The Rule of Code*. Harvard University Press.
- Eru, Eka John.** 2025. Forest Guards and Community Policing in Nigeria: Strategies to Combat Insecurity. NALTF/SCR/008 Volume 1. Abuja: National Assembly Library Trust Fund, Research Department.
- Hills, Alice.** 2012. "Policing a Plurality of Worlds: The Nigeria Police in Metropolitan Kano." *African Affairs* 111(442): 46-66. <https://doi.org/10.1093/afraf/adr078>.
- Homer-Dixon, Thomas.** 1999. *Environment, Scarcity, and Violence*. Princeton University Press.
- Ikuomola, A. D., R.A. Okunola, and A.F. Akindutire.** 2016. Criminality: Illegal logging of woods in Nigeria's South-West forest belt. *International Journal of Sociology and Anthropology* 8(5).
- Kwara State Government.** 2025. *Internal Security Report: The Deployment of Forest Guards for Rural Safety*. Kwara State Press.
- Kwara State Ministry of Justice.** 2025. *Operational Guidelines and Legal Mandate for the Forest Guard Corps*. Kwara State Government Press.
- Lister, Stuart, and Trevor Jones.** 2015. "Plural Policing and the Challenge of Democratic Accountability." In *Police Leadership: Rising to the Top*, edited by J. Fleming, 75-92. Routledge. https://www.researchgate.net/publication/283127375_Plural_policing_and_the_challenge_of_democratic_accountability.
- Mazerolle, Lorraine, Kevin Petersen, Michelle Sydes, and Janet Ransley.** 2024. "Partnerships in Policing: How Third Parties Help Police to Reduce Crime and Disorder." *Elements in Criminology*. Cambridge University Press. <https://doi.org/10.1017/9781009472029>.
- Meagher, Kate.** 2014. "Informal Security, Institutional Hybridity and the State in Africa." *Development and Change* 45(5): 1016-1040. <https://doi.org/10.1111/dech.12115>.
- National Assembly Library Trust Fund.** 2025. *Forest Guards and Community Policing: A Dual Strategy for Rural Security*. NALTF Research Department.
- Ojieleze, Monday.** 2025. "Motivations Behind the Establishment of Amotekun and Regional Security Dynamics in Southwestern Nigeria." *Political and Security Studies Scholarly Journal* 6(3): 29-40. <https://doi.org/10.33445/psssj.2025.6.3.5>.

- Okeke-Ogbuafor, Nwamaka, Tim Gray, and Selina M. Stead.** 2017. "Two Concepts of Community in the Niger Delta: Social Sense of Communalinity, and a Geographical Sense of Place. Are They Compatible?" *Journal of Place Management and Development* 10(3): 254-269. <https://doi.org/10.1108/JPM-D-01-2017-0003>.
- Okoli, A.C., and F.I. Ochim.** 2016. "Forestlands and National Security in Nigeria: A Threat-Import Analysis." *Journal of Political Science and Leadership Research* 2(2): 43. <http://www.iiardpub.org>.
- Okoli, A.C., and F. N. Okpaleke.** 2014. "Banditry and Crisis of Public Safety in Nigeria: Issues in National Security Strategies." *European Scientific Journal* 10(4): 350-362.
- Okoli, Al Chukwuma, and C.O. Ogayi.** 2018. "Herdsman Militancy and Humanitarian Crisis in Nigeria: A Theoretical Briefing." *African Security Review* 27 (2): 129-143.
- Olaleru, F., and A.O. Egonmwan.** 2014. "Wildlife Conservation Challenges in Protected Forest Areas in Nigeria." *African Journal of Environmental Studies* 7(2): 45-58.
- Olowu, Dele, and J. Ayoade.** 2008. *Nigeria's Public Sector Reforms: Issues and Challenges*. Ibadan: Spectrum Books.
- Onuoha, Freedom C., and James Okolie-Osemene.** 2019. "The Evolving Threat of Kidnapping for Ransom in Nigeria." In *Internal Security Management in Nigeria: Perspectives, Challenges and Lessons*, edited by O. O. Oshita, I. M. Alumona, and F. C. Onuoha, 233-258. Singapore: Palgrave Macmillan. https://doi.org/10.1007/978-981-13-8215-4_12.
- Onwuzuruigbo, Ifeanyi.** 2021. "Enclaves of Banditry: Ungoverned Forest Spaces and Cattle Rustling in Northern Nigeria." *African Studies Review* 64(1): 168-191. <https://doi.org/10.1017/asr.2020.46>.
- Osemeobo, G.J.** 2005. "Living on the Forests: Women and Household Security in Nigeria." *Small-scale Forest Economics, Management and Policy* 4(3): 343-357. <https://doi.org/10.1007/s11842-005-0021-x>.
- Raleigh, Clionadh, and Caitriona Dowd.** 2013. "Governance and Conflict in the Sahel's 'Ungoverned Space.'" *Stability: International Journal of Security and Development* 2(2): 1-17.
- Raphael, I.** 2025. Over 1,000 forest guards graduate in Kwara ahead of anti-terror operations. *Western Post*. <https://www.westernpost.ng/over-1000-forest-guards-graduate-in-kwara-ahead-of-anti-terror-operations/>.
- Rufai, M.A.** 2017. "I Am a Bandit: A Decade of Research in Zamfara State Bandits' Camps." *European Scientific Journal* 13(2): 35-52.
- Sowale, T.** 2025. "Decentralized Policing and the Imperative for State-Level Security in Nigeria." *Federal University of Kashere Journal of Politics and International Relations* 4(1).
- Suleiman, M. D., and B. Maiangwa.** 2017. "Nigeria and the 'Making' of Combative Identities." *African Identities* 15(3): 260-277. <https://doi.org/10.1080/14725843.2017.1291324>.
- Tankebe, Justice.** 2013. "Viewing Things Differently: The Dimensions of Public Perceptions of Police Legitimacy." *Criminology* 51(1): 103-135.

Tyler, Tom R. 2006. *Why People Obey the Law*. Princeton University Press.

Warner, J. 2017. "Nigeria and 'Illusory Hegemony' in Foreign and Security Policymaking: Pax-Nigeriana and the Challenges of Boko Haram." *Foreign Policy Analysis* 13(3): 638-661. <https://doi.org/10.1093/fpa/orw051>.

Yamane, Taro. 1967. *Statistics: An Introductory Analysis*. 2nd ed. Harper and Row.

Zedner, Lucia. 2009. *Security*. Routledge.

Integrated UAV-Satellite Communication Architecture with NOMA-based Multi-link Connectivity for Secure and Resilient Wireless Networks

MSc. Rexhep MUSTAFOVSKI, Teaching and Research Assistant*

*Military Academy "General Mihailo Apostolski", Goce Delchev University,
st. Vasko Karangelevski nr. 12, 1000 Skopje, North Macedonia

e-mail: redzep.mustafovski@ugd.edu.mk

 <https://orcid.org/0009-0000-3257-0989>

Abstract

This paper proposes an integrated UAV-satellite communication architecture designed to improve wireless connectivity in dynamic, infrastructure-limited, and contested environments. The framework combines UAV relay platforms, satellite communication, LTE links, cloud-based coordination, and NOMA mechanisms to enhance coverage, spectral efficiency, and service continuity. It also addresses security risks such as interception, interference, and communication disruption. The proposed architecture is applicable to tactical communications, emergency response, critical infrastructure protection, and future beyond-5G/6G networks.

Keywords:

UAV Communication; Satellite Communication; NOMA;
Tactical Networks; Secure Communication; 6G.

Article info

Received: 5 March 2026; Revised: 2 April 2026; Accepted: 4 June 2026; Available online: 30 June 2026

Citation: Mustafovski, R. 2026. "Integrated UAV-Satellite Communication Architecture with NOMA-based Multi-link Connectivity for Secure and Resilient Wireless Networks." *Bulletin of "Carol I" National Defence University*, 15(2): 185-212. <https://doi.org/10.53477/2284-9378-26-24>



© „Carol I” National Defence University Publishing House

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution ([CC BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/))

1. Introduction

The rapid development of wireless technologies has significantly transformed modern information exchange, enabling continuous connectivity across civilian, industrial, and defense sectors. In recent years, Unmanned Aerial Vehicles (UAVs) have emerged as an important component of next-generation wireless systems due to their mobility, rapid deployment capability, and ability to operate in environments where conventional infrastructure is unavailable, damaged, or operationally limited. UAV-assisted platforms can provide temporary or persistent network coverage in remote geographic regions, disaster-affected zones, military operations, and emergency response scenarios where traditional terrestrial systems cannot ensure reliable service availability ([Vinogradov et al. 2019](#); [Liu et al. 2020](#)).

The integration of UAV platforms into wireless networks has attracted considerable attention from both the research community and industry because of their ability to support adaptive network deployment and dynamic resource management. UAVs can function as aerial base stations, relay nodes, or wireless gateways that extend the reach of terrestrial infrastructure and enhance service delivery in challenging operational conditions. Their capability to maintain line-of-sight links with ground terminals and neighboring aerial nodes makes them suitable for high-data-rate transmission, reduced propagation loss, and improved signal stability in urban, rural, and infrastructure-constrained environments ([Cui et al. 2020](#); [Greenberg, Bar, and Klodzh 2019](#)).

The continuous evolution of fifth-generation (5G) and future sixth-generation (6G) wireless systems has further increased the importance of UAV-assisted architectures. Modern wireless environments require high spectral efficiency, low latency, reliable connectivity, and flexible network management to support large numbers of connected devices and mission-critical services. UAV-enabled platforms contribute to these requirements by providing adaptive network structures capable of dynamically allocating resources according to environmental conditions, user distribution, and operational demands ([Duong et al. 2022](#); [Lu et al. 2021](#)).

Beyond extending network coverage, UAV platforms facilitate the integration of heterogeneous wireless technologies within a unified networking framework. Hybrid architectures may combine terrestrial cellular infrastructure, satellite systems, and local wireless data links to ensure uninterrupted service under varying operational conditions. Satellite systems provide wide-area and long-distance connectivity, while cellular infrastructure offers high-capacity access in urban and semi-urban regions. The combination of these technologies with UAV relay platforms enables the development of resilient networking solutions capable of supporting both civilian and defense-related missions, including tactical operations and critical infrastructure protection ([Xu, Kishk, and Alouini 2023](#); [Xiong, Chen, and Ying 2025](#)).

Recent research has also emphasized the importance of advanced multiple-access mechanisms for improving network efficiency in dense wireless environments. Non-Orthogonal Multiple Access (NOMA) has been proposed as an effective technique for enhancing spectral efficiency and supporting simultaneous access by multiple users within the same frequency resources. Unlike conventional orthogonal schemes, NOMA allows multiple users to share identical channels through power-domain multiplexing and differentiated power allocation. This approach increases network capacity and throughput while improving spectrum utilization. The integration of NOMA with UAV-assisted systems enables aerial platforms to support larger numbers of connected users and achieve higher performance in dynamic operational scenarios ([Shen and Ochiai 2021](#); [Kieu-Xuan and Le-Thi 2024](#)).

Despite these advantages, several technical and security challenges remain associated with the deployment and management of UAV-assisted wireless systems. One of the major challenges involves efficient resource coordination in highly dynamic environments characterized by UAV mobility, changing network topologies, and variable user distribution. Effective interaction between aerial relay nodes, terrestrial infrastructure, satellite systems, and centralized management platforms is required to maintain stable connectivity and optimize resource utilization ([Qian et al. 2023](#); [Jung et al. 2023](#)).

Security represents another critical concern. Due to the broadcast nature of wireless channels and the exposed operational characteristics of aerial platforms, UAV-enabled networks are vulnerable to signal interception, jamming, malicious interference, and unauthorized access. Adversarial entities may attempt to disrupt network operations, intercept sensitive information, or degrade service availability during tactical and mission-critical activities. Consequently, the development of secure and resilient UAV communication architectures has become an important research direction in both civilian applications and defense-oriented network environments ([Michailidis et al. 2022](#); [Mustafovski 2025](#)).

The integration of satellite systems, UAV relay platforms, and advanced wireless access mechanisms provides a promising approach for addressing many of these operational and security challenges. Multi-layer architectures combining aerial, terrestrial, and satellite segments can enhance network robustness, extend coverage, and maintain dependable service delivery in complex environments. Such solutions are particularly applicable to emergency response coordination, environmental monitoring, intelligent transportation systems, wireless sensor networks, border surveillance, tactical communications, and operations conducted in infrastructure-degraded regions ([Hu et al. 2024](#); [Gao et al. 2025](#)).

In this context, the development of integrated UAV-assisted networking architectures represents an important research direction for future wireless systems. By combining heterogeneous communication technologies, advanced user-access mechanisms, and centralized coordination, it is possible to create scalable and adaptive infrastructures

capable of supporting diverse operational requirements. Recent research efforts have focused on enabling efficient interaction between UAV platforms, satellite systems, terrestrial infrastructure, and cloud-based management solutions in order to improve reliability, operational effectiveness, and overall network performance ([Hu et al. 2026](#); [Eskandari and Savkin 2024](#); [Mustafovski, Risteski, and Shuminoski 2025a](#)).

This paper presents an integrated UAV-satellite communication architecture that incorporates multi-link connectivity, centralized network control, and NOMA-based user access mechanisms within a unified networking environment. The proposed framework is designed to support reliable and secure wireless services in tactical operations, emergency response scenarios, disaster-affected regions, and infrastructure-limited environments. In addition, the study introduces a conceptual threat-aware model that considers signal interception, malicious interference, and service continuity within heterogeneous wireless networks.

2. Security and Defense Relevance

Reliable communication infrastructure represents one of the fundamental operational requirements in modern security and defense environments. Military operations, crisis response activities, border surveillance missions, and critical infrastructure protection increasingly depend on the availability of secure, adaptive, and resilient wireless communication systems capable of maintaining operational continuity under dynamic and contested conditions. Conventional terrestrial communication infrastructure may become unavailable or degraded due to natural disasters, cyber-attacks, physical destruction, electronic warfare activities, or geographic limitations. In such environments, the ability to rapidly establish communication links and maintain uninterrupted information exchange becomes essential for command coordination, situational awareness, and operational decision making ([Li and Shang 2025](#)).

The integration of Unmanned Aerial Vehicles into wireless communication architectures provides important operational advantages for defense and security-related applications. UAV platforms can be rapidly deployed as aerial relay nodes, temporary communication gateways, or airborne access points capable of extending wireless coverage in areas where fixed infrastructure is damaged or inaccessible. Their mobility and elevated operational position enable the establishment of line-of-sight communication links between dispersed operational units, command centers, emergency response teams, and mobile users operating in complex terrain conditions. This capability is particularly important in tactical communication environments where communication continuity must be preserved despite rapidly changing operational conditions and limited infrastructure availability ([Guo and Yang 2022](#)).

The proposed UAV-satellite communication architecture is especially relevant for mission-critical communication scenarios that require resilient multi-layer

communication support. By integrating satellite communication systems, LTE communication infrastructure, local digital communication links, and UAV-based aerial relay platforms, the architecture enables communication redundancy and adaptive communication routing across heterogeneous wireless technologies. Such integration allows operational communication traffic to be redirected through alternative communication pathways when primary communication links experience degradation, interference, or physical disruption. This capability supports communication continuity during military operations, disaster response coordination, search and rescue activities, and emergency management scenarios. Similar multi-link UAV communication concepts integrating satellite, cellular, and cloud-based communication infrastructures have been explored in practical UAV communication architectures such as MAVNet ([Oak Ridge National Laboratory 2020](#)). Furthermore, the integration of NOMA mechanisms with UAV communication platforms has been shown to improve spectral efficiency and support simultaneous multi-user communication in wireless environments characterized by increasing communication demand ([Thi Tam et al. 2023](#)).

Another important aspect of the proposed framework is its relevance to communication security and operational resilience in contested wireless environments. Modern defense communication systems are increasingly exposed to threats such as communication jamming, signal interception, malicious interference, and unauthorized network access. Adversarial entities may attempt to disrupt communication availability or compromise sensitive operational information transmitted through wireless communication channels ([Michailidis et al. 2022](#); [Mustafovski 2025](#)). The architecture presented in this study incorporates conceptual threat-aware communication modeling that considers interference sources, eavesdropping scenarios, and communication disruption attempts within the wireless environment. The integration of multiple communication technologies and centralized network coordination improves the ability of the communication system to maintain operational functionality even under degraded or hostile communication conditions ([Qian et al. 2023](#); [Jung et al. 2023](#); [Mustafovski, Risteski, and Shuminoski 2025b](#)).

The incorporation of Non-Orthogonal Multiple Access mechanisms further enhances the operational applicability of the framework in dense communication environments where large numbers of users and communication devices require simultaneous network access. Tactical operations, emergency response deployments, and critical infrastructure monitoring systems often involve communication congestion caused by multiple active users operating within limited communication resources. NOMA-based communication improves spectral efficiency and enables more efficient utilization of wireless communication channels, thereby supporting increased communication capacity and improved operational coordination ([Shen and Ochiai 2021](#); [Kieu-Xuan and Le-Thi 2024](#); [Thi Tam et al. 2023](#)).

Overall, the proposed integrated UAV-satellite communication architecture provides

a scalable and operationally relevant framework for supporting secure and resilient wireless communication in defense, security, and crisis management environments characterized by dynamic operational conditions, infrastructure limitations, and increased communication security challenges (Xu, Kishk, and Alouini 2023; Eskandari and Savkin 2024; Mustafovski, Risteski, and Shuminoski 2025c).

3. Research Hypotheses

The increasing integration of Unmanned Aerial Vehicles, satellite communication systems, heterogeneous wireless technologies, and advanced multiple access mechanisms within modern wireless communication environments has introduced new opportunities for improving communication resilience, operational continuity, and network flexibility in complex operational scenarios. However, the effectiveness of such integrated communication architectures depends on the ability of the system to maintain reliable connectivity, efficiently allocate communication resources, and preserve communication continuity under dynamic environmental and operational conditions. In order to examine the operational capabilities and communication performance of the proposed UAV-satellite communication architecture, this study establishes a set of research hypotheses associated with communication availability, spectral efficiency, network resilience, and communication security.

The first research hypothesis assumes that the integration of UAV relay platforms with satellite communication systems, LTE communication infrastructure, and local digital communication links improves communication availability and operational continuity compared with conventional single-link communication architectures. The proposed framework incorporates multiple communication pathways capable of supporting adaptive communication routing and communication redundancy in environments where terrestrial infrastructure may be unavailable, degraded, or exposed to operational disruptions. This hypothesis is particularly relevant for tactical communication environments, emergency response operations, and infrastructure-limited scenarios where communication continuity represents a critical operational requirement.

The second research hypothesis is associated with the implementation of Non-Orthogonal Multiple Access mechanisms within the proposed communication framework. The hypothesis assumes that NOMA-based communication improves spectral efficiency and increases communication capacity by enabling simultaneous communication among multiple users within shared communication resources. The integration of NOMA-based access mechanisms with UAV-assisted communication platforms is expected to support more efficient utilization of available communication bandwidth and improve communication performance in dense wireless communication environments characterized by large numbers of connected users and communication devices.

The third research hypothesis focuses on the operational resilience of the integrated communication architecture under dynamic communication conditions and potential communication disruptions. The hypothesis assumes that the combination of satellite communication systems, UAV relay platforms, and centralized network coordination reduces communication outage probability and improves communication stability in environments exposed to interference, communication congestion, or infrastructure degradation. The proposed multi-layer communication architecture is expected to provide adaptive communication support through alternative communication pathways capable of maintaining operational connectivity during communication failures or degraded network conditions.

The fourth research hypothesis examines the role of centralized network management and adaptive communication coordination within the proposed framework. This hypothesis assumes that cloud-based network coordination and dynamic communication link selection improve communication reliability, optimize communication resource allocation, and reduce the operational impact of communication interference and malicious disruption attempts. The integration of centralized network control mechanisms is expected to support efficient interaction between aerial communication nodes, terrestrial communication infrastructure, and satellite communication systems under varying operational conditions.

The final research hypothesis is related to the security and operational applicability of the proposed architecture within defense and mission-critical communication environments. The hypothesis assumes that the integration of heterogeneous wireless communication technologies and threat-aware communication modeling enhances communication resilience against signal interception, malicious interference, and communication disruption attempts. The proposed framework is expected to support secure and reliable communication operations in tactical environments, disaster response coordination, critical infrastructure protection, and other mission-critical communication scenarios requiring continuous and resilient wireless connectivity.

4 Proposed Architecture and Methodology

4.1. Architecture Overview

The methodological framework proposed in this study is focused on the design and analytical evaluation of an integrated UAV-satellite communication architecture intended to support secure, adaptive, and continuous wireless connectivity in dynamic operational environments. The proposed architecture combines satellite communication systems, aerial relay platforms, terrestrial wireless infrastructure, and Non-Orthogonal Multiple Access-based communication mechanisms within a unified multi-layer communication environment. The framework is developed to support communication continuity in scenarios characterized by infrastructure degradation, communication congestion, operational mobility, and potential

communication threats. Particular emphasis is placed on tactical communication environments, emergency response operations, disaster-affected regions, and infrastructure-limited areas where reliable communication services are essential for operational coordination and information exchange ([Liu et al. 2020](#); [Xu, Kishk, and Alouini 2023](#); [Mustafovski 2025](#)).

The proposed communication architecture is structured as a multi-layer wireless communication environment composed of interconnected aerial, terrestrial, and satellite communication segments coordinated through centralized network management. UAV platforms operate as adaptive aerial relay nodes capable of establishing communication links between mobile users, terrestrial communication infrastructure, and satellite communication systems. By integrating heterogeneous wireless communication technologies within a common operational architecture, the framework enables communication traffic to be dynamically distributed across multiple communication pathways according to network conditions, communication requirements, and operational constraints ([Eskandari and Savkin 2024](#); [Hu et al. 2024](#); [Jung et al. 2023](#)).

Within architecture, UAV relay platforms perform an important operational role by extending communication coverage and supporting communication continuity in environments where direct communication between users and fixed communication infrastructure may not be possible. The elevated operational position of UAV platforms enables the establishment of line-of-sight communication links with ground devices and neighboring communication nodes, thereby reducing signal obstruction and propagation loss caused by buildings, terrain irregularities, vegetation, or infrastructure limitations ([Cui et al. 2020](#); [Greenberg, Bar, and Klodzh 2019](#)). In addition to extending communication range, UAV relay nodes facilitate the interaction between terrestrial communication infrastructure and satellite communication systems, allowing communication services to remain operational under changing environmental and operational conditions ([Hu et al. 2026](#); [Xiong, Chen, and Ying 2025](#); [Li and Shang 2025](#)).

The integrated architecture incorporates satellite communication systems as a long-range communication layer responsible for supporting beyond line-of-sight connectivity and communication continuity in remote or infrastructure-degraded environments. Satellite communication links provide operational redundancy by enabling UAV platforms and centralized network control systems to maintain communication even when terrestrial communication infrastructure experiences disruption or limited coverage ([Li and Shang 2025](#); [Hu et al. 2024](#); [Gao et al. 2025](#)). LTE communication channels and local digital communication links are additionally incorporated within the framework to support short-range and medium-range wireless communication between aerial nodes, mobile users, and terrestrial communication infrastructure. The combination of multiple communication technologies within a unified operational environment improves communication

flexibility, enhances network resilience, and enables adaptive communication routing according to current network conditions and operational requirements (Xu, Kishk, and Alouini 2023; Xiong, Chen, and Ying 2025; Hu et al. 2026).

The architecture also incorporates centralized cloud-based network coordination responsible for monitoring communication conditions, managing communication resources, and coordinating communication flows between UAV relay nodes, terrestrial communication infrastructure, satellite systems, and mobile users. This centralized management approach enables dynamic communication link selection, adaptive routing, and operational coordination across heterogeneous communication technologies (Qian et al. 2023; Jung et al. 2023). Through the integration of multi-link communication support, centralized network coordination, and aerial relay communication mechanisms, the proposed framework is intended to maintain reliable and continuous wireless communication in complex operational environments exposed to mobility, infrastructure limitations, and potential communication disruptions (Eskandari and Savkin 2024; Mustafovski, Risteski, and Shuminoski 2025a).

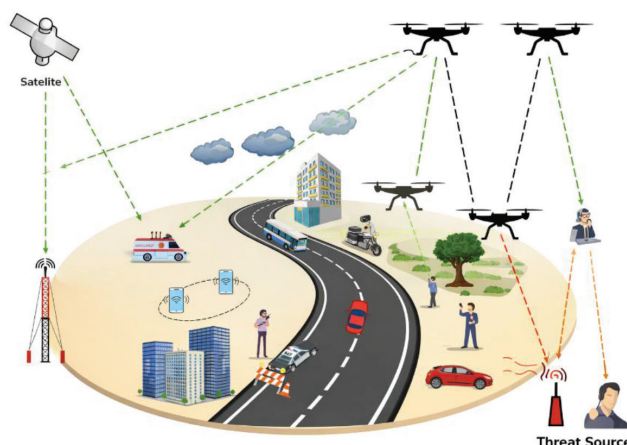


Figure 1 Integrated UAV-satellite Communication Environment for Multi-Layer Wireless Connectivity and Threat Monitoring

Source: Author made.

The figure illustrates an integrated communication environment in which UAV platforms interact with satellite systems, terrestrial infrastructure, and mobile users to support wireless connectivity across urban and road environments. UAVs operate as aerial relay nodes that extend communication coverage and enable data transmission between ground users, communication towers, and centralized network systems. Architecture also represents potential threat sources and eavesdropping activities within the communication environment, highlighting the importance of resilient and secure wireless communication frameworks in complex operational scenarios.

4.2. UAV Relay Communication Layer

Within the proposed communication architecture, UAV platforms operate as adaptive aerial relay nodes responsible for extending wireless communication

coverage, supporting communication continuity, and facilitating data transmission between heterogeneous communication layers. The UAV relay communication layer is designed to enable reliable wireless connectivity in operational environments where direct communication between users and terrestrial infrastructure may be limited, degraded, or temporarily unavailable. By functioning as airborne communication relays, UAV platforms provide dynamic communication support for mobile users, terrestrial communication systems, and centralized network infrastructure operating within complex and changing operational conditions (Liu et al. 2020; Vinogradov et al. 2019; Mustafovski, Risteski, and Shuminoski 2025a).

One of the primary operational advantages of UAV relay platforms is their ability to establish line-of-sight communication links with ground terminals, neighboring aerial nodes, and terrestrial communication infrastructure. The elevated operational position of UAV platforms reduces the impact of physical obstacles such as urban buildings, terrain irregularities, vegetation, and infrastructure obstructions that may degrade communication performance in conventional terrestrial wireless environments (Cui et al. 2020; Greenberg, Bar, and Klodzh 2019). The establishment of line-of-sight communication pathways contributes to reduced signal attenuation, improved signal propagation conditions, and enhanced communication reliability across the wireless communication environment (Duong et al. 2022; Eskandari and Savkin 2024).

The UAV relay communication layer also enables dynamic communication deployment and adaptive network extension according to operational requirements and environmental conditions. UAV platforms can be positioned in areas affected by infrastructure degradation, communication congestion, or limited wireless coverage in order to support temporary or continuous communication services. This capability is particularly important in tactical communication environments, disaster response operations, emergency coordination scenarios, and remote geographic regions where rapid communication deployment and operational mobility are essential. The aerial communication layer, therefore, provides operational flexibility by allowing communication resources to be repositioned dynamically according to mission requirements and communication demand distribution.

Within the proposed framework, UAV relay nodes are additionally responsible for facilitating communication interaction between terrestrial communication infrastructure and satellite communication systems. The aerial communication layer enables data traffic generated by ground users to be transmitted toward centralized network infrastructure through LTE communication channels, local digital communication links, or satellite communication pathways, depending on communication conditions and network availability. This relay functionality enables communication continuity even when one or more communication pathways experience degradation, operational disruption, or limited availability.

The UAV relay communication layer also contributes to communication resilience through multi-node aerial communication coordination. Multiple UAV platforms

can operate simultaneously within the communication environment to support communication redundancy, increase operational coverage, and improve communication reliability across large geographic areas. Communication traffic may be dynamically distributed between aerial relay nodes according to communication quality indicators, operational requirements, and network load conditions. Through the integration of adaptive aerial relay functionality, line of sight communication support, and multi-link communication coordination, the proposed UAV communication layer improves operational connectivity and enables stable wireless communication in dynamic and infrastructure-constrained operational environments.

4.3. Satellite and LTE Communication Integration

The proposed communication architecture integrates satellite communication systems, LTE communication infrastructure, and local digital communication links within a unified multi-layer wireless communication environment designed to support reliable and continuous operational connectivity. The integration of heterogeneous communication technologies enables the architecture to maintain communication availability across varying operational conditions, geographic environments, and infrastructure limitations. By combining multiple communication pathways within the same operational framework, the proposed system supports adaptive communication routing, communication redundancy, and dynamic network coordination between aerial relay platforms, terrestrial communication infrastructure, and centralized network management systems ([Xu, Kishk, and Alouini 2023](#); [Eskandari and Savkin 2024](#)).

Satellite communication systems represent the long-range communication component of the proposed framework and provide beyond-line-of-sight communication support between UAV relay platforms and centralized cloud-based infrastructure. Satellite communication links enable operational connectivity in remote geographic regions, disaster-affected environments, rural areas, maritime environments, and tactical communication scenarios where terrestrial communication infrastructure may be unavailable or degraded. Through the integration of satellite communication systems, UAV relay nodes are capable of transmitting operational data, communication traffic, and network status information directly toward centralized communication infrastructure regardless of terrestrial network availability. This communication capability improves operational continuity and supports resilient wireless communication in infrastructure-constrained operational environments ([Li and Shang 2025](#); [Hu et al. 2024](#); [Gao et al. 2025](#); [Xiong, Chen, and Ying 2025](#)).

The architecture additionally incorporates LTE communication infrastructure in order to support medium-range wireless communication and integration with existing terrestrial communication networks. LTE communication channels provide connectivity between UAV platforms, mobile users, and ground

access infrastructure operating within urban and semi-urban communication environments. The integration of UAV relay nodes with LTE infrastructure enables wireless coverage extension in regions characterized by weak signal propagation, communication congestion, or limited terrestrial communication access. LTE communication pathways also support rapid communication deployment and enable operational interaction between aerial communication nodes and existing wireless communication infrastructure without requiring dedicated standalone communication systems (Lu et al. 2021; Liu et al. 2020).

Local digital communication links are incorporated within the architecture to support short-range and high-speed communication between UAV relay platforms and nearby communication devices. These communication links provide low-latency communication support for operational environments where aerial nodes operate in close proximity to mobile users, emergency response units, or tactical communication teams. Local digital communication pathways enable rapid data transmission and support efficient communication exchange between operational nodes requiring immediate information transfer and localized communication coordination.

The integration of satellite communication systems, LTE infrastructure, and local digital communication links enables the establishment of a multi-link communication environment capable of supporting adaptive communication routing and communication redundancy. Communication traffic generated by ground users or operational devices may be dynamically redirected through alternative communication pathways according to network availability, communication quality indicators, operational priorities, and environmental conditions. In situations where LTE communication infrastructure becomes unavailable, or communication quality degrades due to interference or infrastructure disruption, UAV relay nodes can redirect communication traffic through satellite communication channels or local digital communication links in order to preserve operational connectivity.

The proposed architecture also incorporates centralized network coordination mechanisms responsible for monitoring communication conditions and managing communication link selection across heterogeneous communication technologies. The centralized network management system evaluates communication parameters such as signal quality, communication latency, link availability, and operational communication status in order to determine the most suitable communication pathway for data transmission. This adaptive communication coordination improves communication stability, enhances operational flexibility, and enables communication continuity during dynamic operational conditions and communication disruption scenarios.

Through the integration of satellite communication systems, LTE communication infrastructure, and local digital communication pathways, the proposed framework establishes a resilient multi-layer communication architecture capable of supporting

secure and continuous wireless communication in tactical operations, emergency response environments, disaster recovery scenarios, and infrastructure-limited operational conditions.

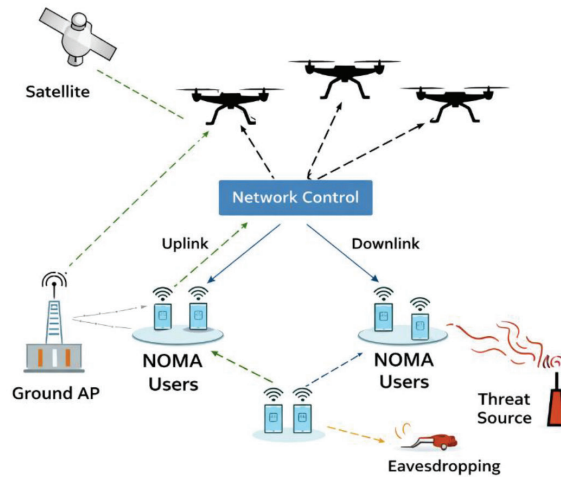


Figure 2 UAV-satellite Communication Architecture with NOMA-Based User Access and Network Control
Source: Author made

The figure presents the proposed UAV-assisted communication architecture that integrates satellite connectivity, aerial relay platforms, ground access infrastructure, and centralized network control. UAV nodes facilitate uplink and downlink communication between NOMA-based users and the network infrastructure, while satellite links support extended connectivity. The architecture also illustrates potential security threats such as interference sources and eavesdropping, highlighting the need for secure and resilient wireless communication frameworks.

4.4. Centralized Cloud-Based Network Coordination

The proposed communication architecture incorporates a centralized cloud-based network coordination layer responsible for communication monitoring, resource allocation, communication routing, and operational management across the integrated wireless communication environment. The centralized coordination mechanism functions as the primary network control component that supervises communication interaction between UAV relay platforms, satellite communication systems, LTE infrastructure, local digital communication links, and mobile user devices. Through centralized operational coordination, the architecture enables adaptive communication management capable of maintaining stable and continuous communication services under dynamic network conditions and varying operational requirements (Qian et al. 2023; Jung et al. 2023; Eskandari and Savkin 2024).

The centralized network management platform continuously collects communication-related information from aerial relay nodes, terrestrial infrastructure, and connected communication devices in order to evaluate current network conditions and operational communication status. Communication

parameters, including signal quality, communication latency, communication link availability, traffic load distribution, packet transmission conditions, and operational network status, are monitored in real time through the cloud-based coordination environment. The continuous monitoring of communication conditions enables the centralized management system to identify communication degradation, communication congestion, infrastructure limitations, and potential operational disruptions affecting communication performance ([Qian et al. 2023](#); [Lu et al. 2021](#); [Jung et al. 2023](#)).

An important function of the centralized coordination layer involves adaptive communication resource allocation across heterogeneous communication technologies. The network management platform dynamically allocates communication resources according to communication demand, operational priorities, user distribution, and communication quality indicators within the network environment. Communication traffic generated by mobile users and operational devices can be distributed between LTE communication infrastructure, local digital communication pathways, and satellite communication channels according to current network conditions and operational requirements. This adaptive resource allocation mechanism improves communication efficiency and supports balanced utilization of available wireless communication resources.

The centralized coordination framework additionally supports dynamic communication routing between communication nodes operating within the integrated network architecture. UAV relay platforms function as intermediate communication nodes that receive communication traffic from ground users and transmit data through the most suitable communication pathway selected by the centralized network management system. Communication routing decisions are based on operational communication parameters, including communication latency, signal quality, communication availability, network congestion, and communication link stability. In situations where primary communication links experience degradation or become unavailable, the centralized coordination layer can redirect communication traffic through alternative communication pathways in order to maintain communication continuity and operational connectivity.

The cloud-based network management system also contributes to operational communication resilience through coordinated multi-link communication control and network redundancy management. Communication links operating within the architecture are continuously evaluated in order to detect communication interruptions, degraded transmission conditions, or abnormal operational behavior. Through centralized communication coordination, the network management platform can initiate adaptive communication link selection and dynamic routing adjustments that improve operational stability and reduce the impact of communication disruptions caused by infrastructure failure, environmental conditions, or malicious interference.

In addition to communication management and routing coordination, the centralized cloud-based framework enables operational synchronization between aerial communication nodes and terrestrial communication infrastructure. The network management system coordinates communication interaction between UAV relay platforms operating within different geographic regions and communication layers, thereby supporting scalable communication deployment and efficient operational coordination across large communication environments. This centralized operational approach improves communication reliability, enhances network flexibility, and enables efficient management of integrated UAV-satellite communication environments characterized by mobility, infrastructure variability, and heterogeneous wireless communication technologies.

4.5. NOMA-Based Multi-User Communication

The proposed communication architecture incorporates Non-Orthogonal Multiple Access (NOMA) as the primary multi-user access mechanism between UAV relay platforms and ground users. The purpose of integrating NOMA within the UAV-assisted communication layer is to improve spectral efficiency, increase simultaneous user access, and support efficient communication in dense operational environments where multiple users require connectivity through limited wireless spectrum resources. In contrast to orthogonal multiple access techniques, where users are separated through different time, frequency, or code resources, NOMA enables multiple users to share the same frequency resource by assigning different power levels according to their channel conditions ([Shen and Ochiai 2021](#); [Kieu-Xuan and Le-Thi 2024](#); [Thi Tam et al. 2023](#)).

Within the proposed architecture, UAV platforms operate as aerial access points that serve multiple ground users through power-domain NOMA. Users located within the coverage area of a UAV relay node are grouped into NOMA clusters according to their channel quality, distance from the UAV, and communication requirements. A user with weaker channel conditions, usually located farther from the UAV or affected by stronger propagation loss, is assigned a higher transmission power coefficient. A user with stronger channel conditions, usually located closer to the UAV or experiencing better signal quality, is assigned a lower transmission power coefficient. This power allocation principle enables both users to share the same communication resource while maintaining decodable signal separation at the receiver side ([Shen and Ochiai 2021](#); [Kieu-Xuan and Le-Thi 2024](#)).

For a NOMA cluster with N users, the transmitted signal from the UAV relay node can be represented as:

$$x = \sum_{i=1}^N \sqrt{a_i P_t} s_i \quad (1)$$

where x denotes the superimposed transmitted signal, P_t is the total

transmission power of the UAV relay node, a_i is the power allocation coefficient assigned to the user i , and s_i represents the information signal intended for the user i .

The power allocation coefficients must satisfy the following condition:

$$\sum_{i=1}^N a_i = 1, 0 < a_i < 1 \quad (2)$$

In this model, higher power allocation is assigned to users with weaker channel gains, while lower power allocation is assigned to users with stronger channel gains. If user j has weaker channel conditions than the user k , the allocation follows:

$$|h_j|^2 < |h_k|^2 \Rightarrow a_j > a_k \quad (3)$$

where h_j and h_k represent the channel coefficients of the corresponding users.

The received signal at the user i can be expressed as:

$$y_i = h_i x + n_i \quad (4)$$

where y_i is the received signal, h_i is the channel coefficient between the UAV relay node and the user i , and n_i represents additive noise. The received signal, therefore, contains the superimposed data streams of all users within the same NOMA cluster.

In order to recover the intended user data, Successive Interference Cancellation (SIC) is applied at the receiver side. Users with stronger channel conditions decode and remove the signals of weaker users before decoding their own information. This decoding process enables efficient separation of superimposed signals and supports simultaneous communication within the same wireless resource block.

The Signal-to-Interference-plus-Noise Ratio (SINR) for the user i can be generally expressed as:

$$SINR_i = \frac{a_i P_t |h_i|^2}{\sum_{k=i+1}^N a_k P_t |h_i|^2 + N_0} \quad (5)$$

where N_0 represents the noise power, and the interference term corresponds to the remaining non-cancelled user signals within the NOMA cluster.

Based on the achieved SINR, the data rate for the user i can be expressed as:

$$R_i = B \log_2(1 + SINR_i) \quad (6)$$

where B denotes the available communication bandwidth.

The total achievable throughput of the NOMA cluster can then be represented as:

$$R_{sum} = \sum_{i=1}^N R_i \quad (7)$$

These equations provide a formal basis for evaluating the spectral efficiency and communication capacity of the NOMA-based UAV communication layer. The integration of NOMA enables the proposed architecture to support multiple users within the same bandwidth resource, which is particularly important in tactical communication environments, emergency response deployments, and critical infrastructure monitoring scenarios where communication demand may increase rapidly, and available spectrum resources may be limited.

The NOMA-based communication layer also supports adaptive communication management through centralized network coordination. The cloud-based network control system can use channel quality indicators, user distance, traffic demand, and link availability to support user grouping and power allocation decisions. By combining UAV relay communication with power domain NOMA, the proposed architecture improves simultaneous user access, enhances spectral efficiency, and supports reliable communication service delivery in dynamic multiuser wireless environments.

4.6. Channel Model and Simulation Parameters

The proposed communication framework incorporates multiple wireless communication links operating across aerial, terrestrial, and satellite communication layers. In order to evaluate the operational behavior of the integrated architecture, the communication environment is represented through a multi-layer channel model that considers communication interaction between UAV relay platforms, mobile users, LTE communication infrastructure, and satellite communication systems. The communication model is intended to represent realistic operational conditions characterized by mobility, variable communication quality, infrastructure limitations, and heterogeneous communication technologies (Xu, Kishk, and Alouini 2023; Hu et al. 2024; Xiong, Chen, and Ying 2025; Eskandari and Savkin 2024).

The first communication segment within the proposed framework consists of UAV-to-user communication links established between aerial relay platforms and ground users operating within the communication coverage area of the UAV nodes. These communication links primarily support short-range and medium-range wireless communication between UAV relay platforms and mobile devices, tactical units, emergency response teams, and operational communication terminals. Due to the elevated operational position of UAV platforms, the communication environment is characterized predominantly by line-of-sight signal propagation conditions. However, communication quality may still be affected by environmental obstacles, urban infrastructure density, terrain irregularities, signal attenuation, and user

mobility. The UAV-to-user communication layer also incorporates NOMA-based user access mechanisms in order to support simultaneous communication among multiple users sharing identical communication resources.

The second communication segment involves UAV to LTE communication links established between aerial relay platforms and terrestrial cellular communication infrastructure. LTE communication pathways provide medium-range wireless connectivity and enable UAV relay nodes to integrate with existing terrestrial communication networks. This communication layer supports communication traffic exchange between aerial platforms and ground-based communication infrastructure operating in urban, semi-urban, and partially infrastructure-constrained environments. LTE communication quality may vary according to network congestion, communication load distribution, signal propagation conditions, and infrastructure availability. The integration of LTE communication channels within the proposed architecture enables adaptive communication routing and improves operational communication flexibility by allowing UAV relay platforms to utilize existing wireless communication infrastructure whenever available.

The third communication segment consists of UAV-to-satellite communication links responsible for long-range and beyond line-of-sight communication between aerial relay nodes and centralized cloud-based network infrastructure. Satellite communication systems provide communication continuity in operational environments where terrestrial communication infrastructure is unavailable, degraded, or operationally inaccessible. This communication layer is particularly important for remote geographic regions, disaster-affected environments, maritime communication scenarios, and tactical operations requiring resilient long-distance communication support. Although satellite communication introduces a higher propagation delay compared with terrestrial communication systems, it significantly improves communication availability and operational coverage across large geographic regions.

The integrated communication environment additionally incorporates local digital communication links operating between nearby UAV nodes and operational devices within localized communication areas. These communication links support low-latency data exchange and rapid communication interaction between aerial communication platforms and nearby operational units requiring high-speed communication services. The integration of local digital communication pathways further contributes to communication redundancy and enables adaptive multi-link communication support within the operational environment.

The simulation environment considers dynamic communication conditions in which communication quality, link availability, and operational network conditions may vary according to user mobility, UAV positioning, communication congestion, environmental interference, and infrastructure availability.

Communication interaction between network nodes is evaluated through uplink and downlink communication flows established across aerial, terrestrial, and satellite communication layers. The integrated channel model, therefore, enables the analysis of communication continuity, adaptive routing behavior, operational communication resilience, and multi-link connectivity within heterogeneous UAV-assisted wireless communication environments.

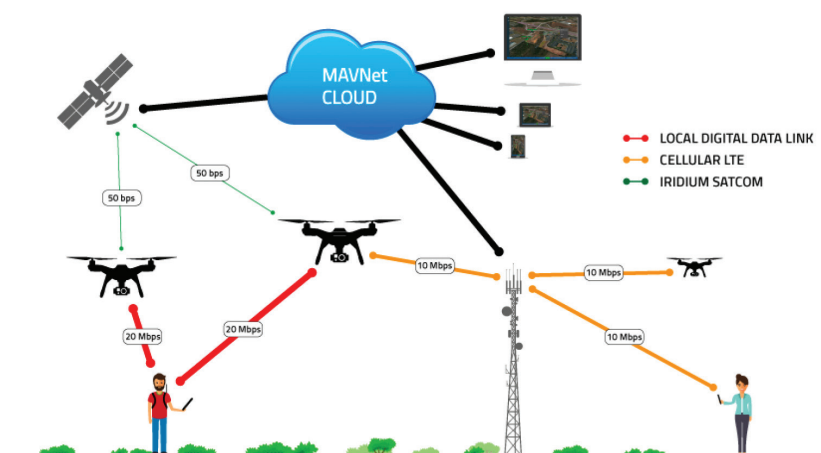


Figure 3 MAVNet Cloud-Based Multi-Link Communication Architecture for Global UAV Connectivity

Source: Adapted by the author from Horizon31 LLC and Oak Ridge National Laboratory (ORNL), "Horizon31 Startup Licenses ORNL Global Communication System for Drones" (2020), for academic and research purposes, with full source attribution provided. Available at: <https://www.ornl.gov/news/horizon31-startup-licenses-ornl-global-communication-system-drones>

The figure illustrates the MAVNet communication architecture developed at Oak Ridge National Laboratory, which enables global control and monitoring of unmanned aerial vehicles through a cloud-based communication system. The architecture integrates multiple communication pathways, including local digital data links, cellular LTE networks, and Iridium satellite communication. UAV platforms connect to a centralized MAVNet cloud server that enables remote operation, data transmission, and coordination of multiple drones through internet connectivity. The use of redundant communication links improves reliability and ensures continuous control of UAV systems even in environments with limited network coverage.

4.7. Threat-Aware Multi-Link Selection Algorithm

The proposed communication framework incorporates a threat-aware multi-link selection mechanism intended to support adaptive communication routing and communication continuity within dynamic wireless communication environments exposed to infrastructure degradation, interference, and potential malicious communication activity. The primary objective of the algorithm is to continuously evaluate the operational status of available communication pathways and dynamically select the most suitable communication link for data transmission

according to current communication conditions and operational requirements. The algorithm operates within the centralized cloud-based network coordination layer and supervises communication interaction between UAV relay platforms, LTE communication infrastructure, satellite communication systems, and local digital communication links (Qian et al. 2023; Jung et al. 2023; Michailidis et al. 2022; Mustafovski, Risteski, and Shuminoski 2025b).

The threat-aware communication model is developed to address operational challenges associated with wireless communication environments characterized by signal attenuation, communication congestion, malicious interference, communication jamming, and potential signal interception attempts. Since the proposed architecture integrates heterogeneous communication technologies operating under varying communication conditions, the communication management system must continuously determine which communication pathway can provide the highest operational communication stability and communication availability. The multi-link selection process, therefore, evaluates communication links according to communication quality indicators and threat-related operational conditions detected within the communication environment.

The algorithm continuously monitors operational communication parameters, including signal quality, communication latency, communication link availability, packet transmission conditions, communication congestion levels, and detected interference intensity across all available communication pathways. LTE communication links, satellite communication channels, and local digital communication pathways are periodically evaluated through the centralized network coordination system in order to identify communication degradation or abnormal operational behavior that may affect communication continuity. Communication links experiencing excessive communication delay, signal degradation, increased packet loss, or detected interference are classified as degraded communication pathways and assigned a lower operational communication priority during the communication routing process.

Within the operational communication environment, UAV relay nodes transmit communication status information and network condition indicators toward the centralized cloud-based coordination system. The centralized management platform processes the collected communication information and dynamically determines the most appropriate communication pathway for operational data transmission. In situations where terrestrial LTE communication infrastructure remains operational, and communication quality indicators satisfy required communication thresholds, communication traffic is primarily routed through LTE communication channels in order to reduce communication delay and improve communication efficiency. However, if LTE communication conditions deteriorate due to infrastructure disruption, network congestion, malicious interference, or communication outages, the algorithm redirects operational communication traffic toward satellite

communication systems or local digital communication pathways in order to maintain communication continuity.

The threat-aware communication model also considers the presence of passive and active communication threats operating within the wireless communication environment. Passive threats include unauthorized signal interception and communication monitoring attempts, while active threats include communication jamming, malicious interference generation, and communication disruption attempts targeting wireless communication links. Communication pathways exposed to increased interference intensity or abnormal communication activity are dynamically deprioritized during the communication selection process in order to reduce the operational impact of malicious communication behavior. This adaptive communication coordination improves communication resilience and enables the architecture to maintain operational functionality under degraded or contested wireless communication conditions.

The operational flow of the proposed multi-link selection mechanism can be summarized through several sequential communication management stages. First, the centralized network coordination layer continuously monitors all available communication links and collects communication performance indicators from UAV relay platforms and network infrastructure components. Second, communication quality parameters, including signal quality, communication latency, communication availability, and detected interference levels, are evaluated for each communication pathway. Third, communication links that fail to satisfy operational communication requirements are temporarily deprioritized within the communication routing process. Fourth, the communication pathway exhibiting the highest operational communication stability and communication quality is selected for data transmission. Finally, the communication routing process is dynamically updated whenever communication conditions change or communication degradation is detected within the operational environment.

The integration of the threat-aware multi-link selection mechanism significantly improves the operational resilience of the proposed UAV-satellite communication architecture. By combining adaptive communication routing, centralized communication coordination, and multi-link communication redundancy, the framework supports continuous wireless communication in tactical operations, emergency response deployments, infrastructure-degraded environments, and operational scenarios exposed to communication interference and malicious communication threats.

5. Results and Discussion

The analytical and conceptual evaluation of the proposed UAV-satellite architecture highlights the operational advantages of integrating UAV relay platforms, satellite

systems, LTE infrastructure, local digital links, and NOMA-based user access mechanisms within a unified wireless networking framework. The proposed solution enables adaptive coordination across heterogeneous technologies and supports reliable service delivery in environments characterized by infrastructure limitations, network congestion, operational mobility, and potential security threats. It should be emphasized that the present study provides an analytical assessment of the proposed framework rather than a full numerical simulation. The evaluation focuses on service continuity, multi-link connectivity, adaptive routing capabilities, spectral efficiency, and operational robustness in comparison with conventional architectures that rely primarily on fixed terrestrial infrastructure.

One of the most significant outcomes of the proposed framework is the establishment of a multi-layer networking environment that integrates aerial relay nodes, terrestrial wireless infrastructure, and satellite systems within a single operational architecture. In conventional wireless networks, connectivity frequently depends on fixed infrastructure such as cellular base stations, communication towers, or wired backbone systems. In contrast, the proposed framework incorporates UAV relay platforms as adaptive aerial nodes capable of dynamically extending coverage and maintaining network operation in environments where terrestrial infrastructure may be degraded, unavailable, or physically inaccessible. Due to their elevated operational position, UAV relay platforms maintain line-of-sight links with both ground users and infrastructure components, thereby reducing signal attenuation and improving service quality in urban, rural, and infrastructure-constrained environments.

The integration of satellite systems further enhances operational robustness by enabling beyond-line-of-sight connectivity between UAV relay platforms and centralized network infrastructure. Satellite links support long-range connectivity and provide redundancy during scenarios characterized by LTE degradation, infrastructure disruption, or service outages affecting terrestrial wireless networks. When terrestrial infrastructure becomes unavailable, the adaptive multi-link coordination mechanism redirects traffic toward satellite channels in order to preserve network operation. Although satellite links introduce higher latency compared with terrestrial technologies, their integration significantly improves service availability and reduces outage probability in remote geographic regions, disaster-affected environments, and defense-oriented operational scenarios.

Another important outcome of the proposed framework is the integration of heterogeneous multi-link technologies, including local digital links, LTE channels, and satellite systems operating simultaneously within the same networking environment. Each layer provides distinct operational characteristics in terms of latency, coverage, and capacity. Local digital links support low-latency and high-speed data exchange between nearby UAV nodes and operational devices. LTE channels provide medium-range connectivity and integration with existing terrestrial infrastructure, while satellite systems offer long-range support and redundancy

across large geographic areas. The availability of multiple transmission paths enables adaptive routing and improves overall network robustness by compensating for degradation or interruption affecting individual links.

The implementation of NOMA-based access mechanisms also contributes significantly to the efficiency of the proposed architecture. In conventional orthogonal systems, resources are allocated separately to individual users, limiting simultaneous access and reducing spectral utilization efficiency in dense environments. Within the proposed framework, NOMA enables multiple users to share identical resources through power-domain multiplexing and adaptive power allocation. Users experiencing weaker channel conditions receive higher transmission power coefficients, while users with stronger channel conditions apply Successive Interference Cancellation to separate superimposed signals. This approach improves spectral efficiency, increases system capacity, and enables UAV relay platforms to support a larger number of connected devices within limited spectrum resources. These advantages are particularly relevant in tactical operations, emergency response deployments, and infrastructure-constrained scenarios characterized by increased traffic demand.

The comparative analysis indicates that the proposed framework differs from existing UAV communication architectures through the integration of UAV relay communication, satellite communication support, LTE connectivity, NOMA-based

TABLE 1. Comparative Analysis of UAV Communication Architectures

Feature	MAVNet Cloud Architecture	UAV-satellite NOMA Architecture	Integrated Proposed Framework
Communication Control	Cloud-based centralized control	Network control center	Integrated cloud and network control
UAV Role	Remote drone operation and monitoring	Aerial relay nodes for NOMA users	Multi-functional aerial communication relays
Communication Links	Local digital link, LTE, satellite	Satellite, UAV links, ground access points	Local digital link, LTE, satellite, UAV relay
User Access Mechanism	Conventional communication access	NOMA-based user communication	NOMA-based multi-user connectivity
Coverage Range	Global connectivity through the internet	Extended coverage through UAV relay	Multi-layer coverage, including satellite and aerial networks
Network Resilience	Redundant communication pathways	UAV relay communication redundancy	Multi-link redundant communication architecture
Security Consideration	Not explicitly modeled	Includes threat source and eavesdropping scenarios	Integrated threat awareness and resilient communication design
Application Domains	UAV fleet management and remote control	Wireless communication research and user access modeling	Emergency response, smart infrastructure, tactical communication

multiuser communication, centralized cloud-based network coordination, and threat-aware adaptive routing within a unified operational communication architecture. Unlike conventional communication frameworks primarily focused on isolated communication functionalities, the proposed architecture incorporates communication redundancy, adaptive multi-link routing, and operational threat awareness intended for tactical and infrastructure-constrained communication environments.

Conclusions

The increasing dependence on continuous wireless connectivity across civilian, emergency response, and defense environments has intensified the need for architectures capable of maintaining reliable network operation under dynamic and infrastructure-constrained conditions. This study presented an integrated UAV-satellite architecture that combines UAV relay platforms, satellite systems, LTE infrastructure, local digital links, centralized cloud-based coordination, and NOMA-based multiuser access within a unified networking framework. The proposed solution was designed to support adaptive routing, network redundancy, and operational continuity in environments characterized by congestion, infrastructure degradation, mobility, and potential security threats.

The analytical and conceptual evaluation demonstrated that the integration of UAV relay platforms with heterogeneous wireless technologies enhances operational flexibility and enables service continuity across multiple networking layers. UAV relay nodes function as adaptive aerial platforms capable of extending coverage and maintaining line-of-sight connectivity between mobile users, terrestrial infrastructure, and centralized network systems. The incorporation of satellite support further enables beyond-line-of-sight connectivity and improves service availability in remote geographic regions, disaster-affected environments, and tactical scenarios where terrestrial infrastructure may be unavailable or degraded.

The proposed multi-link architecture also demonstrated significant operational advantages through the simultaneous integration of LTE channels, satellite systems, and local digital links. The availability of multiple transmission paths enabled adaptive routing and enhanced network robustness through redundant connectivity mechanisms. During LTE degradation or infrastructure disruption, the threat-aware coordination mechanism redirected traffic toward satellite pathways, thereby preserving network operation and reducing the probability of service interruption. This capability is particularly important for defense operations, emergency response missions, and critical infrastructure protection, where uninterrupted information exchange is essential for operational effectiveness.

The implementation of NOMA-based access mechanisms further improved system efficiency. Through power-domain multiplexing and adaptive power allocation, multiple users were able to share identical spectrum resources while maintaining

efficient bandwidth utilization. Users experiencing weaker channel conditions received higher transmission power coefficients, whereas users with stronger channel conditions applied Successive Interference Cancellation to separate superimposed signals. As a result, the proposed framework improved spectral efficiency and increased system capacity in dense operational environments characterized by high traffic demand and limited spectrum resources.

The study additionally addressed security and resilience through the incorporation of threat-aware coordination mechanisms. The proposed architecture considered challenges such as signal interception, malicious interference, communication jamming, and unauthorized eavesdropping. The threat-aware routing mechanism continuously evaluated network conditions and dynamically adjusted path selection according to link availability, latency, signal degradation, and detected interference levels. Links exposed to adverse conditions were deprioritized, while alternative paths maintained uninterrupted service delivery. This adaptive behavior enhanced network resilience and reduced the operational impact of disruption attempts within contested wireless environments.

The comparative analysis demonstrated that the proposed framework differs from existing UAV networking architectures through the integration of UAV relay functionality, satellite support, LTE connectivity, NOMA-based access, centralized cloud coordination, and adaptive threat-aware routing within a unified operational architecture. Unlike conventional solutions that focus primarily on isolated functionalities or standalone UAV management, the proposed framework incorporates redundancy, adaptive coordination, and security-oriented design principles intended for tactical operations, emergency response coordination, disaster recovery environments, and infrastructure-constrained scenarios.

Overall, the analytical evaluation indicates that the proposed UAV-satellite architecture improves service availability, spectral efficiency, adaptive routing capability, and operational resilience within heterogeneous wireless environments. The framework demonstrates strong applicability for tactical communication systems, emergency response operations, infrastructure monitoring, disaster recovery coordination, and mission-critical environments exposed to infrastructure degradation, network congestion, and potential security threats.

It should be emphasized that the present study provides an analytical and conceptual assessment of the proposed architecture rather than a full numerical simulation. Future research will focus on simulation-based performance validation and comparative evaluation of UAV-only, LTE-only, SATCOM-only, and integrated multi-link architectures using metrics such as latency, throughput, packet loss, service availability, and resilience under interference conditions. Additional research directions include optimization of adaptive routing strategies, experimental

validation in realistic operational environments, and the integration of artificial intelligence-based network management mechanisms for beyond-5G and 6G wireless systems.

References

- Cui, Z., C. Briso-Rodríguez, K. Guan, I. Güvenç, and Z. Zhong.** 2020. "Wideband Air-to-Ground Channel Characterization for Multiple Propagation Environments." *IEEE Antennas and Wireless Propagation Letters* 19(9): 1634-1638. <https://doi.org/10.1109/LAWP.2020.3012889>.
- Duong, T. Q., K. J. Kim, Z. Kaleem, M. P. Bui, and N. S. Vo.** 2022. "UAV Caching in 6G Networks: A Survey on Models, Techniques, and Applications." *Physical Communication* 51: 101532. <https://doi.org/10.1016/j.phycom.2021.101532>.
- Eskandari, M., and A. V. Savkin.** 2024. "Integrating UAVs and RISs in Future Wireless Networks: A Review and Tutorial on IoTs and Vehicular Communications." *Future Internet* 16(12): 433. <https://doi.org/10.3390/fi16120433>.
- Gao, Q., L. Su, J. Fu, and Y. Lin.** 2025. "Successful Transmission Probability Analysis of the Satellite-Maritime Uplink: A Stochastic Geometry Based Approach." *Mobile Networks and Applications* 30(1-2): 115-126. <https://doi.org/10.1007/s11036-025-02441-0>.
- Greenberg, E., A. Bar, and E. Klodzh.** 2019. "LOS Classification of UAV-to-Ground Links in Built-Up Areas." In *Proceedings of the IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS)*, November 4-6, 2019, Tel Aviv, Israel, 1-5. Piscataway, NJ: IEEE.
- Guo, Y., and P. Yang.** 2022. "The Effectiveness of Unmanned Aerial Vehicle (UAV) on Farmlands with Artificial Intelligence (AI) System." In *Proceedings of the 7th International Conference on Financial Innovation and Economic Development (ICFIED 2022)*, January 21-23, 2022, Harbin, China, 1664-1669. Dordrecht: Atlantis Press.
- Hu, X., B. Lin, P. Wang, and X. Lu.** 2026. "LEO Satellite and UAV-Assisted Maritime Internet of Things: Modeling and Performance Analysis for Data Acquisition." *Future Internet* 18(1): 24. <https://doi.org/10.3390/fi18010024>.
- Hu, X., B. Lin, X. Lu, P. Wang, N. Cheng, Z. Yin, and W. Zhuang.** 2024. "Performance Analysis of End-to-End LEO Satellite-Aided Shore-to-Ship Communications: A Stochastic Geometry Approach." *IEEE Transactions on Wireless Communications* 23(9): 11753-11769. <https://ieeexplore.ieee.org/document/10496523>.
- Jung, S., S. Jeong, J. Kang, and J. Kang.** 2023. "Marine IoT Systems with Space-Air-Sea Integrated Networks: Hybrid LEO and UAV Edge Computing." *IEEE Internet of Things Journal* 10(23): 20498-20510. <https://doi.org/10.1109/JIOT.2023.3287196>.
- Kieu-Xuan, T., and A. Le-Thi.** 2024. "UAV-Assisted Cooperative NOMA and OFDM Communication Systems: Analysis and Optimization." *Journal of Sensor and Actuator Networks* 13(1): 18. <https://doi.org/10.3390/jsan13010018>.
- Li, Z., and B. Shang.** 2025. "Fundamentals of Satellite-Maritime Communications: Downlink and Uplink Analysis." *IEEE Transactions on Communications* 73: 2191-2206.

- Liu, D., Y. Xu, J. Wang, J. Chen, K. Yao, Q. Wu, and A. Anpalagan.** 2020. "Opportunistic UAV Utilization in Wireless Networks: Motivations, Applications, and Challenges." *IEEE Communications Magazine* 58(5): 62-68. <https://doi.org/10.1109/MCOM.001.1900687>.
- Lu, X., M. Salehi, M. Haenggi, E. Hossain, and H. Jiang.** 2021. "Stochastic Geometry Analysis of Spatial-Temporal Performance in Wireless Networks: A Tutorial." *IEEE Communications Surveys & Tutorials* 23(4): 2753-2801. <https://doi.org/10.1109/COMST.2021.3104581>.
- Michailidis, E. T., K. Maliatsos, D. N. Skoutas, D. Vouyioukas, and C. Skianis.** 2022. "Secure UAV-Aided Mobile Edge Computing for IoT: A Review." *IEEE Access* 10: 86353-86383.
- Mustafovski, Rexhep, Aleksandar Risteski, and Tomislav Shuminoski.** 2025a. "Challenges and Solutions for Enhancing Drone-to-TOC Communication Performance in Military and Crisis Operations." In *Proceedings of the Third International Conference ETIMA 2025*, September 24-25, 2025, Stip, Republic of North Macedonia. <https://js.ugd.edu.mk/index.php/etima/en/article/view/7236/5853>.
- Mustafovski, Rexhep, Aleksandar Risteski, and Tomislav Shuminoski.** 2025b. "Designing a Secure Communication Framework for UAV-to-TOC Operations in Military and Emergency Environments." In *Proceedings of the Third International Conference ETIMA 2025*, September 24-25, 2025, Stip, Republic of North Macedonia. <https://js.ugd.edu.mk/index.php/etima/en/article/view/7237/5877>.
- Mustafovski, Rexhep, Aleksandar Risteski, and Tomislav Shuminoski.** 2025c. "Simulation-Based Performance Analysis of a Secure UAV-to-TOC Communication Framework in Military and Emergency Operations." In *Proceedings of the Third International Conference ETIMA 2025*, September 24-25, 2025, Stip, Republic of North Macedonia. <https://js.ugd.edu.mk/index.php/etima/en/article/view/7238/5879>.
- Mustafovski, Rexhep.** 2025. "Architectural Framework of a Mission-Centric UAV Communication Platform." *Automation of Technological and Business Processes* 17 (3): 44-58. <https://doi.org/10.15673/atbp.v17i4.3324>.
- Oak Ridge National Laboratory (ORNL).** 2020. "Horizon31 Startup Licenses ORNL Global Communication System for Drones." <https://www.ornl.gov/news/horizon31-startup-licenses-ornl-global-communication-system-drones>.
- Qian, L. P., H. Zhang, Q. Wang, Y. Wu, and B. Lin.** 2023. "Joint Multi-Domain Resource Allocation and Trajectory Optimization in UAV-Assisted Maritime IoT Networks." *IEEE Internet of Things Journal* 10(1): 539-552. <https://doi.org/10.1109/IJOT.2022.3201017>.
- Shen, T., and H. Ochiai.** 2021. "A UAV-Enabled Wireless Powered Sensor Network Based on NOMA and Cooperative Relaying with Altitude Optimization." *IEEE Open Journal of the Communications Society* 2: 21-34. <https://doi.org/10.1109/OJCOMS.2020.3042257>.
- Thi Tam, D., B. Cao Nguyen, T. Manh Hoang, L. The Dung, N. V. Vinh, T. Kim, and W. Lee.** 2023. "Combining FD-UAV and NOMA Technologies in IoT Sensor Network with Millimeter-Wave Communications." *International Journal of Communication Systems*: e5492.

Vinogradov, E., H. Sallouha, S. De Bast, M. M. Azari, and S. Pollin. 2019. "Tutorial on UAV: A Blue Sky View on Wireless Communication." *arXiv Preprint*. arXiv:1901.02306.

Xiong, K., X. Chen, and M. Ying. 2025. "On the Performance of Integrated Satellite–Terrestrial Maritime Communications." *IEEE Internet of Things Journal* 12(17): 36183-36196. <https://doi.org/10.1109/JIOT.2025.3580567>.

Xu, J., M. A. Kishk, and M. S. Alouini. 2023. "Space-Air-Ground-Sea Integrated Networks: Modeling and Coverage Analysis." *IEEE Transactions on Wireless Communications* 22(9): 6298-6313. <https://doi.org/10.1109/TWC.2023.3241341>.

Proliferation of Small Arms and Light Weapons and Insecurity in Northwestern Nigeria: A Review

Mubarak Sulaiman JAMIU*

*Department of Politics and Governance, Kwara State University, Malete, Nigeria

e-mail: mubarak.jamiu@kwasu.edu.ng

 <https://orcid.org/0009-0009-6329-7394>

Abstract

This paper critically reviews the proliferation of Small Arms and Light Weapons (SALW) in Northwestern Nigeria, examining their sources, implications, and connections to rising insecurity. Drawing on a wide range of scholarly and institutional literature, the study highlights the way how both locally fabricated and imported SALW contribute to terrorism, banditry, and cross-border crimes, particularly in states like Zamfara, where herder-farmer tensions have escalated into armed conflict. The review also explores global trends, regional vulnerabilities, and the porous borders that facilitate arms trafficking, while identifying key research gaps such as the gendered impact of SALW and the role of emerging technologies. It concludes by emphasizing the need for targeted policy responses that combine security measures with socio-economic development and regional cooperation.

Keywords:

Insecurity; Northwestern Nigeria; Small Arms and Light Weapons; Arms Proliferation.

Article info

Received: 16 November 2025; Revised: 15 December 2025; Accepted: 22 April 2026; Available online: 30 June 2026

Citation: Jamiu, M.S. 2026. "Proliferation of Small Arms and Light Weapons and Insecurity in Northwestern Nigeria: A Review." *Bulletin of "Carol I" National Defence University*, 15(2): 213-228. <https://doi.org/10.53477/2284-9378-26-25>



© „Carol I” National Defence University Publishing House

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution ([CC BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/))

Introduction

The spread of Small Arms and Light Weapons (SALW) has been one of the most critical issues in world security, especially in areas where the instability is chronic, and the governance systems are weak. In this perspective, the concept of SALW is widely interpreted in accordance with the scheme established by the United Nations as being a weapon that is aimed at individuals and groups. Small arms are usually weapons like pistols and rifles, which can be wielded by an individual, whereas the light weapons, like rocket launchers and other high-impact mechanisms, are supposed to be used by groups or in coordinated efforts. This difference is significant, as it is necessary not only to have a clear conceptual picture but to know the patterns of use, circulation, and influence. Even though there are ongoing regulatory measures, these weapons, both locally produced and imported illegally, still find their way out of the formal state control, and therefore contribute to the escalation of insecurity in various settings.

The effects of the proliferation of SALWs go beyond direct violence, and their impacts on human security, economic growth, and governance are far-reaching. Their proliferation has been associated with continued armed conflicts, loss of human rights, abuse of executive power, and instillation of fear among the targeted groups of people. According to the United Nations Institute for Disarmament Research (2006), although state actors can use these weapons reasonably to protect themselves and their countries, a considerable part of them is controlled by non-state actors, including insurgents and militias, as well as criminal groups. This relationship makes it difficult to preserve state order and disrupts larger peacebuilding and post-conflict recovery efforts. The region of the Northwest is of particular concern in Nigeria. Made up of the states of Kaduna, Kano, Jigawa, Katsina, Sokoto, Kebbi, and Zamfara, the region is one of the most populous and geographically vast regions in the country, having a size of about 216, 065 square kilometers. Having more than 54 million inhabitants, most of whom are Hausa and Fulani descent and mostly subscribe to the Islamic religion (Nigerian Population Census 2019), the area has been facing higher insecurity levels within the past several years.

These security issues are based on a complicated combination of socio-economic and political aspects, such as poverty, underdevelopment, the weakness of borders, insurgency, human trafficking, and the lack of system governance (Okoli and Ioroyer 2014). The continuity of these situations has helped to make violence a normalized condition and increase dependency on SALW in the organized and opportunistic types of conflict. There are domestically produced guns and smuggled guns, which have become the key tools of conflict in violent situations throughout the region (Duperas 2020). Despite the fact that previous researchers have explored the elements of proliferation of arms and insecurity in Nigeria, most of the literature is still fragmented and, in most cases, they fail to provide a logical framework of analysis that incorporates the clarity of the concept with region-specific dynamics. It

is on this basis that this paper takes a systematic literature review in order to critically analyze the proliferation of SALW in Northwestern Nigeria.

The paper aims to elucidate major conceptual questions related to SALW, provide a synthesis of the existing literature, and also cover a gap in the current research. Thus, the research paper seeks to better and more consistently illustrate the way SALW proliferation collides with wider security issues in the area, besides serving as a basis for future empirical and policy-based studies.

Revised Problem Statement

Small Arms and Light Weapons (SALW) proliferation has been the main cause of insecurity in Northwestern Nigeria since its unregulated spread has seriously weakened the safety of the population, empowered the capabilities of militants and armed groups, and fueled the development of inter-communal conflicts. Despite increasing amounts of policy reports and field-based research that have been used to describe the magnitude and impact of such proliferation, current analyses are quite fragmented, and they are not well integrated ([Durkin 2019](#)). The patterns of violence and insecurity in the region are, in most cases, seen as issues that are secondly considered as a result of the dynamics of the arms flows, and not as an essential factor that influences the region.

This policy analysis gap restricts the usefulness of policy reactions. The flow of SALW in Northwestern Nigeria is supported by an interrelationship of interdependent causes, such as poverty alleviation, local fabrication, and transnational smuggling channels. Such dynamics are also facilitated by permeable borders and poor institutional capacity in security institutions that together encourage the continuation and growth of black markets in weapons ([Ahmadu 2019](#)). The activities directed towards the control of the proliferation of weapons and the re-establishment of state power are unlikely to be effective without a thorough understanding of these interconnected processes.

In addition, the geographical aspect of the SALW proliferation in major states like Zamfara, Katsina, and Sokoto reveals the necessity to increase the variability of the analysis into a more coordinated and context-specific mode. The study of the interactions and movement patterns within and across these areas is crucial to the development of critical and efficient interventions. In this regard, to understand the issue of SALW proliferation in Northwestern Nigeria, it is necessary to go beyond isolated narratives and access a more systematic and integrated view of the problem.

Revised Methodology

The given study assumes a systematic literature review (SLR) to summarize and critically evaluate the current academic and institutional resources on the proliferation of Small Arms and Light Weapons (SALW) and the resultant insecurity

in Northwestern Nigeria. The method is both a qualitative and an analytical one, which is intended to produce structured knowledge on what is known and what is not known in the literature. The sources used in the review are varied and cover peer-reviewed journal articles, reports by organizations and various bodies, as well as reports by reliable media outlets that were released between 2000 and 2024. The inclusion criteria had been explicitly determined, and the selection of materials was based on their relevance to SALW proliferation, insecurity patterns, and socio-political relationships of the region of Northwestern Nigeria.

The sources that failed to interact with these themes directly or were not deep enough in analysis were not included in the review. To achieve analytical coherence, the chosen literature was systematized and analysed using thematic analysis. The materials were classified into major thematic categories, such as sources and typologies of SALW, local and transnational distribution patterns, associations between SALW and organized violence, security politics in the region, and available policy and institutional responses. The process made it possible to define the points of intersection and contradiction in the literature and the number of analytical gaps.

Moreover, a critical appraisal of the chosen works was performed in order to assess the methodological rigor, contextual relevance, and policy/scholar debate contribution of the selected works. Special attention was also given to the extent to which the current literature is sufficient to reflect the complexity of SALW proliferation and its effects on the insecurity in the region. This organized presentation of the SALW-insecurity nexus in Northwestern Nigeria offers a consolidated and critical description of the topic that presents unexplored aspects of the topic and provides a more comprehensive basis for future research and policy intervention.

Small Arms, Light Weapons and Their Proliferation in Nigeria

There is a need to have conceptual clarity of what is meant by the proliferation of Small Arms and Light Weapons (SALW) before understanding their proliferation. In the international policy and law, the United Nations stipulates that small arms are weapons designed to be used by individuals, and they include pistols, rifles, carbines, light automatic weapons, light weapons that are meant to be used by a group, such as mortars less than 100 mm, rocket launchers, anti-aircraft, and anti-tank weapons. (Eselebor 2019). This difference forms a valuable point of reference when examining the patterns of use, distribution, and effects.

Outside this structure, there are a number of scholars and institutional definitions that have extended these notions. According to Meek and Stott (2004), small arms comprise carbines, semi-automatic weapons, assault rifles, and self-loading rifles, whereas light weapons are mortars, rocket launchers, anti-aircraft guns, and other mounted or high-impact systems. Equally, the Convention on the Control of Small Arms and Light Weapons in Central Africa (2011) defines small arms as handheld, lethal weapons

that shoot out projectiles by a mechanical process, and this reaffirms this point of easy handling and individual usage. The United Nations Institute of Disarmament Research (2006) expands this even further to emphasize their functional diversity; the automatic and semi-automatic firearms have different firing capacities.

Besides this, Saferworld (2012) broadens the conceptual discussion by including ammunition and other associated parts, including cartridges, propellants, and projectiles, as part of the small arms systems. This more global outlook matters, since it highlights the contribution of supply chains and logistics to the perpetuation of employment and spread of these weapons. Collectively, these views show some overlaps as well as divergence in the definition of SALW, especially in terms of scope and constituents.

SALW proliferation has become one of the major causes of insecurity in the Nigerian context. Miller (2022) suggests that these weapons are no longer linked with a state security force, but it has become a frequent tool of control, violence, and economic survival in the hands of non-state actors. They are mostly available, easily accessible, and destructive, and this has led to increasing violence, deaths, displacement, and livelihood destruction. Likewise, Alimba (2017) attributes the prevalence of SALW to the rising strength of armed groups that include OPC, MEND, MASSOB, well-armed groups of herdsmen, and Boko Haram, and assumes that the access to weapons has increased their power and presence as well as their capabilities of action.

These studies are supported by other researchers who confirm the relationship between SALW proliferation and criminal violence. Adamu, Mat, and Taya (2018) point to the importance of small arms in supporting the activities of gangs and criminal organisations, such as armed robbery, kidnapping, and sexual violence. Malam (2014) goes on to support this by arguing that the presence of illicit weapons promotes the application of violence instead of dialogue, deteriorates development, and perpetuates cycles of violence and corruption. Similarly, Ayuba and Okafor (2015) relate the dissemination of armed violence in various regions, such as the Niger Delta, the Northeast, and the Northwest, with the continuity of the illegal arms supply.

Despite these contributions, the current body of literature tends to be more specific on definitions and effects of SALW, and lacks in its integration of clarity of the concept and context dynamics. The absence of this gap highlights a stronger requirement for a more analytical methodology that does not just delimit SALW but also puts their proliferation in a wider context of security issues in Northwestern Nigeria.

The Global Spread of Small Arms and Light Weapons (SALW)

Small Arms and Light Weapons (SALW) have received sustained scholarly and policy interest because of the key place that it plays in the contemporary violence and insecurity patterns. The United Nations (2015) believes that the prevalence

of SALW, even the legally obtained ones, is still strongly linked with the ongoing armed conflicts in various regions. The estimates that have been made at the international deliberations have indicated that hundreds of millions of SALW are already in circulation across the globe, and the weapons have contributed a significant percentage of the casualties in both intra-state and inter-state conflicts. This highlights the magnitude of the issue and the need to institute global actions.

In addition to direct deaths, there are more socio-economic and political impacts of SALW proliferation. As the United Nations Security Council (2015) mentions, such weapons lead to loss of life and a weakening of economic systems, erosion of social cohesion, and institutional instability. They are relatively inexpensive, easy to carry, and especially appealing to state and non-state actors because of their portability and ease of use, thus making their proliferation in various conflict organizations quite easy. According to Ban Ki-moon, over the past decades, hundreds of conflicts have claimed the lives of many people and displaced them, most of which would not have been possible without the convenient accessibility of such weapons.

The transnational aspect of SALW proliferation also makes the problem more complicated. The weakness of state authority in conflict areas has led, in many cases, to the spread of weapons over the borders. As an example, Libya became unstable after the overthrow of Muammar Gaddafi, which led to the spread of weapons in Sub-Saharan Africa, including Mali, Niger, Nigeria, Chad, and Cameroon (United Nations 2015). These trends explain why regional insecurity can create broader security effects due to black market weapons transfers.

Meanwhile, the legal and illegal arms trade in the world market perpetuates the supply of SALW. Small arms and light weapons such as pistols, rifles, machine guns, rocket launchers, and grenades are available in the marketplace through intricate systems that include state actors, private actors, and non-state armed formations (Stockholm International Peace Research Institute 2019). This trade has greatly increased in recent years, with the world witnessing arms transfers at a higher level compared to the previous years, which were seen at the end of the Cold War. The large proportions of global arms distribution are represented by major exporting nations, such as the United States, Russia, China, France, and Germany, although a large portion of states and non-state actors remain among the main recipients.

Moreover, the lack of transparency in transactions of arms, especially illegal ones, makes it hard to effectively regulate and monitor them. As SIPRI (2019) states, not only governments but also a wide variety of non-state armed organizations and international players have been supplied with arms, but in many cases, via informal or even hidden channels. This sophistication adds weight to the continuation of SALW proliferation as a challenge to the national and regional security around the world. Even though the global literature is rich, most of the studies done so far tend to focus on aggregate trends without adequately connecting them to local settings

and processes. This brings out the necessity of more context-based studies, which can relate global trends of SALW flow to regional displays like those found in Northwestern Nigeria.

Nexus between Arms Proliferation, Terrorism, and National Security

The connection between national security, Small Arms and Light Weapons (SALW) proliferation, and terrorism is not a recent topic of analysis in both academic and policymakers' publications. The nexus is especially relevant since the distribution of SALW has a direct effect on the functional ability of terrorists and other non-state actors, directly affecting the overall safety consequences. The United Nations Office on Drugs and Crime (2006) suggests that the twenty-first century has seen the growing overlap between terrorist organisations and transnational criminal networks. Drug trafficking, arms smuggling, money laundering, and other rogue economic phenomena are some of the activities that maintain this convergence and lead to the growth and sustained insecurity.

In this regard, SALW also acts as a key facilitator of terrorism and organised violence. Their portability, affordability, and ease of use make them especially appealing to non-state actors, such as insurgents, bandits, and criminal gangs. According to GIABA (2013), the susceptibility of the socio-economic situation, particularly unemployment and poverty, provides opportunities to join the arms trafficking networks, as well as to engage in terrorist operations. This is the case in Nigeria, where economically marginalised people are usually lured into illicit arms dealings and violent networks at the expense of earning basic survival needs.

Researchers also state that there is a two-way correlation between the proliferation of arms and conflict. Bassey (2003), Edeko (2013), and GIABA (2013) note that the supply of SALW fuels conflict and criminal violence, but at the same time, the uncertainty that persists results in the demand to have more weapons, thus continuing a cycle of insecurity. This vicious circle makes it difficult to deal with arms proliferation or terrorism separately.

In a larger context, the outcomes of the SALW proliferation are not limited to the conventional concept of national security. In their arguments, Barash and Webel (2009) argue that the concept of national security cannot be understood in a purely military sense, but must have social, economic, and political facets. In this respect, the prevalence of SALW is an undermining factor to social cohesion, governance structures, and worsening inequalities, all of which decrease insecurity in the long-term. On the same note, Kelvin (2007) points out that SALW has enabled various violent acts in the form of terrorism, organised crime, civil violence, and human trafficking, thus creating an all-around danger to state and human security.

This nexus is further enhanced by the role of transnational networks and globalisation. The growing interconnectedness of the states has enabled the

cross-border flow of arms; thus, terrorist and criminal groups can acquire arms with relative ease. Research by La Sage (2010) and Ngboawaji (2011) reveals the profitability and sustainability of illegal smuggling networks in Africa, including some of the most important routes, such as the Lagos-Seme-Cotonou route. These networks usually overlap with activities of arms trafficking, which strengthens the supply of SALW in conflict-prone regions. As in Nigeria, Aluede (2017) and Shaw (2017) observe, cross-border trafficking and local production also contribute to the supply of weapons, making it difficult to control it.

Besides that, cross interventions of arms trafficking with other dark economies, especially drug trafficking, have been well recorded. Alphaeus et al. (2013) and Aluede (2017) underline that Nigeria is one of the regions and the whole world involved in drug trafficking because its borders are porous, and its location allows trafficking to thrive. These intersecting illegal markets produce mutually constitutive structures that perpetuate arms proliferation as well as organised violence.

Although the available literature is rather wide, most studies have a tendency to focus on arms proliferation, terrorism, and criminality as individual phenomena. Such fragmentation does not allow a complete picture of how these dynamics can play out in a given situation. The closer nature of the relationship between SALW proliferation, terrorism, and national security needs a more integrated approach to analysis, especially in areas like the Northwestern part of Nigeria.

Sources of the Proliferation of Small Arms and Light Weapons in Nigeria

The distribution of Small Arms and Light Weapons (SALW) in Nigeria has been described to have a number of, although not mutually exclusive, causes, both domestic and international. The available literature establishes some of the crucial avenues through which such weapons are procured, distributed, and maintained in the country. They are cross-border smuggling, arms theft and diversion, armed group activities, local fabrication, and inadvertent peace support operation leakages (Keith Krause 2007).

Cross-border smuggling is one of the most-documented sources. Nigeria has long and mostly unregulated borders with its neighbours, thus providing opportunities to smuggle arms. The borders shared by the country are over 4,000 kilometres in length, as reported by Oke (2002), and there are numerous illegal points of entry that are hard to guard. This difficulty is also described by the reports that several unmanned routes exist, especially in the Nigeria-Benin route (Nigerian Ports Authority Handbook 1995). The magnitude of this issue is indicated by the number of seizures and the assumptions on the number of illegal inflows of arms, with Nigerian Tribune (2018) estimating that great amounts of weaponry and ammunition have been introduced in the country in this manner. The porous boundaries have remained open and have contributed to the continuous supply of SALW into the conflict-prone areas.

Theft and diversion of arms are also a major source of proliferation. Uche and Iwuamadi (2018) associate the emergence of armed banditry, especially in Northwestern Nigeria, with cattle rustling-retaliatory violence cycles, which are associated with the procurement and use of illegal guns. On the same note, Sunday (2023) links tendencies of violent conflict with environmental forces like climate change, which facilitate migration and resource competition, thus raising the demand for weapons. These dynamics show how the need and flow of SALW are produced through local conflicts.

The spread of weapons is also strengthened by the role played by armed groups and militias. According to historical descriptions by Nwankwo and Udeh (2005), the rise of groupings like the Bakassi Boys was directly related to the rise in insecurity and self-defence, resulting in more citizens having access to guns. Similarly, the attainment and employment of arms has been linked to separatist groups such as the Movement of the Actualization of the Sovereign State of Biafra (MASSOB), which are fuelled by a sense of marginalisation and political discontent. The actions of the groups like Yan-daba and Yan-Banga, which were initially connected with the traditional and political organisation, have turned into the types of organised violence that depend on the availability of weapons in Northern Nigeria.

Another important aspect of SALW proliferation is local fabrication. According to Ahmed (2002), the fact that indigenous production of firearms by local blacksmiths was initially meant to serve the purpose of hunting has seen an increase in demand over time. These home-made weapons are sometimes cheap and readily available, and consequently appealing to the criminal gangs and militia. Their presence has led to other categories of violence, such as ethno-religious conflicts in the different regions of the country.

Moreover, they have also highlighted the unintended effects of peace support operations (PSOs) and military operations as a cause of arms leakage. According to Dokubo (2003), when Nigerian personnel were put on international peacekeeping missions, they were exposed to weapons that were occasionally smuggled or diverted into the local markets. Likewise, the reasons for internal deviation, such as a situation when the military forces provided weapons to non-state forces, also demonstrate the institutional weaknesses in the arms regulation systems (Voice of America 2016).

Although these findings have been noted, most of the literature available has a tendency to study these sources separately and fails to indicate the interrelations between them in a proper manner. However, as the reality goes, it is the interplay of the cross-border flows, domestic production, weak institutions, and conflict processes that perpetuate the SALW proliferation in Nigeria. The solution to the issue, therefore, must be holistic and synthesise these various sources, instead of considering them as independent variables.

The Origin of Fulani-Herder Banditry in Zamfara State

The origin of Fulani-herder banditry in Zamfara State is vital in explaining the security crisis in Northwestern Nigeria. Zamfara has been a well-known center of insecurity since the conduct of banditry has been expanding slowly to other states within the region ([Rufa'i 2021](#)). On historical background, banditry in Zamfara is not a recent phenomenon, as it can be traced as far back as the 19th century, when horse-mounted bandits used to raid villages to steal livestock and valuables. During this time, some of the traditional leaders in the Dan-Sadau area were reported to have participated in violent robberies and cattle rustling. The modern Fulbe-herder banditry, however, has a more recent rise due to the intensification of the fights between the herders and farmers on the farmland and destruction of crops as a result of cattle grazing ([Rufa'i 2021](#)).

Government gold mining and smuggling have also led to an increase in armed banditry. Mining sites are frequented by bandits who steal resources and take residents for ransom, which makes the life of local communities and development extremely strained ([OE Watch Africa Commentary 2019](#)). Environmental pressures, population increase, and scandalous government land distributions in places like the Kuyambana forest, Maru, and Zurmi local government districts have aggravated the long-standing conflicts over land and water resources, which, historically, were resolved by community leaders. The developments decreased grazing land for herders and compelled them to encroach on agricultural lands, increasing tensions ([Crises Group Africa Reports 2020](#)).

Another outcome of the rural insecurity was the rise of vigilante forces like Yan Sa Kai (volunteer guards), who were mostly made up of young men belonging to Hausa societies. The primary intention of these vigilantes was to safeguard the villages, but they often meted out severe extrajudicial punishment on alleged robbers, especially the Fulani herders. Among them were indiscriminate arrests, torture, killings, and burning of Fulani communities, which only fuelled interethnic conflicts and had reviving impacts ([Crises Group Africa Reports 2020](#)).

Fulbe communities retaliated by establishing paramilitary organizations, especially Yan-Bindiga (gun owners), to protect cattle and retaliate against vigilante attacks. In some cases, these groups are kidnapped to receive ransom, which they use to purchase weapons and make protective efforts. Their source of income is acquired through the use of criminal acts. With time, these protective organizations became more structured bandit networks, with some becoming the Herder Alliance that further instilled insecurity in the area ([Crises Group Africa Reports 2020](#); Hassan Dantawaye, cited in report).

It has been analyzed that after 2009, cattle rustling and armed banditry increased significantly, especially after the 2011 general elections, when political and

socio-economic tensions increased (Anka 2017). Although some researchers blame the crisis on years of conflicts over grazing land and farmland, others highlight the effect of socio-political marginalization or the opportunistic criminality, as some individuals adopt the role of the Fulani herder and engage in banditry (Omitola et al. 2021).

On the whole, the literature indicates that there is a close relationship between herder-farmer conflicts and the spread of armed banditry in Zamfara. However, there are still loopholes in the real mechanisms by which common herders might have become full-fledged bandits, or the degree to which people in the countryside have been politicized and taken advantage of by the youth or political faction, or the youthful or otherwise dubious criminals. This highlights the multifaceted nature of the phenomenon, which combines historical resentment, economic benefits, environmental factors, and the inefficiency of local authorities.

Review Gaps

Despite the fact that the available literature offers a general insight into the proliferation of small arms and light weapons (SALW) in Nigeria, it has a number of gaps, especially when it comes to the security crises in Northwestern Nigeria.

To start with, there are fewer regional dynamics in the SALW proliferation that are analyzed. Although national-level research points to the overall trends in arms proliferation, limited research on the dynamics of these trends at the hotspot level has been done in Zamfara State. The study of the origin of the Fulani-herder banditry in Zamfara indicates that the availability of SALW has intensified the old herder-farmer tensions, making it easy to organize banditry and ransom kidnappings. Nevertheless, the literature lacks a comprehensive investigation of the way in which the combination of environmental, demographic, and local governance failures is unique in influencing SALW proliferation and insecurity in this region. The targeted regional literature may shed some light on the geographical factors related to armed banditry and the way SALW increases insecurity in the rural areas.

Second, gender and community-level analyses are lacking in the literature. Women and children are most affected by SALW violence in Zamfara, as well as by other problems such as abduction, forced migration, and economic marginalization. Nevertheless, very minimal literature answers their unique susceptibility, coping mechanisms, or their possible involvement in peacebuilding and disarmament. These aspects need to be understood to develop inclusive interventions that can empower community resilience towards the destabilizing impacts of SALW.

Lastly, we noticed a lack of research on the new technologies and international connections affecting SALW proliferation in Northwestern Nigeria. Although cross-border trafficking is mentioned as having been affected by Niger, Chad, and Cameroon, and the participation of external actors, they do not explore the role

of new technology like 3D printing, illicit networks, and the provision of weapons used in peace support operations to support local banditry. This would be further investigated within these technological and international aspects to improve methods of controlling and regulating arms, particularly in areas such as Zamfara, where SALW have become one of the main instruments of formalized criminal and insurgency operations.

It is these gaps that would give a more detailed picture of the interaction between SALW proliferation and localized conflict dynamics, raise security issues like Fulani-herder banditry, and predetermine human and national security outcomes in Northwestern Nigeria.

Research Justification

The gap areas that have been described in the current literature reflect the sense of urgency in conducting specific research on the problem of the proliferation of small arms and light weapons (SALW) in Northwestern Nigeria, and Zamfara State, in particular. Although the existing literature offers broad information on the subject of SALW proliferation and the national security concerns thereof, it overlooks local peculiarities of insecurity identification and fueling by developing and maintaining insecurity at a local level. The Fulani-herder banditry history of Zamfara provides lessons on how SALW respond to environmental factors, socio-political marginalization, and ineffective local governance to enact a chain reaction of violence extending to other states. The close analysis of these localized dynamics is hence significant in explaining the way how insecurity related to arms in the region occurs.

Furthermore, the literature on the topic pays little attention to the gendered and social impacts of SALW proliferation. The women, children, and vulnerable members of the community are disproportionately at risk, with some of the risks being abduction, forced migration, and economic deprivation. Exploring their lives, coping mechanisms, and possible contributions to conflict reduction will give a more inclusive picture of the human costs of SALW proliferation and will inform interventions that are socially aware and efficient.

Lastly, there is the issue of changing technological and international aspects of SALW proliferation that have not been fully explored. The new challenges to arms control in Nigeria are cross-border trafficking, the redistribution of arms during peace support operations, and the development of new technologies like 3D printing. The interaction of these factors with local insecurity will enable more effective policy responses and specific interventions to limit the proliferation of SALW and bring the spread of organized banditry and armed conflict to a minimum.

Overall, the gap in knowledge about the localized drivers of SALW proliferation, the human impacts, and the global connections, in general, justifies this study. Through the use of Zamfara and the Northwestern part in general, the research aims at creating

empirical evidence that can inform policymakers and security organs to come up with specific, effective, and context-sensitive measures to fight the continued threat of small arms proliferation and its effects on the stability of the region.

Conclusion

The available literature on the subject of small arms and light weapons (SALW) proliferation in Nigeria depicts the widespread dangers of such weapons to national security, social cohesion, and economic stability. Whereas the former sources offer impressive information on the overall nature, origins, and effects of SALW, they neglect the important aspects of the problem of the region, gendered consequences, and new technological and international factors. The example of Zamfara State shows that localized conflicts, such as Fulani-herder banditry, are interrelated with the presence and abuse of SALW and generate the cycles of violence that cross the borders of states.

The following knowledge gaps would make it impossible to gain a comprehensive picture of the problem of SALW proliferation in Nigeria. The evidence base required to have a more practical intervention will be represented by research concerning the Northwestern area, the weaknesses of women and children, and the impact of new technologies and foreign actors. After all, a subtle knowledge of these factors will help policymakers, security agencies, and the community involved to come up with context-sensitive and specific measures to counter small arms proliferation, armed violence, and a lasting peace in Nigeria.

CONFLICT OF INTEREST

The author declares no potential conflict of interest.

ACKNOWLEDGMENT

This research received no specific grant from any funding agency.

References

- Adamu, W.R., B.B. Mat, and S.L. Taya.** 2018. "Human Security Under Threat: The Proliferation of Small Arms In Nigeria". *Journal of Humanities And Social Sciences* 23(5), ver.3: 17-21. <https://www.iosrjournals.org/iosr-jhss/papers/Vol.%2023%20Issue5/Version-3/C2305031721%20.pdf>.
- Ahmadu, H.** 2019. "Insight into the dynamics and menace of cattle rustling: A case study of Lake Chad Basin Area in Northern Nigeria". *World Journal of Social Sciences* 6(1): 18-33. <https://doi.org/10.22158/wjssr.v6n1p18>.
- Ahmed, A.M.** 2002. "Indigenous technology for sustainable development". *West Africa* 23(4): 373-378.

- Alimba, C.N.** 2017. "Controlling the Proliferation of Small Arms in Nigeria: Emerging Issues and Challenges". *Global Journal of Arts, Humanities and Social Science* 5 (10): 40-51. <https://ejournals.org/wp-content/uploads/Controlling-the-Proliferation-of-Small-Arms-in-Nigeria.pdf>.
- Alphaeus, K., G.A. Daouda, and M. Udoh.** 2013. *The impact of organized crime on governance in West Africa*. Abuja: Friedrich-Ebert-Stiftung.
- Aluede, J.** 2017. "Border relations in Africa and the impact on Nation-Building: A study of Nigeria and Her Limitrophe Neighbours since the 1960s". *African Journal of Governance and Development* 6(1): 10-26. <https://ajgd.journalofgovernance.com/index.php/ajgd/article/view/73>.
- Anka A.S.** 2017. "Emerging Issues in Zamfara Armed Banditry and Cattle Rustling: Collapse of the Peace Deal and Resurgence of Fresh Violence". *International Journal of Innovative Research and Development* 6 (12): 161-169. <https://docslib.org/doc/10236561/emerging-issues-in-zamfara-armed-banditry-and-cattle-rustling-collapse-of-the-peace-deal-and-resurgence-of-fresh-violence>.
- Ayuba, C. and G. Okafor.** 2015. "The Role of Small Arms and Light Weapons Proliferation in African Conflicts". *African Journal of Political Science and International Relations* vol 9(3):76-85. <https://doi.org/10.5897/AJPSIR2014.0750>.
- Barash, D. and C. Webel.** 2009. *Peace and Conflict Studies*. California: Sage Publications Inc. pp. 324-325.
- Bassey, C.O.** 2003. "The Nature and Character of Civil Wars in West Africa in the 1990s," in Amadu Sesay (ed.), *Civil Wars, Child Soldiers and Post-Conflict Peace Building in West Africa*. Ibadan: College Press and Publishers Limited.
- Crisis Group Africa Report, no 288.** 2020. "Violence in Nigeria's North West: Rolling Back the Mayhem". <https://www.crisisgroup.org/rpt/africa/nigeria/288-violence-nigerias-north-west-rolling-back-mayhem>.
- Dokubo, C.** 2003. *Small Arms as a Threat to National Security: A Nigerian Case Study*. Ilorin: University of Ilorin Press.
- Duperas.** 2020. "Zamfara Conflict-Analysis and Multisectoral Need Assessment". Pastoral Resolve, Search for Common Ground, and Terre des Hommes.
- Durkin, A.** 2019. "Global arms trade highest since end of Cold War". Hinrich Foundation. <https://www.globaltrademag.com/global-arms-trade-highest-since-end-of-cold-war/>.
- Edeko.** 2013. "Border communities, ungoverned spaces and Nigeria's national security". *International Journal of Community and Cooperative Studies* 10(1): 30-43.
- Eselebor W.A.** 2019. "Porous Borders and Human Trafficking in Nigeria". In Oshita O. Alumona I., Onuoha F. (Eds.) *Internal Security Management in Nigeria*. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-13-8215-4_14.
- GIABA Report.** 2013. "The Nexus between Small Arms and Light Weapons and Money Laundering and Terrorist Financing in West Africa". https://www.giaba-fr.net/pdf/613_519_GIABA%20SALW%20Nexus-final.pdf.
- Keith Krause.** 2007. "Small Arms and Light Weapons: Towards Global Public Policy". International Peace Academy. https://www.files.ethz.ch/isn/126967/small_arms_light_weapons_03_2007.pdf.

- Kelvin.** 2007. "ARMS Proliferation and The Challenges of Internal Security: the Nigerian Experience". *IJSSHR-International Journal of Social Science and Humanities Research* 4(09): 1–11.
- Le Sage, A.** 2010. *Africa's irregular security threats: Challenges for U.S. Engagement*. Institute for National Strategic Studies, National Defense University. NDU Press: U.S.A.
- Malam, B.** 2014. "Small Arms and Light Weapons Proliferation And Its Implication for West Africa Regional Security". *International Journal of Humanities and Social Science* 4(8).
- Meek, S., and N. Stott.** 2004. *A guide to the destruction of small arms and light weapons. The Approach of the South African National Defense Force*. Geneva: United Nations Institute for Disarmament Research (INIDIR).
- Miller, P.U.** 2022. *Proliferation of Small Arms and Light Weapons and the Worsening Insecurity in Nigeria, 2010-2021*. Master's Thesis. Unpublished.
- National Population Commission (NPC) [Nigeria] and ICF.** 2019. *Nigeria demographic and health survey 2018 key indicators report*. Abuja, Nigeria, and Rockville, Maryland, USA: NPC and ICF.
- Ngboawaji, D.** 2011. *Trans-national threats and national security concerns: A study of the Nigerian-Benin Republic border*. International Security Journal. MIT Press: U.S.A.
- Nigerian Ports Authority Handbook.** 1995. "Evaluation of Nigerian ports post-concession performance".
- Nigerian Tribune.** 2018. "1000 smuggling routes which form a network of roads around the borders. In 2017 alone were used to smuggle into Nigeria".
- Nwankwo O.O, and C.S. Udeh.** 2005. "Militias Vigilantes and Gangs: Implication and Challenges for Conflict Management". In Adedeji, A.G. and Zabai, I.S. (eds.) *The Military and Management of Internal Conflict in Nigeria*. Abuja: National War College.
- OE Africa Commentary.** 2019. "Gold Mining Connections to Killings in Zamfara State". *OE Africa*. Vol. 9, Issues 1–12.
- Oke, H.K.** 2002. "Small Proliferation in Nigeria: Implication for National Security". NNC Project.
- Okoli, A. and P. Ioryer.** 2014. "Terrorism and humanitarian crisis in Nigeria: Insights from Boko Haram Insurgency". *Global Journal of Humanities and Social Sciences* 14 (1): 39-50. https://globaljournals.org/GJHSS_Volume14/6-Terrorism-and-Humanitarian-Crisis-in-Nigeria.pdf.
- Omitola, Bolaji, Solomon Aderire, Olawale Olufemi Akinrinde, Olumide O. Omodunbi, and Mary Magdalene Sackflame.** 2021. "The Triangle of Terror: Boko Haram, Fulani Herdsmen, Bandits and Organised Insecurity in Nigeria." *Studia Securitatis* 15 (1): 21–33. <https://paper.researchbib.com/view/paper/327822>.
- Rufa'I, M.A.** 2021. *I AM A BANDIT: A Decade of Research in Zamfara State, Bandits' Den*. Designed & Printed by Graphic Concept Academy Diplomat Area, Sokoto – Nigeria.
- Saferworld.** 2012. *Small arms and light weapons. A Training Manual*. Saferworld Publication.
- Shaw, L.** 2017. "Organized crime in Africa: Africa's changing place in the global criminal economy". *The Labour Journal* 21(4): 67-90.

- Stockholm International Peace Research Institute.** 2019. *SIPRI yearbook 2019: Armaments, disarmament and international security*. Oxford University Press.
- Uche, J. C. and C.K. Iwuamadi.** 2018. "Nigeria: Rural banditry and community resilience in the Nimbo community". *Conflict Studies Quarterly* 24: 71-82. <https://doi.org/10.24193/csqs.24.5>.
- United Nations Institute for Disarmament Research.** 2006. *Developing a mechanism to prevent illicit brokering in small arms and light weapons: Scope and implications*. Geneva: United Nations. <https://digitallibrary.un.org/record/587344?v=pdf>.
- United Nations Office for Disarmament Affairs.** 2006. "Crush the Illicit Trade in Small Arms". United Nations Conference to Review Progress made in the Implementation of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in all its Aspects. New York, 26 June – 7 July.
- United Nations.** 2015. "Human cost of illicit flow of small arms, light weapons stressed in security council debate." <https://www.un.org/press/en/2015/sc11889.doc.htm>.
- Voice of America.** 2016. "The third voice of American politics. *American Behavioral Scientist* 61(2): 55-70. *Environment* (Vol. 9, Issues 1–12). U.S. Army TRADOC. <https://oe.t2com.army.mil/>.

Cognitive Warfare and Strategic Uncertainty: Planning under the Threshold in Open Societies

Luis VAZ, MSc*

LTC Cav Pedro FERREIRA, PhD**

*Portuguese Military Academy Research Centre

e-mail: lvazsantos@gmail.com

 <https://orcid.org/0009-0007-4702-2900>

**Portuguese Military Academy Research Centre

e-mail: ferreira.pna@exercito.pt

Abstract

This article examines the way in which open societies can design long-range strategy in the cognitive domain under conditions of strategic uncertainty and persistent sub-threshold competition. Using a conceptual-doctrinal research design grounded in strategic analysis, future-oriented synthesis, and selected operational illustrations from contemporary information competition, the article develops a framework for understanding Cognitive Warfare (CogWar) as a contest over tempo, attention, legitimacy, and decision quality. The analysis advances a double diagnosis. First, the openness paradox: unprecedented connectivity and information abundance coexist with fragmentation, polarisation, and degraded collective sensemaking. Second, the deterrence paradox: a strategic culture centred on the avoidance of escalation incentivises adversaries to employ indirect, deniable methods, operating below the threshold of armed conflict. Drawing on classical strategic theory, information operations literature, and contemporary examples including election interference, synthetic media, and crisis-driven narrative competition, the article argues that cognition has become both the strategic centre of gravity and a principal vulnerability in liberal democracies. The article contributes in three ways. First, it reframes CogWar less as narrative control and more as a struggle over decision tempo and institutional orientation. Second, it connects deterrence theory and the indirect approach to contemporary socio-technical battlefields shaped by algorithmic acceleration and ambiguity. Third, it proposes doctrinal design principles for cognitive defence compatible with democratic governance, emphasising legitimacy, anticipation, coalition interoperability, and institutional coherence. The article concludes that effective cognitive defence depends less on information dominance than on the ability of open societies to sustain lawful speed, strategic orientation, and public trust under conditions of persistent uncertainty.

Keywords:

Cognitive Warfare; Sub-Threshold Competition; Strategic Foresight;
Futures Studies; OODA Loop; Cognitive Security.

Article info

Received: 31 March 2026; Revised: 3 April 2026; Accepted: 21 May 2026; Available online: 30 June 2026

Citation: Vaz, L., and P. Ferreira. 2026. "Cognitive Warfare and Strategic Uncertainty: Planning under the Threshold in Open Societies." *Bulletin of "Carol I" National Defence University*, 15(2): 229-256. <https://doi.org/10.53477/2284-9378-26-26>



© „Carol I” National Defence University Publishing House

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC-SA)

Introduction

This article examines the way in which open societies can design long-range strategy in the Cognitive Warfare (CogWar) domain under conditions of strategic uncertainty, persistent sub-threshold competition, and accelerating technological change. The relevance of the problem rests on a double paradox. First, liberal-democratic societies have never been more connected or information-rich, yet public space is increasingly fragmented, polarised, and exposed to degraded collective sensemaking. Second, the openness that sustains innovation, pluralism, and civic participation also creates vulnerabilities exploitable by adversaries operating through ambiguity, deniability, and information asymmetry. In this environment, cognition – understood as the capacity of societies and institutions to orient, decide, and sustain legitimacy under pressure – emerges simultaneously as a strategic centre of gravity and a principal vulnerability.

The strategic significance of this shift has become increasingly visible across recent crises and geopolitical disputes. Russian interference campaigns in electoral processes, the information contestation surrounding the COVID-19 pandemic, and the rapid circulation of synthetic media during ongoing conflicts such as the war in Ukraine illustrate how contemporary competition increasingly targets perception, orientation, and decision tempo rather than territorial control alone. These operations frequently unfold below the threshold of armed conflict, exploiting legal ambiguity, institutional seams, and the slower deliberative rhythms of open societies.

At the same time, technological acceleration is compressing the interval between signal generation, narrative amplification, and strategic effect. AI-assisted content production, automated distribution systems, algorithmic engagement mechanisms, and synthetic media have significantly reduced the cost and time required to shape public attention and distort institutional orientation ([Chesney and Citron 2019](#); [Singer and Brooking 2018](#)). In practical terms, this means that the decisive variable is often no longer the factual superiority of information itself, but the speed with which coherent interpretations can be formed, legitimised, and operationalised.

Read through a Clausewitzian lens, the character of conflict adapts to socio-technical transformation while remaining subordinate to political purpose ([Clausewitz 1976](#)). Contemporary cognitive competition, therefore, does not reflect the disappearance of strategic logic, but its migration into increasingly dilated battlefields extending across institutions, media ecosystems, digital platforms, and everyday social practices. Under these conditions, the strategic problem is no longer reducible to “countering disinformation” as an isolated activity, but concerns the broader capacity of open societies to sustain orientation, legitimacy, and decision quality under persistent information pressure.

Research Design and Methodological Approach

This article adopts a conceptual-doctrinal and exploratory research design grounded in strategic analysis, future-oriented synthesis, and interdisciplinary literature integration. Rather than pursuing empirical causal testing or operational modelling, the study seeks to clarify how defence institutions in open societies can think about long-range cognitive strategy under conditions of uncertainty and sub-threshold competition.

Methodologically, the article combines four analytical pillars. First, it draws on classical strategic theory, particularly the Clausewitzian concepts of war, deterrence theory, and the indirect approach ([Clausewitz 1976](#); [Hart 1967](#); [Schelling 1966](#); [Beaufre 1965](#)). Second, it incorporates contemporary literature on information operations, media ecosystems, algorithmic amplification, and disinformation dynamics ([Benkler, Faris, and Roberts 2018](#); [Rid 2020](#); [Singer and Brooking 2018](#)). Third, it integrates conceptual perspectives associated with strategic foresight and Futures Studies, particularly regarding uncertainty, horizon scanning, and anticipatory governance ([Schoemaker 1995](#); [Cascio 2020](#)). Finally, the article engages selected operational illustrations from contemporary crises and geopolitical disputes – including electoral interference, pandemic-related narrative competition, and synthetic media proliferation – not as formal case studies, but as analytical examples intended to ground the conceptual discussion in observable strategic dynamics.

The article employs a limited and practice-oriented Futures Studies perspective. The purpose is not predictive forecasting, but the development of anticipatory orientation mechanisms capable of reducing strategic surprise and preserving institutional adaptability under volatile conditions. Accordingly, the proposed approach emphasises horizon scanning, alternative scenarios, signposts, and iterative reassessment integrated into institutional decision cycles.

Several limitations should be acknowledged. Given its conceptual and doctrinal nature, the article does not propose an operational playbook for tactical execution units, nor does it rely on classified material, quantitative modelling, or field-based empirical research. Its primary focus remains at the level of governance, strategic culture, and institutional design within NATO and EU-oriented open societies. The article, therefore, prioritises analytical coherence and doctrinal applicability over predictive precision or operational prescription.

Conceptual Boundaries and Contribution

For the purposes of this article, Cognitive Warfare refers to activities intended to influence, degrade, or disrupt perception, orientation, and decision-making processes across civil-military environments. The concept is treated not merely as strategic communication or disinformation, but as a broader contest over tempo, attention, legitimacy, and institutional coherence. Open societies are understood as liberal-democratic systems characterised by plural media ecosystems, legal constraints on state authority, institutional transparency, and politically contested public spaces.

The article contributes in four ways. First, it reframes CogWar less as a struggle for narrative dominance and more as a contest over decision tempo and strategic orientation. Second, it links the contemporary return of the indirect approach to the deterrence logic and escalation constraints that structure sub-threshold competition in open societies. Third, it integrates Futures Studies and strategic foresight into the cognitive domain through a lightweight anticipatory framework compatible with democratic governance. Finally, it proposes doctrinal design principles centred on legitimacy, lawful speed, coalition interoperability, and institutional coherence as foundations for long-range cognitive defence.

Structure of the Article

The article proceeds in four sections. The first section, “Double Paradoxes: Establishing the Problem in Open Societies,” develops the openness paradox and the deterrence paradox as the structural conditions shaping contemporary cognitive competition. The second section, “Deterrence Fixation and the Return of the Indirect Approach in Dilating Battlefields,” examines how ambiguity, deniability, and tempo function within sub-threshold strategic competition. The third section analyses the techno-operational environment of CogWar, focusing on speed, scale, scope, attribution challenges, and planning horizons. The fourth section, “From Method to Doctrine,” develops doctrinal principles for cognitive defence in open societies, emphasising legitimacy, anticipation, institutional coordination, and coalition alignment.

Rather than offering technological solutions or operational recipes, the article argues that effective cognitive defence ultimately depends on the ability of open societies to sustain strategic orientation, lawful speed, and public legitimacy under conditions of persistent uncertainty and accelerated information competition.

Double Paradoxes: Establishing the Problem in Open Societies

This section develops the article’s central analytical diagnosis: contemporary CogWar emerges from the interaction between two structural paradoxes shaping open societies in accelerated information environments. The first is the openness paradox: the same conditions that enable democratic pluralism, innovation, and large-scale participation also generate fragmentation, information volatility, and vulnerabilities exploitable through manipulation and ambiguity. The second is the deterrence paradox: the long strategic emphasis on escalation avoidance and deterrence stability has incentivised adversaries to pursue indirect, deniable, and sub-threshold forms of competition designed to erode orientation and decision quality without triggering conventional military response.

Taken together, these paradoxes relocate the strategic centre of gravity from primarily physical assets toward societal cognition and institutional decision-making. The decisive contest increasingly concerns not only military capabilities or territorial control, but the ability of open societies to sustain coherent orientation, legitimacy, and operational tempo under persistent information pressure.

The Openness Paradox: Abundance with Fragmentation

Over recent decades, networked digital infrastructures have dramatically expanded access to information and participation in public discourse. Generally speaking, such openness should strengthen democratic accountability, diversify knowledge production, and improve collective learning. Yet, the same technological transformations have also altered the conditions under which public reasoning occurs. Information itself is no longer scarce; attention has become the limiting strategic resource ([Simon 1971](#)).

Contemporary digital platforms operate according to engagement-driven logics that prioritise salience, emotional activation, and continuous interaction rather than epistemic quality or coherence. Algorithmic systems amplify content capable of generating rapid behavioural responses, frequently rewarding novelty, outrage, identity affirmation, and emotional polarisation ([Sunstein 2009](#); [Pariser 2011](#)). Over time, these dynamics contribute to fragmented information ecosystems in which different social groups increasingly operate within partially disconnected interpretive environments.

The strategic significance of this fragmentation lies not merely in the circulation of false information but in the degradation of shared orientation mechanisms. Public discourse becomes more volatile and temporally compressed, while institutional processes – investigation, verification, deliberation, and consensus-building – retain comparatively slower rhythms. In operational terms, this creates widening asymmetries between the speed of narrative circulation and the speed of institutional sensemaking.

The COVID-19 pandemic illustrated this dynamic with unusual clarity. During the global health crisis, institutional communication competed simultaneously against conspiracy narratives, peer-to-peer amplification, emotionally charged content, and conflicting expert interpretations circulating across digital platforms. The World Health Organisation itself characterised the phenomenon as an “infodemic,” recognising that the challenge extended beyond misinformation narrowly understood and involved the broader erosion of orientation under conditions of information abundance and accelerated uncertainty ([World Health Organization 2020](#)).

Competing narratives regarding vaccines, public health restrictions, and institutional credibility frequently spread faster than formal verification processes, contributing to distrust, polarisation, and difficulties in coordinated policy implementation.

Research on “network propaganda” further suggests that contemporary manipulation often succeeds less through direct persuasion than through salience disruption and interpretive overload ([Benkler, Faris, and Roberts 2018](#)). In many cases, the objective is not to convince the public of a coherent alternative reality, but to fragment attention, increase uncertainty, and degrade confidence in institutional arbiters. Under such conditions, the strategic contest increasingly concerns who frames first, who sustains interpretive tempo, and whose orientation mechanisms remain operational under stress.

Technological acceleration amplifies these vulnerabilities. AI-assisted content generation, synthetic media, automated amplification systems, and low-cost distribution infrastructures significantly reduce barriers to influence operations (Chesney and Citron 2019). Content that once required substantial organisational resources to produce and disseminate can now be generated rapidly and circulated globally at a marginal cost close to zero. The proliferation of deepfake technologies and AI-generated political material during electoral cycles and geopolitical crises further compresses verification windows, increasing pressure on institutions already operating under time constraints.

Yet openness remains simultaneously a vulnerability and a strategic strength. Open societies possess capacities for redundancy, distributed scrutiny, peer correction, and adaptive learning unavailable to more centralised systems. Independent media, plural institutions, civil society networks, and coalition-based verification mechanisms can increase resilience – provided that institutional legitimacy and decisional tempo are preserved. The openness paradox, therefore, does not imply that democratic systems are inherently weaker, but rather that their resilience depends increasingly on the quality and speed of collective orientation under accelerated information conditions.

The Deterrence Paradox: Escalation Avoidance and Sub-threshold Strategy

The second paradox emerges from the strategic logic of deterrence and escalation management that has shaped Western security thinking since 1945. Nuclear deterrence and escalation avoidance contributed significantly to preventing direct great-power confrontation. However, this strategic success also displaced competition into domains operating below the threshold of conventional armed conflict, where ambiguity, deniability, and incremental pressure could be employed at lower political and strategic cost (Freedman 2013; Mazarr 2015).

Contemporary adversaries increasingly exploit this environment through indirect approaches combining information, cyber, diplomatic, economic, and psychological instruments calibrated to remain beneath formal escalation thresholds. In these contexts, ambiguity itself becomes operationally valuable. Attribution uncertainty slows institutional response, complicates coalition coordination, and raises the political costs associated with retaliation or escalation.

Russian interference campaigns in Western electoral processes exemplify this logic, particularly in the 2016 U.S. elections, where official investigations documented a coordinated active-measures campaign combining cyber activity, social media manipulation, and political interference (U.S. Senate Select Committee on Intelligence 2020). Rather than relying on direct coercion, such operations frequently combined plausible deniability, proxy actors, coordinated amplification networks, selective leaks, and information disruption strategies designed to increase political friction and institutional hesitation. Similarly, information operations preceding and accompanying the war in Ukraine demonstrated how narrative pre-positioning, synthetic media

circulation, and digitally accelerated influence ecosystems could shape international interpretation windows before conventional military events fully unfolded.

Thomas Schelling's concept of coercion as the manipulation of expectations through uncertainty and risk remains particularly relevant in this context ([Schelling 1966](#)). Under sub-threshold conditions, adversaries frequently seek not decisive persuasion, but hesitation, distraction, delay, and cumulative erosion of orientation. The operational objective is often to stretch institutional decision cycles, exploit legal and bureaucratic seams, and impose disproportionate cognitive and political costs on defenders.

The deterrence paradox, therefore, resides in the unintended strategic consequences of escalation avoidance itself. The more costly and dangerous overt confrontation becomes, the greater the incentives for indirect competition exploiting ambiguity and deniability. Conventional deterrence models – structured around visible force, attribution clarity, and proportional response – map imperfectly onto environments where effects are cumulative, diffuse, and politically internalised over time.

Reinterpreted through a Clausewitzian perspective, this does not represent a departure from strategic logic, but an adaptation of the conflict's character to socio-technical conditions ([Clausewitz 1976](#); [Gray 2010](#)). Political objectives remain central, yet the relevant battlespace increasingly extends across media ecosystems, institutional processes, digital platforms, and social trust structures. Under such conditions, time itself becomes a strategic variable: whoever imposes orientation delays and interpretive instability gains operational advantage without necessarily crossing conventional thresholds of war.

Centre of Gravity in Open Societies: Cohesion and Decision Quality

Taken together, the openness and deterrence paradoxes reposition societal cognition as a central strategic variable in liberal democracies. The critical capability increasingly concerns whether institutions and publics can sustain coherent orientation, legitimate decision-making, and adaptive coordination under conditions of uncertainty, information saturation, and persistent cognitive pressure.

In this context, the centre of gravity of open societies lies less in information control than in the preservation of decision quality and societal cohesion. Three interrelated vulnerabilities become particularly significant.

First, decision latency emerges as a strategic risk. If investigative, legal, and communicative processes cannot operate at sufficient speed relative to narrative circulation, opportunities for pre-emptive framing and coordinated response are lost. Delayed orientation allows ambiguity and emotionally charged interpretations to stabilise before institutional clarification becomes effective.

Second, cohesion gaps create exploitable fractures across social, regional, political, or information lines. Cognitive operations frequently target bridging institutions and trust relationships – electoral/political and judicial systems, public health authorities,

armed forces, scientific expertise, or media credibility – precisely because disruption at these points can generate disproportionate societal effects.

Third, legitimacy erosion undermines the long-term capacity of institutions to sustain compliance and collective action. In open societies, legitimacy functions not merely as a normative value, but as an operational capability. Responses perceived as disproportionate, opaque, or procedurally inconsistent may achieve temporary tactical effects while degrading long-term trust and institutional resilience.

TABLE 1. The three linked vulnerabilities

Vulnerabilities	Definition
Decision Latency	If investigative, legal, and communicative processes cannot keep pace with the speed of narrative formation and diffusion, opportunities for pre-emptive framing and coordinated response are lost. Latency can reflect process design (e.g., clearance bottlenecks), resource limits, or inter-agency coordination gaps
Cohesion Gaps	Where publics segment along social, regional, or informational lines, adversaries can target bridging points (e.g., electoral administration, public-health compliance, military credibility) to produce outsized disruption. Cohesion does not imply unanimity; it implies sufficient cross-group trust to sustain contested decisions
Legitimacy Erosion	Even when decisions are substantively sound, deficits in transparency and proportionality can degrade acceptance, making subsequent decisions harder. In open societies, legitimacy is a capability to be designed and maintained—not a by-product to be assumed

Source: Author's own elaboration.

Importantly, these vulnerabilities are cumulative rather than isolated. Delayed decisions can intensify fragmentation; fragmentation can weaken legitimacy; weakened legitimacy further slows coordinated response. Cognitive competition, therefore, exploits systemic interactions across institutional, technological, and societal layers simultaneously.

Time, Ambiguity, and the Shifting Cost Curve

A defining feature of contemporary CogWar is the increasing strategic utility of time and ambiguity. Technological acceleration alters operational cost curves in at least three ways.

First, speed. AI-assisted content production, automated scheduling systems, and algorithmic amplification dramatically reduce the interval between conception, dissemination, and strategic effect. Early framing advantages accumulate rapidly because initial interpretations frequently anchor subsequent public understanding.

Second, scale. Digital infrastructures enable near-zero marginal distribution costs and highly targeted dissemination strategies. Coordinated influence campaigns can therefore achieve disproportionate visibility relative to their resource base, particularly when amplified through emotionally engaging content and algorithmically optimised interaction loops.

Third, scope. Contemporary operations move fluidly across domains and

jurisdictions, linking online discourse, diaspora networks, economic concerns, security debates, and physical-world behaviour. Information effects increasingly ricochet between digital and physical environments, generating complex feedback loops difficult to isolate or contain.

These transformations lower barriers to entry while increasing the operational advantages associated with ambiguity and rapid iteration. Adversaries can probe institutional reactions, test narratives, and adjust tactics at relatively low cost. Defenders, by contrast, remain constrained by legal standards, attribution requirements, coalition coordination processes, and democratic accountability mechanisms.

The result is a shifting asymmetry in which attackers benefit from low-cost experimentation while defenders bear the heavier burden of verification, proportionality, and legitimacy preservation.

Why Paradoxes Matter for Strategy

The strategic relevance of the double paradox lies in the risk of analytical misdiagnosis.

One risk is over-kinetic framing: interpreting CogWar primarily through models derived from conventional force-on-force conflict. Such approaches may underestimate how small, deniable, and cumulative information actions can generate strategic effects by degrading orientation and slowing decision-making rather than by physically destroying capabilities.

The opposite risk is over-managerial framing: reducing cognitive competition to communication management, reputational defence, or isolated “counter-disinformation” initiatives. These risks obscure the strategic intent underlying sub-threshold operations, which frequently aim to shape alliance behaviour, impose political costs, and weaken institutional confidence over extended periods.

TABLE 2. Strategic Implications of the Double Paradox

Paradox-Driven Risk	Strategic Implications
Over-kinetic framing	If planners default to models suited to physical force-on-force contests, they may overlook how small, deniable interventions generate strategic effect by degrading decision quality rather than by seizing territory. Measures of success tend therefore to require decision latency, recovery time, and indicators of cross-group bridging, not merely message volumes or takedown counts
Over-managerial framing	If, conversely, planners treat CogWar as a purely communicative or reputational problem, they may obscure adversary doctrine and intent. Sub-threshold campaigns are strategic, not accidental: they are designed to impose costs, signal resolve, test alliances, and sow doubts about state capacity
Normative slippage	Attempts to “harden” the information environment may drift toward illiberal practices that undercut legitimacy. In open societies, means and ends are inseparable: proportionality, transparency, and due process must be built into planning from the start. The credibility gained by adhering to such guardrails is itself a deterrent, as it narrows the political space in which adversaries can claim overreach

Source: Author’s own elaboration.

A third risk concerns normative slippage. Attempts to “harden” information environments through excessive control, surveillance, or exceptional measures may erode precisely the legitimacy and openness that constitute democratic strategic strengths. In open societies, means and ends cannot be separated cleanly: procedural legitimacy, transparency, and proportionality are not secondary ethical concerns, but operational conditions of long-term resilience.

From Problem to Programme

The double paradox, therefore, establishes the article’s central strategic problem: how can open societies preserve decision quality, legitimacy, and operational tempo under conditions of persistent cognitive competition without undermining the democratic principles they seek to defend?

Two implications follow.

First, classical strategic concepts remain highly relevant when reinterpreted for contemporary socio-technical battlefields ([Hart 1967](#); [Beaufre 1965](#); [Schelling 1966](#); [Clausewitz 1976](#); [Rid 2020](#); [Gray 2010](#)). Deterrence, coercion, ambiguity, and the indirect approach continue to shape strategic competition, although their operational grammar increasingly unfolds through information, cognitive, legal, and institutional mechanisms rather than purely military confrontation.

Second, the techno-operational environment structurally favours actors capable of integrating anticipation, orientation, and action into repeatable institutional routines. Effective cognitive defence, therefore, depends less on episodic reaction than on anticipatory governance capacities capable of reducing strategic surprise while preserving legitimacy and coalition coherence.

The following sections develop these implications further by examining the return of the indirect approach in sub-threshold competition, the operational conditions imposed by accelerated technological environments, and the doctrinal principles required for long-range cognitive defence in open societies.

Deterrence Fixation and the Return of the Indirect Approach in Dilating Battlefields

The previous section established how openness and deterrence generate structural vulnerabilities exploitable through cognitive competition. This section examines why contemporary strategic rivalry increasingly unfolds below the threshold of armed conflict and why the indirect approach has regained relevance under conditions of information acceleration, attribution ambiguity, and socio-technical complexity.

The central argument is that the long post-1945 emphasis on deterrence stability and escalation avoidance has unintentionally incentivised indirect and deniable forms of competition operating across what may be described as dilating battlefields – operational environments extending beyond conventional military theatres into institutions, digital infrastructures, legal systems, media ecosystems, and everyday social practices. In such environments, strategic effect derives less from territorial

seizure or direct destruction than from the ability to impose delay, uncertainty, fragmentation, and decision friction on adversaries over time.

Deterrence fixation and competition under the threshold

Since the end of the Second World War, Western strategic culture has been profoundly shaped by the imperative of preventing large-scale interstate war. Nuclear deterrence, escalation management, and alliance stability became central organising principles of Euro-Atlantic security architecture. While this strategic orientation contributed significantly to reducing direct great-power confrontation, it also encouraged competitive behaviour to migrate into domains operating below the threshold of conventional war (Freedman 2013; Mazarr 2015).

Contemporary sub-threshold competition exploits precisely those areas where attribution is uncertain, legal thresholds remain contested, and proportional responses are politically difficult to calibrate. Rather than seeking decisive military confrontation, adversaries frequently pursue cumulative strategic gains through information pressure, cyber operations, economic leverage, political disruption, proxy actors, and cognitive manipulation calibrated to remain ambiguous enough to avoid overt escalation.

The annexation of Crimea in 2014 represented a particularly illustrative example of this transition. Russian operations combined military positioning, information operations, political ambiguity, proxy structures, and strategic narrative shaping in ways that complicated attribution, delayed international consensus, and fragmented response coordination. Similar dynamics later emerged in electoral interference campaigns targeting Western democracies, where influence operations relied less on overt persuasion than on amplifying distrust, polarisation, and institutional friction. Such operations reveal an important asymmetry. For defenders operating within democratic and legal constraints, attribution is not merely technical but political. Responses frequently require evidentiary thresholds, coalition coordination, legal justification, and public legitimacy. Adversaries exploiting deniability can therefore impose disproportionate decisional and institutional costs at relatively low operational risk.

Thomas Schelling's analysis of coercion remains particularly relevant in this context (Schelling 1966). Strategic influence increasingly operates through the manipulation of expectations, uncertainty, and escalation perceptions rather than through confrontation alone. The objective is often not immediate persuasion, but hesitation: increasing the political and cognitive costs associated with response while stretching institutional decision cycles.

This dynamic helps explain why contemporary strategic competition increasingly favours persistent, incremental, and ambiguous pressure rather than overt escalation. The strategic success of deterrence at higher levels of conflict has unintentionally expanded the operational attractiveness of the grey zone.

The indirect approach, updated

The contemporary return of the indirect approach reflects this strategic environment. Classical theorists such as B. H. Liddell Hart and André Beaufre argued that

effective strategy often operates most successfully by shaping the adversary's perceptions, orientation, and strategic choices indirectly rather than through frontal confrontation ([Hart 1967](#); [Beaufre 1965](#)). Under current conditions, this logic has acquired renewed relevance through digitally mediated and cognitively accelerated forms of competition.

The indirect approach in contemporary CogWar environments seeks not necessarily to impose coherent ideological alternatives, but to increase uncertainty, degrade coordination, and impose cognitive friction across institutional systems. Operationally, this may involve:

- exploiting information asymmetries;
- amplifying social fragmentation;
- targeting alliance cohesion;
- manipulating tempo and attention;
- saturating public discourse with contradictory signals;
- or exploiting legal and bureaucratic seams between institutions.

Importantly, many of these operations function through cumulative rather than spectacular effects. Small-scale information interventions, selective leaks, coordinated amplification campaigns, nuisance cyber incidents, and synthetic media circulation may individually appear insufficient to justify a major response. Yet over time, their aggregated impact can degrade trust, increase decision latency, and weaken institutional coherence.

The war in Ukraine further demonstrated how indirect approaches increasingly combine military and information dimensions into integrated strategic ecosystems, with EU analyses identifying Ukraine as a primary target of Russian foreign information manipulation and interference ([European External Action Service 2023](#)). Prior to and during kinetic operations, competing narratives circulated across social media platforms, encrypted communication channels, state-affiliated media systems, and international digital networks. Deepfake videos, manipulated imagery, selective framing, and coordinated amplification efforts illustrated how information operations can shape interpretation windows before facts are fully verified.

This evolution reflects an important doctrinal shift: the indirect approach is no longer confined to military manoeuvre or diplomatic signalling alone. It increasingly unfolds through socio-technical architectures capable of influencing orientation, tempo, and legitimacy simultaneously.

Dilating battlefields: a Clausewitzian reading

A Clausewitzian perspective helps clarify the continuity underlying these transformations. Clausewitz argued that while the nature of war remains enduringly tied to political purpose, friction, and uncertainty, its character evolves according to historical and technological conditions ([Clausewitz 1976](#)). Contemporary cognitive competition, therefore does not invalidate classical strategic theory; rather, it demonstrates how strategic interaction adapts to socio-technical change.

Under current conditions, the battlespace becomes increasingly dilated. Strategic interaction extends beyond physical theatres into media infrastructures, digital platforms, institutional procedures, public discourse, economic systems, and social trust networks. These environments are not secondary information “backgrounds” to conflict but operational terrains in their own right.

The decisive effects sought within these dilated battlefields are frequently cognitive and institutional rather than kinetic. Strategic success may manifest as:

- delayed political decisions;
- alliance hesitation;
- fragmented public interpretation;
- reduced institutional legitimacy;
- or increased societal fatigue and uncertainty.

The relevant variables therefore increasingly concern tempo, orientation, and coherence. In practical terms, a state may retain overwhelming conventional military superiority while nevertheless experiencing strategic paralysis if institutional decision-making becomes sufficiently slowed, fragmented, or delegitimised under persistent information pressure.

This perspective also dissolves simplistic distinctions between “peace” and “war.” Cognitive competition frequently unfolds continuously across peacetime, crisis, and conflict phases, with information and psychological shaping operations persisting before, during, and after kinetic escalation. Contemporary strategy must therefore operate across an extended temporal horizon in which orientation and anticipation become continuous rather than episodic activities.

The grammar of sub-threshold coercion

Although contemporary sub-threshold operations vary significantly across actors and theatres, they frequently share a common operational grammar organised around ambiguity, deniability, tempo, and asymmetry.

First, ambiguity is deliberately engineered into operational design. Attribution complexity increases political hesitation and complicates coalition coordination. Cyber incidents, proxy actors, front organisations, commercial intermediaries, and transnational digital networks all contribute to creating uncertainty regarding authorship and intent.

Second, deniability functions as a protective buffer against escalation. By maintaining a plausible distance between sponsor and effect, adversaries reduce the likelihood of proportional retaliation while preserving operational flexibility.

Third, tempo advantage constitutes a central strategic objective. Automated amplification systems, coordinated posting networks, synthetic media generation, and pre-positioned digital ecosystems enable rapid narrative circulation before institutional verification processes can stabilise interpretation. Early framing advantages become particularly powerful under accelerated information conditions because initial narratives frequently shape subsequent public understanding even after corrections emerge.

TABLE 3. The grammar of sub-threshold coercion

Expressions	Definitions
Ambiguity by design	Actions are calibrated to keep motivation and sponsorship contestable. This exploits the evidentiary standards of open societies and buys time
Deniability through indirection	Proxies, front organisations, and cross-border channels create distance between initiator and effect. Attribution becomes a political decision as much as a technical one
Tempo advantage	Content automation, coordinated posting, and pre-positioned channels allow rapid onset. If detection and orientation lag, early frames anchor public interpretation
Seam exploitation	Campaigns look for institutional seams (between ministries, regulators, and courts) and informational seams (between platforms, languages, or jurisdictions). These seams are friction points that can be multiplied at low cost
Cost-imposition asymmetry	Small acts (e.g., a targeted leak, a crafted rumour, a nuisance cyber-incident) impose disproportionate costs on defenders, who must investigate, brief, coordinate, and respond within legal and ethical constraints
Typical effects	Delay, distraction, doubt. Success is often negative: what does not happen (delayed decisions, shelved policies, aborted reforms). Persuasion is not required; uncertainty can be enough

Source: Author's own elaboration.

Fourth, sub-threshold competition systematically exploits institutional seams. Legal jurisdictions, inter-agency coordination gaps, alliance consultation procedures, and differences between public and private governance systems create friction points that can be targeted at relatively low cost. The strategic objective is often less to “win” a narrative outright than to increase institutional complexity, coordination burdens, and decisional fatigue.

Finally, these operations are characterised by cost asymmetry. Relatively small actions can impose disproportionate burdens on defenders required to investigate, coordinate, attribute, communicate, and respond within democratic and legal constraints. This asymmetry favours persistence, experimentation, and iterative adaptation by attackers.

Importantly, the cumulative effects of such operations are frequently negative rather than affirmative. Success may consist not in changing beliefs directly, but in generating sufficient uncertainty, delay, or fragmentation to prevent coherent collective orientation and timely institutional response.

Implications for open societies

For open societies, the return of the indirect approach creates several strategic dilemmas. The first is the temptation to interpret cognitive competition primarily as a communication problem. Such framing risks reducing strategy to messaging or “counter-disinformation” campaigns while neglecting the broader institutional and temporal dimensions of sub-threshold competition. Cognitive operations target not only narratives, but also decision processes, coordination mechanisms, and legitimacy structures.

The second is the opposite temptation: responding through excessive securitisation or illiberal hardening measures that undermine democratic legitimacy and public trust. Attempts to defend openness through opaque control mechanisms, exceptional restrictions, or disproportionate surveillance may ultimately damage the very societal resilience they seek to protect.

A more sustainable approach requires adapting deterrence logic to the cognitive domain without abandoning democratic constraints. This implies acting simultaneously on three interconnected dimensions.

First, reducing attacker payoff windows by shortening institutional detection-to-decision cycles and improving lawful decisional tempo. Second, strengthening societal resilience through credible intermediaries, coalition coordination, and cross-group trust structures capable of reducing fragmentation and interpretive instability. Third, increasing reputational, diplomatic, legal, and political costs associated with covert influence operations, particularly through coalition-based attribution and coordinated transparency measures.

In this context, legitimacy itself becomes a strategic capability. Responses perceived as proportionate, transparent, and procedurally coherent strengthen institutional credibility and reduce opportunities for adversarial exploitation.

Bridge to Sections 3 and 4

If the previous section established cognition as a strategic centre of gravity in open societies, this section has shown why contemporary competition increasingly operates through indirect, deniable, and sub-threshold mechanisms exploiting tempo, ambiguity, and institutional friction across dilating battlefields.

The next section, therefore, examines the techno-operational environment enabling these dynamics. Specifically, it analyses how acceleration, automation, platform architectures, attribution complexity, and transnational information ecosystems reshape operational possibilities and planning horizons in contemporary CogWar environments.

Section 4 subsequently translates these insights into doctrinal design principles for cognitive defence in open societies, focusing on legitimacy, anticipation, institutional coordination, and coalition interoperability as foundations for long-range strategic adaptation.

Techno-Operational Environment of CogWar

Contemporary CogWar unfolds within a techno-operational environment characterised by accelerated information circulation, low barriers to entry, transnational connectivity, and increasingly blurred distinctions between civilian and strategic infrastructures. Under these conditions, the operational advantage frequently belongs not to actors possessing the greatest volume of information, but to those capable of shaping orientation, exploiting tempo asymmetries, and operating effectively across fragmented socio-technical ecosystems.

Three interrelated characteristics are particularly decisive in shaping the contemporary operational environment of CogWar: speed, scale, and scope. Together, they alter the cost structure of influence operations while simultaneously increasing the pressure placed on institutional decision-making processes in open societies.

TABLE 4. Speed–Scale–Scope Matrix: Mechanisms, Effects, and Defensive Implications

Dimension	Mechanisms (enablers)	Operational effects	Implication for defence
Speed	Automation (bots/schedulers), AI-assisted authoring, synthetic media	Concept→circulation in minutes; first-mover framing anchors later interpretation (Chesney and Citron 2019)	Shorten verification / coordination; institutional readiness to reduce decision latency to prevent decision drift
Scale	Near-zero marginal distribution; programmatic ads; look-alike audiences; coordinated inauthentic behaviour	Attention hijacking via repeated, affect-rich content; simulated mass (Singer and Brooking 2018; Benkler, Faris and Roberts 2018)	Focus on reach/decay metrics; coalition messaging and credible intermediaries to counter saturation
Scope	Cross-platform, encrypted groups, diaspora media; issue transits (health, economy, security)	Online–offline ricochet; more seams (jurisdictional, linguistic, regulatory, institutional)	Pre-aligned coordination across defence, civil authorities, and Allies; institutional mechanisms to manage jurisdictional seams; shared interpretative indicators across the system

Source: Author’s own elaboration.

First, speed. AI-assisted content generation, automated distribution systems, coordinated amplification networks, and synthetic media technologies dramatically reduce the interval between narrative conception, dissemination, and strategic effect. Information operations that previously required substantial organisational resources can now be conducted rapidly and iteratively at comparatively low cost. The increasing availability of generative AI tools further compresses production cycles, enabling real-time adaptation of messaging, imagery, and audiovisual manipulation during unfolding crises.

The strategic significance of speed lies in the anchoring effect of early interpretation. Under accelerated information conditions, initial narratives frequently shape subsequent public understanding even when later corrections emerge. During the first phases of the war in Ukraine, for example, competing interpretations circulated globally across digital platforms before many institutional actors had established verified situational awareness. Similar dynamics have appeared during electoral crises, terrorist incidents, and public health emergencies, where rapid emotional framing often precedes institutional clarification.

Second, scale. Contemporary digital infrastructures permit near-zero marginal distribution costs combined with increasingly precise audience targeting

mechanisms. Coordinated inauthentic behaviour, bot amplification systems, programmatic advertising ecosystems, and algorithmic recommendation architectures allow relatively small actors to achieve disproportionate information visibility ([Singer and Brooking 2018](#)). Research on networked media ecosystems further suggests that emotionally activating content spreads more efficiently across digital platforms than slower, verification-dependent institutional communication ([Benkler, Faris, and Roberts 2018](#)).

This asymmetry creates an operational environment in which repetition, emotional salience, and visibility frequently matter more immediately than factual robustness. Cognitive operations, therefore, exploit the logic of platform amplification itself, using algorithmic engagement incentives to increase interpretive instability and information saturation.

Third, scope. Contemporary CogWar environments operate across increasingly interconnected and transnational information ecosystems. Influence operations no longer remain confined to isolated media channels or national information spaces.

Instead, narratives circulate fluidly across:

- social media platforms;
- encrypted messaging applications;
- diaspora networks;
- digital influencers;
- state-affiliated media systems;
- commercial information infrastructures;
- and cross-border online communities.

This trans-domain circulation produces ricochet effects between digital and physical environments. Online narratives influence offline political behaviour, while physical events are rapidly reintegrated into digital amplification cycles. During the COVID-19 pandemic, for example, public health decisions, protest movements, conspiracy narratives, institutional trust, and geopolitical competition became deeply intertwined across multiple information layers simultaneously.

Taken together, speed, scale, and scope generate a structurally asymmetric environment. Attackers benefit from low-cost experimentation, rapid iteration, and ambiguity, while defenders remain constrained by verification requirements, legal standards, coalition coordination, and democratic accountability mechanisms.

Attribution, deniability, and the politics of proof

One of the defining characteristics of contemporary CogWar environments is the growing difficulty of attribution under conditions of information complexity and transnational connectivity. Attribution is not merely a technical process of identifying origin points or digital signatures; it is fundamentally political and strategic.

Open societies typically require high evidentiary thresholds before publicly attributing hostile influence activities to state or non-state actors. Democratic institutions must consider legal standards, diplomatic consequences, coalition

coordination, intelligence protection, and public legitimacy before formal attribution occurs. Adversaries exploit this asymmetry through operational architectures specifically designed to complicate proof and delay response.

Contemporary influence ecosystems frequently rely on:

- proxy actors;
- front organisations;
- third-country digital infrastructure;
- commercial intermediaries;
- unofficial online communities;
- and coordinated but loosely networked amplification channels.

The objective is not necessarily perfect concealment, but sufficient ambiguity to slow institutional orientation and complicate proportional response.

Russian electoral interference campaigns and coordinated online influence operations offer particularly illustrative examples. In many cases, attribution emerged incrementally through the aggregation of intelligence indicators, forensic analysis, investigative journalism, and platform disclosures rather than through immediately observable evidence. During this interval, uncertainty itself functioned as a strategic resource, generating hesitation, polarisation, and interpretive contestation.

Similarly, the increasing availability of synthetic media technologies introduces new attribution challenges. Deepfake videos, AI-generated audio, manipulated imagery, and synthetic identity systems reduce confidence in evidentiary authenticity while increasing verification burdens on institutions and media organisations ([Chesney and Citron 2019](#)). Even poorly executed synthetic content may achieve strategic effect if circulated rapidly enough to shape initial public interpretation before debunking occurs.

Under such conditions, the politics of proof become central to strategic competition.

Defenders must simultaneously:

- preserve evidentiary credibility;
- avoid premature attribution;
- maintain coalition coherence;
- and respond quickly enough to prevent interpretive destabilisation.

This tension produces a persistent decisional dilemma in open societies: institutional legitimacy requires procedural caution, yet excessive caution increases operational latency and widens attacker payoff windows.

For this reason, contemporary cognitive defence increasingly depends on coalition-based attribution mechanisms and tactic-level transparency. Publicly exposing operational techniques, amplification methods, and influence architectures may, in some cases, prove strategically more effective than waiting for definitive actor attribution. The objective becomes reducing ambiguity sufficiently to preserve orientation and resilience, even when perfect certainty remains unattainable.

Small-state constraints, allied leverage

The techno-operational environment of CogWar creates particular challenges for small and mid-sized states. Unlike major powers, smaller states frequently operate

with:

- limited specialised personnel;
- reduced technological infrastructure;
- slower procurement cycles;
- narrower intelligence capabilities;
- and limited leverage over global digital platforms.

These constraints increase dependence on external information infrastructures and allied coordination mechanisms. Smaller states may struggle to independently monitor large-scale information ecosystems, rapidly attribute complex operations, or sustain continuous strategic communication efforts across multiple domains simultaneously.

At the same time, small-state vulnerabilities are not purely technical. Cognitive operations targeting smaller states may achieve disproportionate strategic effects because institutional ecosystems are often more compressed and socially interconnected. Limited redundancy across media, political, or administrative systems can increase susceptibility to cascading trust erosion and institutional fragmentation.

However, alliance integration also creates strategic opportunities. NATO and European Union structures provide forms of interpretive interoperability, shared situational awareness, joint attribution capacity, and coordinated strategic signalling that smaller states would struggle to sustain independently. In this sense, coalition integration functions not merely as military reinforcement, but as cognitive and institutional amplification.

The challenge lies in balancing coalition coordination with national political legitimacy and decision autonomy. Effective cognitive defence, therefore, depends less on information centralisation than on interoperable orientation mechanisms capable of preserving shared understanding across allied systems while respecting national institutional frameworks.

This suggests that the strategic value of alliances in the cognitive domain increasingly resides in:

- shared interpretive frameworks;
- coordinated transparency;
- joint exercises;
- common indicators and warning mechanisms;
- and rapid institutional communication channels.

Such structures reduce fragmentation and improve collective orientation without requiring uniform political responses.

Implications for planning horizons

The accelerated and uncertain nature of contemporary CogWar environments places significant pressure on traditional strategic planning models. Linear forecasting assumptions become increasingly fragile under conditions characterised by rapid technological adaptation, information volatility, and nonlinear escalation

dynamics. Under VUCA/BANI conditions, effective planning therefore depends less on predictive precision than on anticipatory adaptability ([Bennett and Lemoine 2014](#); [Cascio 2020](#)). The operational objective is not to forecast specific events accurately, but to reduce strategic surprise while preserving decision optionality and institutional coherence under uncertainty.

A Futures Studies perspective becomes particularly relevant in this context because it shifts attention from deterministic prediction toward structured anticipation, horizon scanning, and scenario-oriented orientation mechanisms ([Schoemaker 1995](#)). In practical terms, this implies integrating lightweight anticipatory routines into institutional decision cycles rather than treating foresight as a separate specialised activity.

Three nested planning horizons become particularly useful.

The first is the immediate operational horizon, focused on rapid situational awareness, interpretive stabilisation, and short-cycle institutional coordination during unfolding information events. Here, tempo and decisional clarity are decisive. The second is the medium-term adaptive horizon, concerned with recurring patterns, evolving tactics, institutional vulnerabilities, and alliance coordination mechanisms. At this level, organisations seek to identify trends, recurring seams, and emerging operational methods.

The third is the long-range strategic horizon, where the focus shifts toward technological evolution, changes in media ecosystems, societal resilience, geopolitical shifts, and structural transformations in the information environment itself.

Importantly, these horizons must remain interconnected. Institutions unable to connect long-range anticipation with operational decision cycles risk producing strategically irrelevant foresight disconnected from actionable orientation. Conversely, institutions focused exclusively on immediate response may gradually lose the ability to interpret structural transformations shaping future cognitive competition.

This reinforces a central argument of the article: effective cognitive defence depends less on technological sophistication alone than on institutional capacity to sustain coherent orientation across time under conditions of persistent uncertainty.

What to measure: toward an operational evaluation framework

One of the persistent difficulties in the cognitive domain concerns evaluation. Traditional military metrics – territory seized, forces destroyed, kinetic effects generated – translate imperfectly into environments where strategic outcomes frequently concern orientation, legitimacy, and decision quality rather than physical destruction.

For this reason, assessment frameworks in CogWar environments should prioritise operational and institutional indicators rather than purely information outputs such as message volume or content removal statistics.

Several dimensions become particularly relevant.

First, decision latency: the interval between detection, orientation, and coordinated

institutional response. Reducing latency without undermining legitimacy becomes a central strategic objective.

Second, recovery time: the ability of institutions and publics to restore operational coherence following information disruption or accelerated narrative surges.

Third, cohesion and trust indicators: measures associated with institutional credibility, cross-group bridging, and the persistence of shared orientation mechanisms under stress.

Fourth, norm compliance: whether responses remain proportionate, lawful, transparent, and democratically legitimate over time.

These indicators are necessarily imperfect. Cognitive competition unfolds through diffuse, cumulative, and nonlinear effects that resist precise quantification. Nevertheless, such measures provide more strategically meaningful orientation than simplistic metrics centred exclusively on visibility, engagement, or content suppression. Importantly, the purpose of evaluation in the cognitive domain should not be to produce illusions of certainty, but to improve institutional learning and adaptive capacity over time.

Bridge to Section 4

This section has examined how accelerated technological environments, attribution complexity, and transnational information ecosystems reshape the operational conditions of contemporary cognitive competition. The analysis suggests that the decisive challenge for open societies lies not merely in information management, but in sustaining lawful speed, institutional coherence, and anticipatory orientation under persistent uncertainty.

The final section, therefore, shifts from operational environment analysis toward doctrinal implications. Specifically, it develops design principles for cognitive defence in open societies centred on legitimacy, anticipation, procedural coherence, and coalition interoperability as foundations for long-range strategic adaptation.

From Method to Doctrine: Design Principles for Cognitive Defence in Open Societies

The preceding sections established cognition as a strategic centre of gravity in open societies and identified time, ambiguity, attribution, and decision quality as decisive variables in sub-threshold competition. The remaining challenge is doctrinal: how can defence institutions translate these insights into a sustainable cognitive defence posture without undermining the democratic foundations they are tasked to protect? This section, therefore, moves from analytical method to doctrinal design. It does not propose an operational playbook or a centralised model of narrative control. Instead, it articulates principles that can guide doctrine, education, planning, and institutional adaptation in NATO and EU-oriented open societies. The aim is to define the trade-offs that cognitive defence must manage if it is to remain strategically effective, legally bounded, and politically legitimate.

Tempo versus Legitimacy

Cognitive competition rewards speed. Early framing advantages can shape public interpretation before institutional verification, legal assessment, or coalition coordination are complete. In accelerated information environments, delayed orientation can become a strategic vulnerability: institutions may be factually correct but operationally late.

Yet in open societies, speed cannot be pursued at the expense of legitimacy. Cognitive defence measures perceived as opaque, disproportionate, politically instrumentalised, or procedurally irregular may produce short-term tactical gains while eroding public trust. This is a central doctrinal tension: democratic institutions must become faster without becoming arbitrary.

The relevant objective is therefore not maximum speed, but lawful speed. This means pre-defining authorities, thresholds, communication routines, evidentiary standards, and escalation pathways before crisis conditions emerge. Institutional tempo should arise from prior alignment and rehearsed procedures, not improvised exceptionalism.

In practical doctrinal terms, this implies:

- clear mandates for monitoring, assessment, and response;
- pre-agreed thresholds for escalation;
- rapid but reviewable decision processes;
- communication protocols that distinguish confirmed facts from assessed probabilities;
- and mechanisms for correction when initial assessments change.

Lawful speed protects both effectiveness and legitimacy. It shortens the attacker's payoff window while preserving the procedural credibility on which democratic resilience depends.

Anticipation versus Democratic Accountability

Strategic anticipation is indispensable in the cognitive domain. Because influence operations often unfold gradually through pre-positioned narratives, trust erosion, and repeated probing, institutions cannot rely solely on reactive crisis response. They need horizon scanning, scenario thinking, and early-warning indicators capable of identifying emerging vulnerabilities before they become acute.

However, anticipation carries its own democratic risks. Foresight mechanisms can drift toward technocratic control if they are used to pre-empt public debate, classify dissent as threat activity, or insulate security assessments from scrutiny. In open societies, the purpose of anticipation cannot be narrative management or political pre-emption. It must be orientation: improving preparedness while preserving pluralism and contestation.

The doctrinal distinction is essential. Cognitive defence should not seek to determine what citizens ought to believe. It should seek to improve institutional capacity to

detect hostile manipulation, understand evolving threat patterns, and respond proportionately when adversarial activity targets decision quality, public trust, or institutional legitimacy.

Accordingly, anticipatory practices should be:

- explicitly bounded in scope;
- separated from partisan political interests;
- subject to legal and institutional oversight;
- periodically reviewed;
- and open to correction when assumptions prove wrong.

This is where Futures Studies can contribute without becoming predictive or controlled. Horizon scanning, alternative scenarios, signposts, and structured uncertainty analysis help institutions think across multiple plausible futures while avoiding deterministic threat narratives. Used properly, foresight strengthens democratic accountability because it makes assumptions visible and revisable rather than hidden inside crisis improvisation.

Institutional Speed versus Procedural Safeguards

CogWar exploits seams between institutions, jurisdictions, legal regimes, and public-private systems. Fragmented mandates, unclear escalation routes, slow clearance procedures, and competing institutional vocabularies all increase decision latency. In this sense, bureaucratic friction can become an operational vulnerability.

The doctrinal temptation is to respond through centralisation: creating single authorities, emergency powers, or command structures capable of bypassing ordinary procedures. In some crisis conditions, central coordination may be necessary. Yet excessive centralisation risks weakening the very safeguards that differentiate democratic cognitive defence from authoritarian information control.

The more sustainable doctrinal answer is not to collapse procedural safeguards, but to make them interoperable under stress. Institutions should know in advance how their mandates connect, how information flows across agencies, how legal advice is obtained rapidly, how public communication is coordinated, and how private platforms, civil society actors, and allied partners are engaged.

This requires shared interpretive frameworks rather than unified command over public discourse. Defence institutions, intelligence services, regulators, public communicators, electoral authorities, public health agencies, and diplomatic actors may all perceive different parts of the same cognitive operation. Without a common vocabulary and pre-agreed coordination routines, these perceptions remain fragmented.

Doctrinal design should therefore prioritise:

- shared taxonomies of cognitive threats and influence techniques;
- inter-agency exercises;
- standing liaison mechanisms;

- pre-cleared communication templates;
- legal review pathways;
- and after-action learning processes.

Procedural safeguards should not be seen as obstacles to tempo. Properly designed, they are the conditions that allow institutions to act quickly without losing legitimacy.

Coalitional Alignment versus National Autonomy

Contemporary CogWar is rarely confined within national boundaries. Influence operations across languages, platforms, jurisdictions, diaspora networks, and alliance spaces. This makes coalition coordination increasingly important, particularly for small and mid-sized states that lack the scale, technological capacity, or platform leverage to act alone.

NATO and EU contexts offer significant advantages: shared situational awareness, common threat vocabularies, joint exercises, coordinated attribution, strategic signalling, and institutional learning across national systems. Coalitional alignment can reduce ambiguity, increase reputational costs for hostile actors, and strengthen resilience through shared indicators and comparative experience.

Yet cognitive defence cannot simply be outsourced to alliances. Political legitimacy, legal authority, public communication, and democratic accountability remain nationally anchored. Each state must retain responsibility for how it interprets threats, communicates with its citizens, and calibrates response within its constitutional and political context.

The doctrinal challenge is therefore to distinguish between shared cognition and sovereign decision. Shared cognition refers to common indicators, analytical categories, warning mechanisms, and interpretive frameworks. Sovereign decision refers to nationally accountable choices regarding attribution, legal action, public communication, diplomatic response, or operational measures.

Effective doctrine should seek interoperability of interpretation, not uniformity of response. Allies do not need to react identically to every cognitive threat. They do need to recognise comparable patterns, understand each other's thresholds, communicate rapidly, and coordinate when collective action increases legitimacy or deterrent effect.

For smaller states in particular, this distinction is crucial. Coalitions can provide scale, expertise, and credibility, but national institutions must remain the primary holders of democratic trust. The goal is not dependency, but reinforced autonomy through interoperable alignment.

Doctrinal Implication

Taken together, these four design tensions suggest that cognitive defence in open societies should be understood less as a discrete capability set than as a decision discipline. Its effectiveness depends on how institutions organise time, legitimacy, anticipation, procedure, and coalition alignment under conditions of uncertainty.

This has several doctrinal implications.

First, cognitive defence should be integrated into strategic planning rather than treated as an episodic communication function. The relevant problem is not only what messages are produced, but how institutions orient themselves, decide, coordinate, and learn under information pressure.

Second, cognitive defence should privilege resilience over control. Open societies cannot and should not seek information dominance through coercive narrative management. Their comparative advantage lies in credible institutions, plural verification, lawful transparency, and adaptive learning.

Third, doctrine should define trade-offs explicitly. Speed must be balanced with legitimacy; anticipation with accountability; coordination with safeguards; coalitional alignment with national autonomy. If these tensions remain implicit, crisis conditions will force ad hoc decisions that may undermine trust.

Fourth, evaluation should focus on decision quality, latency, recovery, cohesion, and norm compliance rather than superficial visibility metrics. The success of cognitive defence is not measured by narrative victory alone, but by the sustained ability of institutions and publics to remain oriented and legitimate under pressure.

The doctrinal conclusion is therefore clear: cognitive defence ultimately concerns the disciplined organisation of democratic decision-making under persistent strategic manipulation, drawing on longstanding military experience in orientation, coordination, anticipation, and action under conditions of uncertainty.

Conclusions

This article examined how open societies can design long-range strategy in the cognitive domain under conditions of strategic uncertainty, technological acceleration, and persistent sub-threshold competition. Drawing on a conceptual-doctrinal and futures-oriented analytical framework, the analysis argued that contemporary CogWar is best understood not primarily as a struggle for narrative dominance, but as a contest over orientation, tempo, legitimacy, and decision quality across increasingly dilated socio-technical battlefields.

The analysis identified two structural paradoxes shaping the strategic environment of open societies. The openness paradox demonstrated how the same information and technological conditions that enable democratic pluralism, innovation, and participation also generate fragmentation, accelerated information volatility, and vulnerabilities exploitable through manipulation and ambiguity. The deterrence paradox showed how the long post-1945 emphasis on escalation avoidance and strategic stability unintentionally incentivised indirect and deniable forms of competition operating below the threshold of armed conflict.

Taken together, these paradoxes reposition cognition as a strategic centre of gravity. Under contemporary conditions, strategic advantage increasingly derives from the ability to preserve institutional orientation, lawful decisional tempo, coalition coherence, and public legitimacy under persistent information pressure. The

challenge is therefore not merely technological or communicational. It concerns how democratic systems organise anticipation, coordination, and strategic adaptation under uncertainty.

The article further argued that the techno-operational environment of CogWar amplifies these pressures through speed, scale, and scope. AI-assisted content generation, synthetic media, automated amplification, and transnational digital ecosystems compress verification windows, complicate attribution, and increase asymmetries between rapidly adaptive attackers and procedurally constrained defenders. In such environments, ambiguity and time themselves become operational instruments.

Against this background, the article proposed a doctrinal perspective centred on four design tensions: tempo versus legitimacy; anticipation versus democratic accountability; institutional speed versus procedural safeguards; and coalitional alignment versus national autonomy. These tensions cannot be eliminated, but they can be managed explicitly through strategic doctrine, anticipatory governance routines, and interoperable institutional frameworks capable of sustaining lawful speed and adaptive coordination under pressure.

The central implication is that cognitive defence in open societies should be understood less as a discrete operational capability than as a disciplined approach to democratic decision-making under conditions of persistent strategic manipulation. This does not imply the militarisation of democratic public space, but rather the adaptation of doctrinal disciplines long developed within military contexts – anticipation, coordination, orientation, and action under uncertainty – to the governance requirements of open societies operating in accelerated information environments.

In this sense, military institutions possess relevant experience not because democratic societies should emulate wartime command structures, but because military doctrine has historically grappled with many of the organisational problems now re-emerging in the cognitive domain: friction, ambiguity, tempo asymmetry, adversarial adaptation, coalition coordination, and decision-making under uncertainty. The contribution of military thought, therefore, lies less in securitising information space than in informing how democratic institutions can preserve coherence and legitimacy while operating under persistent cognitive pressure.

The article also suggests that effective cognitive defence depends less on information dominance than on resilience of orientation. Open societies cannot realistically eliminate ambiguity, prevent all manipulation, or control information ecosystems without undermining the very freedoms that constitute their strategic legitimacy. Their comparative advantage lies instead in the ability to sustain credible institutions, plural verification mechanisms, coalition interoperability, lawful adaptation, and public trust over long temporal horizons.

Several limitations should nevertheless be acknowledged. Given its conceptual and doctrinal orientation, the article did not seek to produce empirical causal testing, operational modelling, or quantitative measurement frameworks. The operational illustrations included throughout the analysis were intended to ground the conceptual discussion rather than function as formal comparative case studies. Future research could therefore expand this framework through empirical examination of decision latency in crisis environments, comparative analysis of national cognitive defence models, alliance interoperability mechanisms, or the development of operational indicators capable of assessing institutional resilience under information pressure.

Ultimately, the strategic challenge confronting open societies is neither purely information nor purely technological. It is epistemological and organisational. In increasingly accelerated and contested information environments, the ability of democratic systems to think, decide, coordinate, and adapt coherently under uncertainty may become one of the defining strategic variables of contemporary competition.

References

- Beaufre, André.** 1965. *An Introduction to Strategy, with Particular Reference to Problems of Defence, Politics, Economics, and Diplomacy in the Nuclear Age*. New York: Praeger.
- Benkler, Yochai, Robert Faris, and Hal Roberts.** 2018. "Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics." Edited by Oxford University Press. <https://doi.org/10.1093/oso/9780190923624.001.0001>.
- Bennett, Nate, and G. James Lemoine.** 2014. "What VUCA Really Means for You." January–February.
- Cascio, W.F.** 2020. "Managing a Brittle, Anxious, Nonlinear, Incomprehensible World."
- Chesney, Robert, and Danielle Keats Citron.** 2019. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107(6): 1753-1819.
- Clausewitz, Carl von.** 1976. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press.
- European External Action Service.** 2023. "1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence." Brussels: European External Action Service.
- Freedman, Lawrence.** 2013. *Strategy: A History*. Oxford: Oxford University Press.
- Gray, Colin S.** 2010. *The Strategy Bridge: Theory for Practice*. Oxford: Oxford University Press.
- Hart, Liddell.** 1967. *Strategy*. 2nd revised edition. New York: Frederick A. Praeger.
- Mazarr, Michael J.** 2015. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. Carlisle, PA: U.S. Army War College Press.

- Pariser, Eli.** 2011. *The Filter Bubble: What the Internet Is Hiding from You*. New York: Penguin Press.
- Rid, Thomas.** 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux.
- Schelling, Thomas.** 1966. *Arms and Influence*. New Haven, CT: Yale University Press.
- Schoemaker, Paul J.H.** 1995. "Scenario Planning: A Tool for Strategic Thinking." 36(2) ed.: 25–40.
- Simon, Herbert A.** 1971. *Designing Organizations for an Information-Rich World*. Edited by Martin Greenberger. Vols. Computers, Communications, and the Public Interest. Baltimore: Johns Hopkins University Press.
- Singer, P.W., and Emerson T. Brooking.** 2018. *Like War: The Weaponization of Social Media*. Boston: Houghton Mifflin Harcourt.
- Sunstein, Cass R.** 2009. *Going to Extremes: How Like Minds Unite and Divide*. Oxford: Oxford University Press.
- World Health Organization.** 2020. "Managing the COVID-19 Infodemic: Promoting Healthy Behaviours and Mitigating the Harm from Misinformation and Disinformation." Geneva: World Health Organization.

ACKNOWLEDGEMENTS

We would like to acknowledge the support of the Military Academy Research Centre (CINAMIL), which has been instrumental in the completion of this research.

FUNDING INFORMATION

The authors declare that no funding or financial support was received from any organisation, institution, or individual for the research, design, execution, or writing of this work.

CONFLICT OF INTEREST STATEMENT

The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

DATA AVAILABILITY STATEMENT

The data supporting this study are derived from publicly available sources and referenced within the article. No additional datasets were generated or analysed specifically for this research.

DECLARATION ON AI USE

The author confirms that AI tools, including language models such as ChatGPT, NotebookLM, and DeepL, were used solely to enhance the writing process, improve readability, and assist with grammar and formatting. All intellectual content, analysis, and critical arguments are the result of the author's original work. The AI tools were not used to generate research findings or substitute independent scholarly work.

Contemporary Warfare and the Transformation of the Global Military Paradigm

MAJ Cristian-Alexandru SALAC, PhD Candidate*

*Ministry of National Defence

e-mail: salac_cristian@yahoo.com

 <https://orcid.org/0009-0000-2157-2698>

Abstract

This article analyzes the transformation of the global military paradigm in the context of the technological and strategic developments of the 21st century, using a qualitative approach based on the analysis of specialized literature and the conceptual interpretation of contemporary conflicts. The analysis employs illustrative examples from the Russo-Ukrainian War, the Nagorno-Karabakh conflict, and the field of cyber operations in order to highlight recent transformations of the operational environment. The findings indicate that contemporary warfare is evolving toward a multidimensional model in which the cyber, information, economic, and space domains are becoming as relevant as the traditional military dimension.

The analysis shows that emerging technologies – digitalization, artificial intelligence, drones, and orbital infrastructures – not only support military operations, but also reshape the criteria of strategic superiority, favoring actors capable of coherently integrating information and innovation. Furthermore, the cyber and information dimensions enable the conduct of persistent strategic competition below the threshold of open armed conflict.

The results highlight the need to adapt military structures to a multidomain operational model characterized by interdependence, decision-making speed, and technological integration. This paper contributes to the conceptual clarification of contemporary warfare and emphasizes the strategic implications of ongoing transformations for global security.

Keywords:

Contemporary Warfare; Hybrid Warfare; Cybersecurity; Multi-domain Operations;
Emerging Technologies; Information Superiority.

Article info

Received: 29 January 2026; Revised: 19 February 2026; Accepted: 17 March 2026; Available online: 30 June 2026

Citation: Salac, C.A. 2026. "Contemporary Warfare and the Transformation of the Global Military Paradigm."
Bulletin of "Carol I" National Defence University, 15(2): 257-272. <https://doi.org/10.53477/2284-9378-26-27>



© „Carol I” National Defence University Publishing House

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC-SA)

Introduction

The developments in the security environment over recent decades indicate a profound structural transformation in the nature of warfare and in the way military power is conceived, organized, and employed. Contemporary conflicts can no longer be analyzed exclusively through the lens of conventional armed confrontations between states, but must instead be understood as multidimensional processes conducted simultaneously across interconnected domains – physical, information, economic, cyber, and space-related ([Freedman 2017](#), 45-52; [Mazarr 2015](#), 3-7).

Concepts such as hybrid warfare, gray-zone competition, information operations, and cyber conflicts have become essential for understanding the new dynamics of international security. Digital technologies, artificial intelligence, autonomous systems, and orbital infrastructures are no longer merely support tools, but structural factors that influence the distribution of power and the doctrinal architecture of armed forces ([Horowitz 2010](#), 4-8; [Johnson 2022](#), 1397).

The purpose of this research is to analyze the manner in which the technological and strategic transformations of the 21st century contribute to redefining the global military paradigm and shaping a persistent multidimensional conflict model characterized by the simultaneous integration of conventional and non-conventional instruments.

To achieve this purpose, the paper pursues the following research objectives: identifying the main characteristics of contemporary warfare in relation to the traditional paradigm;

- analyzing the role of emerging technologies in the transformation of modern conflicts;
- examining the impact of the cyber and informational dimensions on security;
- evaluating the implications of these transformations on the organization and functioning of modern armed forces.

In order to provide structure to the analytical approach, the following research questions are formulated:

1. To what extent do current technological transformations alter the nature of armed conflicts?
2. What is the role of the cyber and informational dimensions in redefining power relations?
3. How do these developments influence the organization and functioning of the modern military?

Through this approach, the paper contributes to the conceptual clarification of contemporary warfare and highlights the strategic implications of ongoing transformations for global security and the organization of armed forces, in line

with recent directions emphasized in the literature on security and strategic studies (Manolache 2023, 164).

1. Research Methodology

This paper is based on a qualitative, analytical, and conceptual approach, suitable for studying complex phenomena in the field of international security and the transformation of contemporary conflicts. Given the dynamic and multidimensional nature of modern warfare, the research aims to identify and interpret the main strategic, technological, and doctrinal trends influencing the redefinition of the global military paradigm.

The units of analysis used in this research consist of relevant contemporary conflicts (the Russo-Ukrainian War and the Nagorno-Karabakh conflict), recent doctrinal developments (multi-domain operations), and technological transformations applied to the military environment (drones, cyber capabilities, and artificial intelligence). The analysis seeks to identify the relationships among technological development, changes in the operational environment, and the doctrinal adaptation of military actors.

The comparative analysis was conducted by relating the analyzed cases and developments to three main criteria: the expansion of conflict into non-conventional domains, the integration of emerging technologies, and the transformation of military actors' decision-making and operational processes.

The methodological approach primarily employs a literature review, selecting relevant academic works from the fields of strategic studies, international security, and military technologies. The analyzed sources include articles from indexed journals, monographs, and research reports, which provide both theoretical perspectives and interpretations of recent developments in the security environment. The selection of sources was based on their relevance, timeliness, and contribution to understanding the transformation of contemporary warfare.

In order to increase analytical consistency, the research also uses illustrative examples from recent conflicts to highlight the practical applicability of the analyzed concepts and the manner in which technological transformations influence the conduct of contemporary operations.

The study also employs the comparative analysis method to highlight the differences and continuities between the traditional paradigm of warfare and contemporary forms of conflict, such as hybrid warfare, gray-zone competition, and cyber confrontations. This method enables the identification of novel elements and the determining factors of change, particularly in relation to the development of emerging technologies.

Furthermore, the paper uses conceptual analysis aimed at clarifying and defining key concepts such as "hybrid warfare," "multi-domain operations," "cybersecurity,"

and “persistent strategic competition.” This approach contributes to a coherent understanding of the theoretical framework and to the integration of various perspectives existing in the specialized literature.

The data analysis methods are predominantly qualitative, based on critical interpretation, information correlation, and the identification of causal relationships between the analyzed variables (technology, strategy, actors, and operational environments). The research does not employ quantitative methods or statistical instruments, as its primary objective is to explain and understand phenomena rather than measure them.

The limitations of the research derive from the predominantly theoretical nature of the analysis and the absence of extensive empirical studies or quantitative datasets. Nevertheless, the conceptual-analytical approach makes it possible to highlight major trends and formulate relevant conclusions regarding the evolution of contemporary conflicts.

By employing these methods, the research aims to provide an integrated perspective on the transformation of the global military paradigm and to contribute to the development of the conceptual framework necessary for analyzing warfare in the 21st century.

2. The Metamorphosis of Warfare in the 21st Century

The 21st century marks a profound transformation of warfare, not only in technological terms, but also in conceptual and strategic ones. The analysis of recent developments in the security environment highlights the fact that contemporary conflicts can no longer be reduced to conventional military confrontations between states, but must instead be understood as multidimensional phenomena in which the physical, information, economic, and cyber domains interact continuously (Freedman 2017, 48-49).

The analyzed transformations indicate a structural change in the way power is exercised, reflected in the expansion of the battlefield beyond the classical military dimension. This evolution suggests that contemporary warfare is acquiring the characteristics of a continuous process marked by ambiguity, interdependence, and persistent competition below the threshold of open conflict (Mazarr 2015, 6-7). Strategic relevance is no longer determined exclusively by the ability to project force, but by the capability of actors to integrate military and non-military instruments into a coherent framework of influence.

2.1. The Transition from Conventional Conflicts to Hybrid Warfare

Hybrid warfare represents one of the most relevant manifestations of the transformation of conflict in the 21st century. Specialized literature indicates that these forms of conflict are characterized by the integration of conventional military actions with non-traditional tactics, such as cyberattacks, disinformation campaigns,

economic pressure, and the use of proxy actors (Hoffman 2018, 30).

It can be observed that the defining characteristic of hybrid warfare lies in the adaptive synchronization of these instruments, aimed at exploiting the adversary's systemic vulnerabilities. In this sense, the strategic objective is no longer necessarily the immediate control of territory, but rather political and institutional destabilization (Mazarr 2015, 10-11).

Recent conflicts, particularly the war in Ukraine, suggest that hybrid actions may precede and accompany conventional operations, confirming their integrated and flexible nature (Watling 2023, 5-6). Therefore, the hypothesis according to which contemporary warfare is evolving toward a multidimensional model, in which non-conventional instruments become essential, is confirmed.

The Russo-Ukrainian War represents one of the most relevant examples of the convergence between conventional operations and hybrid instruments. Beginning with the annexation of Crimea in 2014 and continuing with the 2022 invasion, the Russian Federation combined classical military operations with cyberattacks, disinformation campaigns, and energy pressure. The synchronized use of these instruments aimed not only at achieving territorial advantages but also at the political and psychological destabilization of the adversary.

2.2. State and Non-State Actors in the New Conflict Dynamics

The interaction between state and non-state actors constitutes a defining element of contemporary conflicts. Non-state actors no longer represent merely peripheral entities, but rather relevant actors capable of influencing strategic dynamics at both the regional and global levels (Salehyan 2009, 16-17).

Through the use of transnational networks, the information environment, and infrastructural vulnerabilities, these actors are capable of generating strategic effects disproportionate to the resources they possess. This evolution confirms the growing asymmetry of conflicts, in which the advantage no longer belongs exclusively to actors with conventional military superiority (IISS 2024, 15-16).

The interdependence between state and non-state actors contributes to increasing the complexity of conflicts, requiring the development of integrated strategies that combine military, political, and information instruments. In this context, international cooperation and collective security mechanisms become essential for managing emerging risks.

2.3. The Gray Zone and Competition Below the Threshold of Direct Confrontation

The concept of the "gray zone" describes a spectrum of strategic competition situated between peace and war, in which actors seek to obtain advantages through ambiguous, gradual, and difficult-to-attribute actions. Conceptual analysis highlights that this form of competition represents a defining characteristic of the contemporary security environment (Mazarr 2015, 6-7).

Operations conducted within the gray zone, including cyberattacks, information influence campaigns, and economic pressure, enable the gradual erosion of an adversary's security without triggering open conflict. This approach reduces the risk

of direct escalation and complicates deterrence processes and strategic responses (NATO 2022, 5-7).

Recent NATO strategic documents emphasize that hybrid threats and persistent competition below the threshold of armed conflict represent one of the principal challenges to Euro-Atlantic security, as they combine military and non-military instruments in a manner that is difficult to attribute and counter (NATO 2022, 5-7).

Gray-zone competition confirms the transformation of warfare into a continuous process characterized by persistent and multidimensional pressure and strongly demonstrates the hypothesis that the traditional distinction between peace and war is becoming increasingly blurred, being replaced by a continuum of strategic confrontation.

3. Technology as a Transformative Force in Contemporary Warfare

Technology represents one of the principal factors driving the profound transformation of contemporary warfare, influencing not only tactical capabilities but also the way military power is conceived and employed at the strategic level. The analysis of specialized literature highlights that the integration of emerging technologies alters the distribution of power and the competitive advantage among actors, favoring those capable of rapidly adopting and integrating innovation (Horowitz 2010, 4–8).

Military superiority is no longer determined exclusively by material resources or the size of armed forces, but by the ability to integrate technology into coherent operational structures and to exploit informational advantages (Horowitz 2010, 15; Biddle 2022, 32).

3.1. The Digital Revolution and Its Impact on Military Tactics

The digital revolution constitutes one of the main structural factors behind the transformation of contemporary warfare, simultaneously influencing the tactical, operational, and strategic levels. The integration of information technologies into military structures has generated an operational environment characterized by extensive connectivity and continuous data flows. This process enables the real-time analysis and utilization of data originating from multiple sources. Recent literature highlights that digitalization redefines the manner in which military power is generated and employed, surpassing the traditional paradigm based on material superiority (Jensen, Valeriano, and Maness 2019, 212–214).

The results of the analysis indicate that information becomes an essential force multiplier, while operational success increasingly depends on the ability to collect, integrate, and exploit data at a faster pace than the adversary. The integration of digital technologies leads to the compression of the decision-making cycle and to the growing relevance of information superiority, which enables actors to obtain strategic advantages even under conditions of material inferiority (Biddle 2022, 35).

At the tactical level, digitalization facilitates the coordination of dispersed units and the integration of weapon systems into common networks, contributing to increased

operational flexibility. At the same time, this dependence on digital infrastructures generates significant vulnerabilities, as information systems become targets for cyberattacks capable of producing disproportionate strategic effects (Kello 2013, 18-21). Therefore, the hypothesis according to which the digital revolution fundamentally transforms the logic of military action, shifting the emphasis from quantitative superiority to informational superiority, is confirmed.

3.2. Drones and the Reduction of Technological Monopoly

The proliferation of unmanned aerial vehicles (UAVs) represents one of the most significant technological developments in contemporary warfare, contributing to changes in the balance of power and reducing barriers to access to aerial capabilities. Specialized literature shows that drones enable both states and non-state actors to conduct surveillance, reconnaissance, and precision-strike operations at relatively low costs (Boyle 2015, 4).

These systems contribute to the reduction of technological monopoly, redistributing strategic advantage and favoring the emergence of asymmetric forms of conflict. Recent conflicts, particularly the war in Ukraine, demonstrate the central role of drones in transforming combat tactics and increasing the importance of remote operations, where precision and adaptability become decisive factors (Watling 2023, 5-6).

The Nagorno-Karabakh conflict (2020) highlighted the major impact of drones on the balance of power at the tactical and operational levels. Azerbaijan employed Bayraktar TB2 drones and loitering munitions to neutralize Armenian air defense systems and armored equipment, demonstrating the capacity of relatively accessible systems to produce significant strategic effects. Subsequently, the war in Ukraine confirmed this trend through the large-scale use of FPV drones for the identification and engagement of targets in real time.

These developments suggest that the accessibility of autonomous technologies reduces the exclusive advantage of traditional military actors and encourages the emergence of asymmetric forms of competition based on flexibility and rapid adaptation.

Analyses conducted by the Royal United Services Institute show that the use of tactical drones in Ukraine contributed to reducing the time between target identification and strike execution, significantly increasing the effectiveness of artillery and reconnaissance operations (Watling 2023, 18-19).

Therefore, drones represent not merely a technological instrument, but a factor that directly influences the conduct of conflicts and the distribution of power among actors.

3.3. Artificial Intelligence, Autonomous Systems, and the Automation of the Battlefield

The integration of artificial intelligence and autonomous systems into the military domain marks a significant stage in the transformation of contemporary warfare. These technologies enable the rapid analysis of data, pattern identification, and the optimization of operational decisions under conditions of high uncertainty (Scharre 2018, 37-38).

The results of the analysis indicate that artificial intelligence contributes to accelerating the decision-making cycle and increasing operational efficiency, becoming an information-based force multiplier. Recent literature emphasizes that the use of autonomous systems raises significant ethical and strategic challenges, particularly regarding decision-making responsibility and human control over the use of force (Johnson 2022, 1397-1399).

Recent studies on the integration of artificial intelligence into the military domain suggest that the automation of analytical and decision-support processes may fundamentally alter the pace and logic of contemporary conflicts (Payne 2021, 76-77). Moreover, recent analyses concerning the integration of artificial intelligence into military affairs suggest that autonomous systems will significantly influence decision-making speed and the architecture of future operations (Konaev 2023, 15-16).

Therefore, the analysis highlights that the integration of artificial intelligence transforms not only military capabilities but also the very nature of decision-making in warfare.

3.4. The Militarization of Space and Orbital Infrastructures

Outer space has become an essential operational domain for the conduct of modern military operations, providing decisive strategic advantages in communications, navigation, and surveillance. Recent analyses in the field of strategic studies indicate that orbital infrastructures are directly integrated into the architecture of multidomain operations (Manolache 2023, 163).

Dependence on these infrastructures generates critical vulnerabilities, since the disruption or destruction of space systems may affect command-and-control capabilities. In addition, the development of anti-satellite capabilities and cyberattacks against orbital systems amplifies the risks associated with space security. Thus, the trend toward the expansion of conflict into new domains, including outer space, is confirmed, reinforcing the multidimensional character of contemporary warfare.

4. The Cyber Dimension of Conflict: A Vector in Contemporary Warfare

The cyber dimension has become a central component of contemporary conflicts, redefining the manner in which power is exercised in international relations. Unlike the traditional domains of confrontation, cyberspace enables the conduct of operations with significant strategic impact without the mobilization of conventional military force, altering the relationship among cost, attribution, and strategic effect in contemporary competition (Kello 2013, 7; Schmitt 2017, 3).

Specialized literature emphasizes the fact that cyber operations can influence political, economic, and social processes, affecting the stability of states without necessarily generating a direct military response (Kello 2013, 8). The difficulty of attributing attacks, combined with the relatively low costs of conducting them, encourages the use of cyber instruments as part of persistent strategic competition.

In this context, control over digital infrastructures and information flows becomes an essential element of power.

4.1. Cyberattacks and the Vulnerability of Critical Infrastructures

Cyberattacks against critical infrastructures highlight the vulnerabilities generated by the extensive digitalization of modern societies. Energy, financial, communication, and transportation systems are deeply interconnected, and this interdependence creates the conditions for cascading effects, in which the disruption of one element may affect the entire system.

A relevant example is the cyberattack against Ukraine's energy infrastructure in 2015, which caused power outages affecting approximately 230,000 people. The operation demonstrated that cyberattacks can generate significant strategic effects without the use of conventional armed force, highlighting the vulnerability of digitally integrated critical infrastructures.

Analyses in the specialized literature show that such attacks can produce major dysfunctions without the use of armed force, affecting the functioning of essential services and generating economic and social instability (Kello 2013, 18-19). Recent examples, including cyber operations associated with the conflict in Ukraine, highlight the ability of these actions to amplify the effects of confrontation through the disruption of critical infrastructures.

The asymmetric character of cyberattacks enables actors with limited resources to generate disproportionate strategic effects. This reality alters the traditional logic of conflict, in which material superiority no longer guarantees security. Consequently, the protection of critical infrastructures becomes a strategic priority, while cybersecurity is increasingly integrated into national defense policies.

4.2. Information Warfare: Disinformation and Strategic Manipulation

Information warfare constitutes an essential dimension of contemporary conflicts, in which influencing perceptions becomes a strategic objective in itself. The development of digital platforms and social networks has facilitated the conduct of disinformation campaigns capable of affecting social cohesion and decision-making processes at both the national and international levels.

Recent studies highlight that informational manipulation can erode trust in institutions, amplify social polarization, and influence electoral behavior, thereby contributing to the internal destabilization of states (Jensen, Valeriano, and Maness 2019, 219). Unlike traditional propaganda, these operations employ algorithms and digital amplification mechanisms that enable the rapid and widespread dissemination of content.

This dynamic reflects a significant change in the way power is exercised, in which control over narratives becomes as important as military superiority. In this context, the distinction between truthful information and disinformation becomes increasingly difficult, complicating response and counteraction processes.

4.3. Cyber Defense and the Development of National Resilience

The growing complexity of cyber threats has led to a paradigm shift in the approach to security, moving from the strictly technical protection of systems toward the development of resilience. This involves not only preventing attacks, but also the ability to absorb their impact and rapidly restore the functioning of affected systems. Specialized literature points out that cyber resilience requires the integration of institutional mechanisms, coherent public policies, and cooperation between the public and private sectors. The interdependence of critical infrastructures means that security can no longer be ensured exclusively at the national level, making international coordination necessary.

In this context, the capacity of states to manage cyber risks becomes an essential indicator of security. Continuous adaptation to the evolution of threats and the development of rapid-response mechanisms are fundamental elements for maintaining stability in the digital environment.

4.4. The Integration of Cyber Capabilities into Military and Geopolitical Strategies

The cyber dimension has progressively been integrated into military and geopolitical strategies, becoming an instrument for the projection of power and strategic influence. States are developing offensive cyber capabilities that enable them to conduct espionage, disruption, and influence operations without crossing the threshold of open armed conflict.

This evolution extends the logic of gray-zone competition, in which strategic pressure is exerted through non-conventional instruments, exploiting ambiguity and the difficulty of attribution (Mazarr 2015, 3-7). Within this framework, conflict is no longer limited to discrete episodes of confrontation, but acquires the character of a continuous process.

The integration of the cyber dimension into state strategies influences the global balance of power, as digital capabilities become an essential element of strategic competitiveness. This reality requires the development of adapted doctrinal and legal frameworks, as well as the strengthening of international cooperation for managing associated risks.

Recent literature in the field of international law applicable to cyberspace highlights the difficulties in defining the threshold between cyber operations and acts of aggression, as well as the problems related to attribution and state responsibility (Schmitt 2017, 11-12).

5. The Transformation of the Modern Military

The transformation of the modern military reflects the adaptation of military structures to a security environment characterized by complexity, interdependence, and the accelerated pace of technological change. Armed forces can no longer be analyzed exclusively through the lens of troop size or conventional capabilities, but rather as integrated systems capable of operating simultaneously across multiple domains and exploiting the advantages provided by emerging technologies.

Specialized literature highlights that this transformation has a dual dimension: on the one hand, technological, through the integration of digital systems and artificial intelligence, and on the other hand, organizational, through the adaptation of doctrines and decision-making processes ([Manolache 2023](#), 169-170). The accelerated pace of change requires the development of flexible structures capable of responding rapidly to developments in the operational environment.

5.1. The Concept of Multi-Domain Operations (MDO)

The concept of Multi-Domain Operations (MDO) reflects the evolution of military thinking toward the simultaneous integration of effects across the land, air, naval, cyber, and space domains. This approach goes beyond the traditional logic of combined operations, emphasizing rapid coordination and the synchronization of capabilities in complex operational environments.

Recent doctrinal strategies developed by the U.S. Department of Defense emphasize the necessity of integrating capabilities from all operational domains into a common command-and-control architecture based on rapid data exchange and real-time coordination ([U.S. Department of Defense 2022](#), 11-13).

The Multi-Domain Operations concept is reflected in recent U.S. Army doctrine, which aims to integrate effects generated across the land, air, naval, cyber, and space domains into a unified command-and-control system. The conflict in Ukraine demonstrates the applicability of this model through the integration of satellite imagery, tactical drones, and precision artillery into an accelerated decision-making cycle.

Recent analyses emphasize that operational success depends on the ability to integrate information originating from multiple domains and to generate convergent effects against the adversary ([Manolache 2023](#), 165-166). System interconnectivity and data-processing speed become determining factors of military effectiveness, while superiority is no longer associated with control over a single domain, but rather with the capacity to act coherently across all domains.

This evolution implies significant doctrinal and organizational adaptations, including the development of command structures capable of managing the complexity of multidomain operations.

5.2. The Digitalization of Logistics and the Optimization of Supply Chains

Military logistics has undergone an accelerated process of transformation driven by the integration of digital technologies and the increasing complexity of the operational environment. Modern systems enable the real-time monitoring of resources, the anticipation of logistical requirements, and rapid adaptation to changes on the battlefield.

Studies in the field show that the digitalization of logistics contributes to increased operational efficiency by reducing uncertainty and optimizing resource distribution. Supply chains become more transparent and flexible, enabling the sustainment of operations in contested or unstable environments.

This transformation changes the role of logistics, which is no longer merely a support function but a strategic element capable of directly influencing operational

outcomes. The ability to ensure continuity of supply and manage disruptions becomes an essential factor of military success.

5.3. Interoperability and the Modernization of Allied Forces

Interoperability represents a fundamental condition for the effective functioning of contemporary military alliances. The technological compatibility of systems, the harmonization of doctrines, and the standardization of procedures enable the conduct of joint operations and reduce operational friction.

Specialized literature highlights that interoperability is not limited to technical aspects, but also includes organizational and cultural dimensions. Multinational exercises and information sharing contribute to strengthening collective response capabilities and increasing operational cohesion.

The modernization of allied forces is closely linked to the integration of emerging technologies and the development of common command-and-control systems. This evolution strengthens the ability of alliances to respond rapidly and effectively to contemporary threats.

5.4. The Role of Emerging Technologies in the Transformation of Military Mindset

Emerging technologies influence not only the technical capabilities of armed forces but also the manner in which military thinking is conceived. The integration of artificial intelligence and autonomous systems drives the transition from linear planning to adaptive decision-making processes based on the continuous analysis of data.

Recent studies highlight that this transformation involves a redefinition of the role of the human factor, which must manage interaction with automated systems and understand their limitations (Johnson 2019, 1417-1418). Military decision-making becomes the result of collaboration between humans and technology, raising challenges related to responsibility and control.

This evolution requires the development of an organizational culture oriented toward innovation, continuous learning, and adaptability. Armed forces capable of integrating these technologies into flexible structures may obtain significant advantages in a strategic environment characterized by uncertainty and persistent competition.

The analysis suggests that the future of global conflicts will be dominated by persistent forms of multidomain competition, in which information, cyber, and economic instruments will become as relevant as the direct use of military force. This trend indicates the emergence of a conflict model characterized by permanent strategic competition and the simultaneous integration of pressure across multiple operational domains.

6. Perspectives on the Future of Global Conflicts

The evolution of global conflicts indicates a structural transformation in the way strategic competition is conducted, marking a transition from high-intensity

conventional confrontations toward persistent forms of multidimensional competition. Economic interdependence, accelerated digitalization, and the development of emerging technologies contribute to shaping a security environment in which strategic pressure can be exercised continuously without crossing the threshold of open armed conflict (Mazarr 2015, 3-7; NATO 2022, 5-7).

This evolution reflects a change in the logic of conflict, in which the gradual accumulation of effects on infrastructures, perceptions, and decision-making processes becomes more relevant than achieving decisive victories on the battlefield. Recent studies emphasize that state actors increasingly prefer the use of indirect instruments capable of generating strategic advantages without direct military escalation (Jensen, Valeriano, and Maness 2019, 212–214).

A central element of future conflicts is the deep integration of the cyber dimension into geopolitical strategies. Cyberspace offers opportunities for conducting influence operations, sabotage, and intelligence gathering, all characterized by difficulties of attribution and low operational costs. This reality encourages the development of strategies based on continuous pressure, in which cyber, information, and economic instruments are used in an integrated manner to alter the balance of power.

At the operational level, future conflicts will be characterized by the acceleration of the decision-making cycle and the integration of autonomous systems into combat processes. The ability to rapidly correlate information from multiple sources and generate coordinated effects across several domains becomes a determining factor of military effectiveness. Specialized literature highlights that superiority is no longer associated exclusively with the mass of forces, but with the capacity to integrate technology, information, and organizational structures into a coherent system (Manolache 2023, 168-170).

Another defining element is the growing role of non-state actors and asymmetric conflicts. These actors are capable of exploiting infrastructure and information vulnerabilities of states, generating strategic effects without possessing comparable conventional military capabilities. This trend contributes to the complexity of the security environment and to the difficulty of conflict management.

In the long term, international stability will depend on the ability of actors to manage the balance between technological innovation and regulatory mechanisms. The accelerated development of artificial intelligence, autonomous systems, and cyber capabilities raises issues related to control, responsibility, and predictability. The absence of clear normative frameworks may amplify risks and increase systemic instability.

The future of global conflicts will be defined by persistent competition, in which the distinction between peace and war becomes increasingly difficult to delineate. The ability of states to integrate technology, develop resilience, and manage the complexity of the security environment will represent a decisive factor in maintaining strategic advantage.

Conclusions

The analysis confirms that contemporary warfare has undergone a structural transformation, evolving from the paradigm of conventional confrontations toward a multidimensional model in which the cyber, informational, economic, and space domains acquire an importance comparable to the traditional military dimension. This evolution supports the hypothesis that the nature of conflict in the 21st century is defined by interdependence, ambiguity, and persistent competition below the threshold of direct confrontation.

The examination of the role of emerging technologies highlights that digitalization, artificial intelligence, and autonomous systems represent not merely instruments of operational efficiency, but factors that reconfigure power relations and the conduct of conflicts. The ability to integrate and exploit information becomes a central determining element of strategic advantage, confirming the hypothesis regarding the transformation of the criteria of military superiority.

The analyzed examples, such as the Russo-Ukrainian War, the use of drones in the Nagorno-Karabakh conflict, and cyber operations against critical infrastructures, demonstrate that strategic advantage is increasingly determined by the capacity for multidomain integration and the rapid exploitation of information.

The cyber and information dimensions demonstrate that the disruption of critical infrastructures and the exploitation of digital vulnerabilities enable the exercise of continuous strategic pressure without direct military escalation.

From a methodological perspective, the use of a qualitative, analytical, and conceptual approach, based on the analysis of specialized literature and the comparison between traditional and contemporary forms of conflict, made it possible to identify coherent trends and causal relationships among technology, strategy, and the transformation of the military paradigm. This approach provides a relevant interpretative framework for understanding the evolution of conflicts in the 21st century.

The theoretical contribution of the paper consists of integrating the concepts of hybrid warfare, multidomain operations, and gray-zone competition into a unified interpretative model of contemporary conflict. The analysis supports the idea that modern warfare is evolving toward a persistent form of multidimensional strategic competition, in which the distinction between peace and conflict becomes increasingly difficult to establish.

The analysis also emphasizes that strategic advantage is no longer determined exclusively by material resources, but by the capacity to integrate technology, information, and decision-making processes into a coherent and adaptable system. This conclusion has direct implications for the manner in which states shape their defense strategies and develop their military capabilities.

The paper provides an analytical perspective on the transformation of contemporary warfare and contributes to clarifying the relationship between technology, strategy,

and security, highlighting the main directions of evolution of global conflicts.

Based on the analysis conducted, the paper proposes the interpretation of contemporary warfare through the concept of "persistent multidimensional conflict," defined as a form of strategic competition conducted simultaneously across the military, cyber, information, economic, and space domains, characterized by continuity, strategic ambiguity, and technological integration. Unlike the classical paradigm of conventional confrontation, this model highlights that strategic advantage is determined primarily by the ability of actors to integrate information, technology, and simultaneously applied pressure across multiple domains into a coherent mechanism of influence and operational adaptation.

However, the present research has certain limitations generated by its predominantly conceptual character and the absence of quantitative empirical analyses or in-depth case studies. Although the adopted approach enables the identification of major trends and the formulation of relevant conclusions, the integration of empirical data could strengthen the validity of the results.

Future research could focus on the comparative analysis of recent conflicts, the use of mixed methods (qualitative and quantitative), and the evaluation of the impact of emerging technologies on different categories of actors. Furthermore, exploring the relationship between artificial intelligence, decision-making autonomy, and strategic stability represents a relevant direction for the further development of the field.

References

- Biddle, Stephen.** 2022. "Back in the Trenches: Why Attrition Still Dominates the Battlefield." *International Security* 46(4): 32-35. <https://direct.mit.edu/isec/article/46/4/7/109111/Back-in-the-Trenches-Why-Attrition-Still>.
- Boyle, Michael J.** 2015. "The Legal and Ethical Implications of Drone Warfare." *International Journal of Human Rights* 19(2): 4. <https://doi.org/10.1080/13642987.2014.991210>.
- Freedman, Lawrence.** 2017. *The Future of War: A History*. New York: Public Affairs.
- Hoffman, Frank G.** 2018. "Examining Complex Forms of Conflict: Gray Zone and Hybrid Warfare." *PRISM* 7(4): 30-47. <https://ndupress.ndu.edu/Media/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/>.
- Horowitz, Michael C.** 2010. *The Diffusion of Military Power: Causes and Consequences for International Politics*. Princeton, NJ: Princeton University Press.
- International Institute for Strategic Studies (IISS).** 2024. "The Military Balance 2024." *The Military Balance* 124(1): 15-16. London: Routledge. <https://doi.org/10.4324/9781003485834>.
- Jensen, Benjamin M., Brandon Valeriano, and Ryan C. Maness.** 2019. "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist." *Journal of Strategic Studies* 42(2): 212-219. <https://doi.org/10.1080/01402390.2018.1559152>.

- Johnson, James.** 2019. "Artificial Intelligence & Future Warfare: Implications for International Security." *International Affairs* 95(6): 1397-1418. <https://doi.org/10.1093/ia/iiz125>.
- Manolache, Ionela Cătălina.** 2023. "The Role of Multi-Domain Operations in Modern Warfare." *Land Forces Academy Review* 28(3): 163-170. <https://doi.org/10.2478/raft-2023-0020>.
- Kello, Lucas.** 2013. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38(2): 7-21. https://doi.org/10.1162/ISEC_a_00138.
- Konaev, Margarita.** 2023. *The Future of Conflict: Autonomous Systems and Artificial Intelligence*. Washington, DC: Center for Security and Emerging Technology (CSET).
- Mazarr, Michael J.** 2015. *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. Santa Monica, CA: RAND Corporation. <https://doi.org/10.7249/RR1003>.
- NATO.** 2022. *NATO Strategic Concept*. Brussels: North Atlantic Treaty Organization. <https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf>.
- Payne, Kenneth.** 2021. *I, Warbot: The Dawn of Artificially Intelligent Conflict*. London: Hurst Publishers.
- Salehyan, Idean.** 2009. *Rebels without Borders: Transnational Insurgencies in World Politics*. Ithaca, NY: Cornell University Press. <https://www.degruyterbrill.com/document/doi/10.7591/9780801459214/html>.
- Scharre, Paul.** 2018. *Army of None: Autonomous Weapons and the Future of War*. New York: W. W. Norton & Company.
- Schmitt, Michael N.** 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. <https://doi.org/10.1017/9781316822524>.
- U.S. Department of Defense.** 2022. *Joint All-Domain Command and Control (JADC2) Strategy*. Washington, DC: U.S. Department of Defense. <https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf>.
- Watling, Jack.** 2023. *The War in Ukraine and the Evolution of Modern Warfare*. London: Royal United Services Institute (RUSI).

The Determinants of Military Combat Capacity Longevity: between Physical Specialization, Training Volume, and Recovery

Dumitru Cătălin COHAL, PhD*

*"Nicolae Bălcescu" Land Forces Academy, Sibiu

e-mail: Cohalcatalin@gmail.com

Abstract

Maintaining an optimal level of military physical readiness constitutes a strategic objective for the military organization, having a direct impact on operational efficiency and the longevity of the soldier's combat capacity. Despite accelerated technological progress, the human factor remains the determinant of success in military actions; the adoption of a healthy lifestyle results from the complex interaction of biological, psychological, and social factors. In the initial stages of a military career, the goal is to achieve a high level of physical readiness early on, coupled with its continuous preservation and optimization. Contemporary approaches promote a holistic, salutogenic vision of military physical training, grounded in the integration of physical, mental, nutritional, spiritual, and recovery components. This research is based on a theoretical analysis of specialized literature that highlights the importance of the balance between specialization, training volume, and recovery strategies. It emphasizes the role of parameters such as BMI (Body Mass Index), HRV (Heart Rate Variability), and sleep quality in preventing injuries and sustaining career continuity. Further applied studies are necessary to validate these perspectives within the current Romanian military context.

Keywords:

Military Physical Education; Longevity; Operational Efficiency; Salutogenesis; Holistic.

Article info

Received: 4 March 2026; Revised: 4 April 2026; Accepted: 27 April 2026; Available online: 30 June 2026

Citation: Cohal, D.C. 2026. "The Determinants of Military Combat Capacity Longevity: between Physical Specialization, Training Volume, and Recovery." *Bulletin of "Carol I" National Defence University*, 15(2): 273-284. <https://doi.org/10.53477/2284-9378-26-28>



© „Carol I” National Defence University Publishing House

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution ([CC BY-NC-SA](https://creativecommons.org/licenses/by-nc-sa/4.0/))

Introduction

Achieving and establishing an optimal level of a soldier's combat capacity represents a fundamental objective in the periodization of activities carried out within the military organization. A soldier's combat capacity is grounded in specialized military knowledge and the attainment of an adequate level of moral and physical readiness, as well as their continuous preservation and improvement. Regardless of the level of technological development characterizing the contemporary military space, the human factor remains the central element of all operational actions. While maintaining an optimal level of military readiness depends on several aspects, the soldier's physical and mental health status plays a decisive role in achieving the proposed goals.

From a salutogenic perspective on the approach to physical education, three main components define the Sense of Coherence (SOC): comprehensibility, manageability, and meaningfulness ([Antonovsky 1987](#), 15-19). These constitute relevant theoretical benchmarks for the foundation and optimization of educational interventions applicable to the field of military physical education, aiming for the sustainable preparation of personnel and the maintenance of an optimal state of health. Understanding the world we live in, resource management, and the significance of one's own actions provide the soldier with a solid foundation for adequate operational readiness. Acquiring awareness of the importance of maintaining a healthy lifestyle is the result of a complex interaction between biological, psychological, and social factors ([Guo et al., 2021](#)).

In designing the initial trajectory of an excellent military career, the goal is the early attainment of a high level of combat capacity. This level plays an essential role both in the efficient fulfillment of intended combat missions and in the role of a citizen adapted to society, involved and devoted to moral values. New approaches to the development of individual combat capacity promote a holistic, salutogenic-oriented vision of physical training, based on five core pillars centered on the soldier's physical and mental health. Their operational efficiency is determined by:

1. Physical readiness;
2. Mental readiness;
3. Nutritional readiness;
4. Spiritual readiness;
5. Recovery strategies.

The present study represents a theoretical analysis of specialized literature with applicability to the modern military environment in Romania. Critical analysis of literature sources suggests that early specialization and the attainment of high levels of military physical performance are desirable; however, these must be correlated with other essential factors of integrative preparation. In the absence of this balanced approach, the risk of physical injuries, psychological disorders, and even

the abandonment of the military career increases significantly, thereby affecting the longevity of the military career with direct implications for the social sphere.

Maintaining adequate parameters regarding Body Mass Index (BMI), recovery – specifically Heart Rate Variability (HRV) and sleep quality – and the correct identification and interpretation of stress factors, alongside a low history of injuries, have been identified in the literature as protective factors associated with the continuity and efficiency of military activity. In the long term, the cumulative effect of these practices is reflected in the development of an organizational culture where physical and mental preparation, at both individual and group levels, is not imposed, but embraced ([Fullagar et al., 2015](#)).

Therefore, the longevity of a soldier's combat capacity depends on an optimal balance between the timing of specialization, training volume and intensity, and effective recovery strategies. This critical investigation of the specialized literature represents a first step toward shifting the organizational vision regarding physical training conducted in an organized and scientific manner. The research necessitates further completion through applied studies conducted on extensive samples of military personnel at various stages of their careers. The pragmatic goal of this research is to present to specialists in the field the necessity of a holistic approach to military physical training – grounded in salutogenic information – by demonstrating the long-term effects of this approach on increasing personal resilience in relation to probable life events and by fostering an awareness of the origins of health.

I. Military Physical Specialization

Individual combat capacity is linked to the soldier's level of specialized training and technical equipment, but also to their physical, mental, nutritional, spiritual, and recovery preparation. Together, these allow the soldier to dominate the adversary in combat. More simply put, they provide the soldier with lethal qualities in relation to the enemy. Military physical training represents a fundamental component of military instruction, playing a direct and decisive role in the operational efficiency of personnel. Military physical training not only ensures the physical capacity to fulfill combat tasks; it also contributes to mental endurance, injury prevention, and team cohesion. Physical training allows the soldier to fulfill assigned missions, survive on the battlefield, and effectively utilize their weaponry and equipment, but only in close connection with the other aspects that consolidate sustained combat capacity. Therefore, physical training is an integrated part of the soldier's individual combat capacity, which is defined as a lethal physical and mental system that offers the soldier the possibility of battlefield supremacy and a healthy return home ([Adler et al., 2009](#)). With these values at the center, the goal is to maintain a high level of health among military personnel. Without systemic issues related to troop or individual health, combat preparations can proceed according to developed plans. Over time, by forming an organizational culture in this regard, one can speak pragmatically

about the longevity of the military career. This approach directly results in a series of positive effects worth addressing to raise awareness of operational efficiency.

Effects of Military Physical Training on a Soldier's Operational Efficiency:

- a) Efficiency: Soldiers in good physical condition learn combat actions approximately 20% faster and execute them with greater skill. Physical training allows them to cope with intense physical and psychological demands, such as carrying heavy loads, moving quickly over rough terrain, overcoming natural obstacles, and maintaining vigilance without compromising their health.
- b) Endurance and Resilience: Military physical training develops physiological and psychomotor capacities essential for survival and success under conditions of stress, chronic fatigue, and hostile environments.
- c) Injury Prevention: Through well-structured training, the soldier learns elements of the physiology of the musculoskeletal system, recovery, and nutrition, reducing the risk of injuries or imbalances within the body during missions.
- d) Increased Precision and Confidence: Physical training improves shooting accuracy and the ability to maintain vigilance and precision despite physical exertion.
- e) Developing a Warrior Spirit: Rigorous physical training not only affects the muscular system but also shapes a warrior mindset, increasing self-confidence, self-discipline, and group cohesion.
- f) Adaptability: The physical training process is adapted to the modern requirements of the battlefield, ensuring that soldiers are prepared for various climatic and terrain conditions (Nindl et al., 2013).

1.1. Early Physical Specialization in the Military Career

The first steps in a military career involve going through the stages of recruitment, selection, admission, and initial professional training. During the selection stage, the motor skills of the candidates are tested, among other attributes. Starting from the premise that those selected are motor-fit to carry out physical and psychological activities specific to the military environment, it is self-evident that physical specialization begins from a certain level of performance rather than from zero (Lai et al., 2026). Depending on each candidate's aspirations and their physical and mental performance, they follow an initial stage of professional training after the admission exam, aimed at achieving specialization within a well-established timeframe in a specific area of interest, both for the military system and, especially, for the respective candidate.

From the perspective of physical specialization, the goal is to develop those motor skills that grant the soldier the ability to execute assigned missions successfully and without adverse effects on their health. To this end, the design of a soldier's physical training must adhere to a series of basic rules and principles constructed in such

a way that the longevity of their career does not suffer. Early attainment of a high level of military physical readiness is supported by solid theoretical arguments that emphasize operational performance, injury prevention, and the development of resilience. This, therefore, represents a strategic necessity of the military system, not just a physical training requirement per se (Vaara et al., 2022).

1.2. Theoretical Arguments for Early Achievement of a High Level of Readiness

Early physical preparation aims to rapidly transform the soldier into a secure, efficient, and long-lasting operational resource. Achieving this goal must not overlook the fact that at the heart of the military system stands the human being – a complex entity, not a simple robot to be programmed, with multiple needs and individual aspirations. The primary objective for military physical training specialists is to minimize the time allocated to meeting the performance criteria necessary for successful mission execution while simultaneously reducing injuries and accounting for the attrition rate (dropout).

Key Theoretical Arguments:

- a) Optimization of Physiological Adaptations and Reduction of Injury Risk: Early preparation allows the body to gradually adapt to intense strength and endurance loads, lowering the risk of stress fractures and musculoskeletal injuries during basic training. Soldiers who reach a high level of physical readiness before joining combat units are less prone to attrition.
- b) Increased Physical and Mental Resilience (Mental Toughness): Achieving a high level of physical readiness is closely linked to the ability to cope with stress, fatigue, and uncertainty in combat conditions. Early training builds a solid foundation of resilience, helping to maintain focus and discipline under pressure. Military physical training provides the soldier with the capability to be lethal against the enemy and return home healthy.
- c) Increased Prompt Operational Capacity: The immediate physical availability of soldiers is crucial for the military organization. The fact that a soldier is prepared 24/7 to execute assigned missions provides the system with adequate operational capacity.
- d) Development of Lifestyle and Functional Military Habits: Attaining a high level of physical readiness facilitates the creation of new neural pathways and healthy habits, such as proper nutrition and the correct ratio between training and rest, which are necessary to maintain performance over the long term.
- e) Effectiveness of Specialized Training: A soldier can more rapidly assimilate specific technical and tactical skills when they possess a sustained level of physical training, compared to a soldier who must build a physical foundation in parallel with learning techniques (Knapik et al., 2006).

1.3 Risks Associated with Excessive Physical Specialization for Soldiers

Although specialization is necessary to master advanced technologies, a balanced army requires a combination of technical experts (specialists in specific fields or

combat arms) and leaders capable of understanding the big picture (generalists) to face hybrid and unpredictable threats. Physical specialization aims to develop a physically complete soldier, rather than merely focusing on the particular development of specific motor qualities or skills of temporary interest. Excessive physical specialization (hyper-specialization) within the armed forces, while potentially increasing efficiency in a narrow domain, presents significant strategic, operational, and personal risks. In an unpredictable security environment characterized by hybrid threats and rapid technological changes, a narrow approach can become a weakness. Therefore, the goal is for physical training to adopt a salutogenic direction over time, centering on the individual's awareness that, above all, maintaining health, avoiding injury, and preserving a balanced lifestyle can lead to increased longevity in a successful career. The primary risk of physical hyper-specialization is related to plateauing and obsolescence. When the expertise acquired by a soldier is no longer current or relevant, they often exhibit general apathy toward retraining or discovering new values. Furthermore, excessive physical wear and tear can lead to a repulsion toward continuing even basic physical training. Consequently, physical preparation is intended to be vectorial – adapted to the new challenges of the modern battlefield, continuous, and conscious. Conducting physical training in an organized manner under the guidance of specialists can prevent the risks and side effects of excessive physical training ([Southwick and Charney 2012](#)).

II. Methodology

The present study is based on a theoretical-conceptual research design with exploratory and applied dimensions, aimed at establishing an integrative model for optimizing the longevity of a soldier's combat capacity. The methodological framework integrates a systematic literature review in the fields of motor sciences, exercise physiology, military psychology, and military physical education; a documentary analysis of military regulations defining physical training concepts; and structured conceptual modeling. The objective was to theoretically clarify the relationship between military physical specialization and the sustainability of operational performance. Information regarding the impact of training volume and intensity on maintaining long-term combat capacity was analyzed, alongside the role of systematic recovery in preventing functional wear and performance decline ([Zatsiorsky and Kraemer 2006](#)).

Information and documentation sources were selected based on:

- a) Relevance to the field of military physical education and exercise physiology;
- b) Scientific impact (peer-reviewed publications, official normative documents);
- c) Conceptual contribution to understanding the relationship between training volume, motor specialization, and biological adaptation;
- d) Applicability within structured institutional contexts.

The conceptual analysis procedure aimed to determine the degree of normative compatibility between the principles of functional sustainability and the current

training structure. The conceptual analysis was carried out through a structured four-stage procedure:

- I. Identification of theoretical constructs;
- II. Thematic categorization;
- III. Analysis of information sources;
- IV. Presentation of the theoretical model.

The analysis of the military normative framework took into account educational and instructional regulations, which were addressed through a structured content analysis focused on the following key benchmarks: military physical education objectives and performance standards, training planning structure, provisions regarding injury prevention and recovery, and flexibility in adapting to individual characteristics. The methodological result of the study provides a conceptual framework for implementing physical training programs designed to optimize combat capacity longevity by balancing the relationship between physical specialization and training volume, and planned recovery and prevention of operational wear. Given its exploratory and conceptual nature, the study does not include empirical validation. Further quantitative research is required to evaluate measurable effects on operational performance and the duration of maintaining combat capacity throughout a military career, viewed through the lens of holistic military physical training.

III. Training Volume in the Military Environment

Unlike the civilian environment, where physical training is predominantly oriented toward achieving competitive performance, military physical training – specifically the dosage of training amount and intensity – aims to develop general and specific functional capacity. This is designed to fulfill missions under conditions of high physical and psychological stress (Cohal 2025). Depending on the specifics of each branch and specialization, military physical training is based on three major directions of implementation: precision, progressivity, and operational integration.

3.1. Precision of Execution and the Kinesthetic Dimension

The precision of execution represents the foundation of military physical readiness. From a neurophysiological perspective, this involves the development of kinesthetic capacity – that is, the soldier's ability to perceive the position of body segments, the amplitude of movements, and the ratio between muscle tension and relaxation. Through the controlled repetition of exercises, the soldier develops stable motor patterns which, through synaptic consolidation, transform into functionalisms (Chen et al., 2025).

These functionalisms are essential in operational situations where reaction time and correctness of execution can have direct implications for individual and collective security. Exercise complexes are designed to optimize the motor parameters

required for each specialization (e.g., endurance and explosive strength for infantry, coordination and balance for special forces, etc.). Thus, precision is not just a biomechanical objective, but a vector of tactical efficiency.

3.2. Progressivity

The progressive nature of military training involves applying classic principles of periodization, adapted, however, to institutional and operational realities. Periodization can be structured into:

- A. Annual Macro-cycles: Correlated with mission planning and physical evaluations;
- B. Meso-cycles (4–8 weeks): Oriented toward the development of a dominant motor quality;
- C. Weekly Micro-cycles: Featuring alternation between volume and intensity loads.

The principle of supercompensation is essential in this logic. The relationship between training load and functional adaptation can be explained through the classic supercompensation model. Following a phase of temporary decrease in functional capacity (fatigue), there is always a phase of increase above the initial level, provided that recovery is adequate.

Incorrect application of this principle can lead to either stagnation or chronic overtraining. In the Romanian military environment, the major challenge lies in harmonizing the scientific periodization of training volume with the requirements of the operational schedule, which can disrupt optimal adaptation cycles. Simply put, training continuity in the military environment must always be weighed against operational demands.

3.3. Operational Integration

The amount of training (total duration, number of repetitions, distance covered, etc.) and intensity (relative to individual maximum capacity) must be calibrated according to functional objectives. Intense physical effort must be adapted within the operational context and must align with the primary objective of the organization. This conceptual representation indicates the existence of a functional optimum, which is essential in the military environment. Here, the goal is not a singular maximal performance, but rather the maintenance of constant, long-term operational capacity and the quality of health status ([Kyröläinen et al., 2008](#)).

Military functional performance must be evaluated through multiple indicators:

- 1. VO₂max and aerobic endurance;
- 2. Relative strength and anaerobic capacity;
- 3. Postural stability and coordination;
- 4. Psychophysical resilience.

Therefore, individual awareness regarding the “origins of health” and the importance of maintaining it – alongside the implementation of modern monitoring systems

(HRV, lactate assessment, subjective scales of perceived exertion – RPE) – could optimize the ratio between volume, intensity, and recovery.

IV. Physical Recovery

In the architecture of military physical training, recovery should not necessarily be understood as a mere break between two cycles of exertion, but rather as a strategic component of maintaining combat capacity. In an operational context, optimal combat capacity is not a one-time objective, but a functional state that must be preserved over the long term under conditions of repeated demand, psychological stress, and tactical unpredictability. Viewed this way, the recovery process acquires significant value and must be seen as an integral part of the general military physical training process ([Deuster and Silverman 2013](#)).

4.1. The Importance of Recovery in Maintaining Combat Capacity

Physical recovery allows the soldier to maintain control over their own body and offers the possibility of extending their active operational status and, above all, their health. Physical recovery plays a decisive role in maintaining a high level of combat capacity, which represents a multidimensional construct including physical, cognitive, and psychological parameters. From a physiological perspective, the relationship between load and functional capacity can be conceptualized as an adaptation process dependent on the balance between stress and recovery ([Feigel et al., 2026](#)). If the demand constantly exceeds the capacity for restoration, a progressive decline in performance occurs. In the absence of adequate recovery, the progressive degradation of physiological resources leads, in the short and medium term, to:

1. Diminished strength and endurance;
2. Increased reaction time;
3. Impaired decision-making clarity;
4. Increased vulnerability to injuries.

For the military environment, this decrease in physiological resources not only affects the individual soldier or a group of soldiers at a specific point in time but also the entire organizational structure. Consequently, recovery becomes an operational security factor that deserves to be treated with great responsibility by commanders and acknowledged by all military personnel. In support of this goal, specialized training for commanders regarding military physical education, as well as the knowledge and utilization of specialized technology in the field, can be determining factors in supporting the maintenance of an optimal level of operational readiness.

4.2. Physiological Indicators of Recovery

The implementation of a modern recovery monitoring system within military structures could contribute to optimizing training and reducing injuries. Traditional military culture, predominantly oriented toward discomfort tolerance, can have an inhibiting effect that leads to the false reporting of fatigue. Therefore, it is necessary to develop an organizational culture that differentiates physical effort between

resilience and harmful overloading. Relevant indicators include:

- a) Heart Rate Variability (HRV)
 - a. HRV reflects the balance between the sympathetic and parasympathetic nervous systems. Increased variability indicates a good capacity for adaptation and recovery, while a persistent decrease may signal accumulated fatigue or chronic stress.
 - b. In the military environment, HRV monitoring could provide an objective tool for adjusting training volume and intensity, especially during periods of intense instruction or preceding external missions.
- b) Sleep Quality and Duration Sleep is essential for:
 - a. Muscle recovery processes;
 - b. Cognitive functions;
 - c. Hormonal regulation (cortisol, testosterone);
 - d. The immune system.
- c) Accumulated Fatigue and Subjective Perception of Effort. These can be analyzed using RPE (Rating of Perceived Exertion) scales and wellness questionnaires, which can complement the objective data of the recovery monitoring system (Plews et al., 2013).

4.3. Modern Injury Prevention Strategies

Musculoskeletal injuries represent one of the primary causes of temporary unavailability within military structures. Their prevention must be systemic and multidimensional. Even though the military environment operates on the principle of uniformity, adapting training to individual anthropometric and functional characteristics can significantly reduce the risk of injury. Periodic testing (strength, mobility, stability) allows, to a certain extent, for the adjustment of physical training programs. A modern and proven alternative is the integrative neuromuscular training method (Chen et al., 2025). This is generally based on stabilization, proprioception, and motor control exercises designed to reduce the incidence of ligament and muscle injuries. Integrating these into a daily routine (10–15 minutes) can have a disproportionately large impact on a soldier's long-term health.

Furthermore, managing cumulative load by respecting the acute-to-chronic workload ratio reduces the risk of injuries. The salutogenic approach to military physical education and physical training can also contribute significantly to injury prevention. Over time, the soldier comes to realize that the origin of health does not lie in treating diseases or accidents, but in the way they perceive their health through the regular performance of scientific physical exercise.

Health level is not exclusively a medical issue, but also a matter of leadership. Commanders must understand the relationship between recovery, performance, and operational efficiency. In this regard, their personal example concerning physical training offers subordinates, in addition to the specialized information conveyed, courage, confidence, and the desire to fulfill their assigned missions. A culture of prevention, as part of physical training, indirectly contributes to reducing the logistical and medical costs within the system.

Conclusions

The longevity of a soldier's combat capacity is not the result of maximum training intensity, but rather of an intelligent balance between demand and recovery, between specialization and adaptability, and between performance and health. The proposed model focuses on the origins of the soldier's health status and supports the transition from an organizational culture based on sustained, permanent maximal effort to a culture of sustainable performance, scientifically grounded and salutogenically oriented.

Regarding early specialization, studies show that while it is effective in the short term, an excessively narrow focus can lead to plateaus, functional obsolescence, and a decrease in motivation. A vectorial, adaptive, and continuous approach is more suitable for the contemporary security environment. Last but not least, it must be concluded that leadership plays a determinant role in implementing a sustainable physical training model for the military system.

References

- Antonovsky, A.** 1987. *Unraveling the Mystery of Health: How People Manage Stress and Stay Well*. San Francisco: Jossey-Bass.
- Adler, A.B., P.D. Bliese, D. McGurk, C.W. Hoge, and C.A. Castro.** 2009. "Battlemind training: Building soldier resilience". *Military Medicine* 174(1): 45–50.
- Chen, B., L. Deng, Y. Liu, X. Deng, and X. Yuan.** 2025. "The Effect of Integrative Neuromuscular Training on Enhancing Athletic Performance: A Systematic Review and Meta-Analysis". *Life* 15(8): 1183. <https://doi.org/10.3390/life15081183>.
- Cohal, D.** 2025. "Effective Methods for Optimizing Effort Capacity in the Military Pentathlon". *Balneo and PRM Research Journal* 16(3): 860. <https://doi.org/10.12680/balneo.2025.860>.
- Department of the Army.** 2020. *FM 7-22 Holistic Health and Fitness (H2F)*. Washington, DC.
- Deuster, P.A., and M.N. Silverman.** 2013. "Physical fitness and resilience in military personnel". *Journal of Strength and Conditioning Research* 27(4): 1164–1175.
- Feigel, E.D., A. McCarthy, J.T. Fuller, L. Rosenblum, M. Lovalekar, T. Ojanen, K. Pihlainen, B.J. Martin, K.J. Koltun, T.L.A. Doyle, and B.C. Nindl.** 2026. "Nonlinear analysis reveals duration and gradient-dependent disruption of load carriage gait variability during an outdoor 6.72 km time trial in military personnel". *Applied Ergonomics* 130: 104639. <https://doi.org/10.1016/j.apergo.2025.104639>.
- Fullagar, H.H.K., S. Skorski, R. Duffield, D. Hammes, A.J. Coutts, and T. Meyer.** 2015. "Sleep and athletic performance". *Sports Medicine* 45(2): 161–186. <https://doi.org/10.1007/s40279-014-0260-0>.
- Guo, R., M. Sun, C. Zhang, Z. Fan, Z. Liu, and H. Tao.** 2021. "The role of military training in improving psychological resilience and reducing depression among college

freshmen.” *Frontiers in Psychiatry* 12: 641396. <https://www.frontiersin.org/journals/psychiatry/articles/10.3389/fpsyt.2021.641396/full>.

Knapik, J.J., B.H. Jones, S.W. Bullock, M. Canham-Chervak, and S. Canada. 2006. “Injury rates and injury risk factors among U.S. Army soldiers”. *American Journal of Preventive Medicine* 30(4): 350–356.

Kyröläinen, H., J. Karinkanta, M. Santtila, H. Koski, M. Mäntysaari, and T. Pullinen. 2008. “Effects of military training on physical performance and hormonal responses”. *European Journal of Applied Physiology* 102 (5): 541–551.

Lai, S., Z. Wang, X. Gao, J. Sun, Z. Yang, Z. Kang, Y. Xu, and H. Liu. 2026. “Military training efficacy on physical fitness and mental health in college students”. *WORK: A Journal of Prevention, Assessment & Rehabilitation*. <https://doi.org/10.1177/10519815251409137>.

Nindl, B.C., S.J. Sharp, W.J. Kraemer, J.J. Marx, M.D. Stephenson, and J.S. Volek. 2013. “Operational physical performance and readiness”. *Journal of Strength and Conditioning Research* 27(4): 1164–1175.

Plews, D.J., P.B. Laursen, A.E. Kilding, and M. Buchheit. 2013. “Heart rate variability and training intensity distribution in elite endurance athletes”. *European Journal of Applied Physiology* 113: 3061–3070.

Southwick, S.M., and D.S. Charney. 2012. *Resilience: The Science of Mastering Life’s Greatest Challenges*. Cambridge University Press.

Vaara, J.P., H. Groeller, J. Drain, H. Kyröläinen, K. Pihlainen, T. Ojanen, C. Connaboy, M. Santtila, P. Agostinelli, and B.C. Nindl. 2022. “Physical training considerations for optimizing performance in essential military tasks”. *European Journal of Sport Science* 22:43-57. <https://doi.org/10.1080/17461391.2021.1930193>.

Zatsiorsky, V.M., and W. Kraemer. 2006. *Science and Practice of Strength Training*. Human Kinetics.

Hybrid Crisis Management: An Integrated Response to Contemporary Asymmetric Threats

Cristiana Maria ALMAŞAN, PhD Candidate*

*Bucharest University of Economic Studies, Romania

e-mail: cristianaa.almasan@gmail.com

 <https://orcid.org/0009-0009-6789-9149>

Abstract

This article examines the transformation of hybrid conflict over the period 2007-2024 and its impact on the resilience of states within the Euro-Atlantic area, with an emphasis on the interaction among the cyber, information, economic, and legal-political dimensions. Methodologically, the study employs a comparative case-study approach, to highlight variations in vulnerability and institutional responses to hybrid threats. The analysis integrates a resilience-cycle framework, correlated with a multidimensional operational taxonomy. The results indicate a structural mutation of hybrid conflict, in which information and cyber instruments become central to the production of strategic effects. The study also highlights the consolidation of internal mobilisation and offensive legal actions (lawfare) as distinct vectors of hybrid power that are insufficiently integrated into existing theoretical and normative frameworks. The principal conclusion shows that institutional and societal resilience constitutes the essential condition of contemporary deterrence, being determined by the coherence of the normative framework, operational capacity, and the level of investment in cyber and information security. The study proposes an integrated analytical framework for the assessment and management of hybrid threats, with relevance for national and Euro-Atlantic security policies.

Keywords:

Hybrid Conflict; Institutional Resilience; Cybersecurity; Disinformation; Information Warfare; Generative Artificial Intelligence; Euro-Atlantic Security; Prevention; NATO; the European Union.

Article info

Received: 4 April 2026; Revised: 30 April 2026; Accepted: 3 June 2026; Available online: 30 June 2026

Citation: Almaşan, C.M. 2026. "Hybrid Crisis Management: An Integrated Response to Contemporary Asymmetric Threats"
Bulletin of "Carol I" National Defence University 15(2): 285-310. <https://doi.org/10.53477/2284-9378-26-29>



© „Carol I” National Defence University Publishing House

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC-SA)

Introduction

The evolution of the international security environment over the past decade reveals a structural change in the nature of conflict: conventional military means are increasingly replaced or complemented by instruments that operate below the legal threshold of armed conflict, targeting the political, economic, social, and information vulnerabilities of the adversary state. These actions, known in the specialised literature as hybrid conflict, are not a new reality but rather an extension of historic practices of subversion, today amplified by technological advances, by generative artificial intelligence, and by the high degree of interconnection of modern societies ([Hoffman 2007](#); [Renz 2016](#); [Cullen and Reichborn-Kjennerud 2017](#)).

What renders this theme acutely topical is the unprecedented simultaneous overlap of hybrid threats of different kinds within the same geographical area and the same temporal interval. The large-scale Russian invasion of Ukraine, launched in February 2022 and ongoing at the time of writing, demonstrated that hybrid and conventional actions are not mutually exclusive but can combine synergistically. In parallel, disinformation campaigns amplified by artificial intelligence, cyber actions directed against NATO critical infrastructure, and proven electoral interference in several member states, including Romania (2024), have shown that no country is sheltered from such aggressions ([ENISA 2024](#); [CCDCOE 2024](#); [SRI 2023](#)).

A methodological clarification is required regarding the analytical framework adopted. The specialised literature operates with several competing taxonomic systems: PMESII (Political, Military, Economic, Social, Information, Infrastructure), used in NATO operational planning and in intelligence analysis ([Giannopoulos, Smith and Theocharidou 2021](#); [NATO 2022](#)); DIME (Diplomatic, Information, Military, Economic), established in American strategic doctrine ([Chambers 2016](#); [Hoffman 2007](#)); and MPECI (Military, Political, Economic, Civil, Information), present in certain European Union documents. At the same time, the term hybrid conflict coexists with competing concepts in academic literature: full-spectrum warfare denotes the synchronised use of all instruments of power across the entire spectrum of conflict ([Hoffman 2007](#); [Fridman 2018](#)); parallel warfare describes the simultaneous attack on multiple critical systems of the adversary with the aim of overwhelming its capacity to respond ([Warden 1995](#)); and shadow warfare emphasises the deliberately undeclared and ambiguously attributable character of the actions ([Mumford 2013](#); [Berzins 2014](#)). The present study employs the term hybrid conflict as a concept established in NATO doctrine, recognising that the three alternative terms are complementary, each illuminating a different dimension of the phenomenon: the breadth of instruments, the logic of their synchronisation, and strategic ambiguity, respectively, all of which dimensions are incorporated into the proposed model. The functional six-domain structure adopted is logically compatible with PMESII, but adapted for operationalisation at the level of crisis management and national institutional resilience.

The present study proceeds from the observation that the academic literature often treats hybrid threats either from an exclusively military perspective or from an exclusively cyber or information one, without proposing an integrated framework of analysis and response. Accordingly, the objectives of the research are: (1) to develop an updated functional taxonomy of hybrid instruments, compatible with contemporary analytical frameworks; (2) to construct a model of crisis management with named actors and quantifiable indicators; (3) to undertake a comparative assessment of Romania's resilience capabilities relative to states with consolidated experience; and (4) to formulate concrete public-policy recommendations. The methodology combines an analysis of strategic documents adopted at the level of NATO, the European Union, and the states examined, a synthesis of recent academic literature, and an analysis of institutional reports published over the period 2022-2024 ([Strachan-Morris 2022](#); [Giannopoulos, Smith, and Theocharidou 2021](#)).

The structure of the article reflects these objectives: section 1 elaborates the conceptual framework and the taxonomy of hybrid threats; section 2 proposes the integrated crisis-management model; section 3 analyses six documented cases; section 4 assesses the specific case of Romania; section 5 formulates conclusions and public-policy recommendations.

1. The conceptual framework of hybrid conflict

1.1. The evolution of the concept of hybrid conflict

Although the term hybrid conflict was established in the specialised literature through the work of Hoffman (2007), the phenomenon it describes is not new. The combination of military means with political, economic, and propagandistic pressure has been systematically practised throughout history; the novelty lies in the speed, scale, and degree of coordination with which this combination can today be orchestrated, also through generative artificial intelligence ([Fridman 2018](#); [Gioe, Goodman, and Omand 2022](#)). Gerasimov (2013) outlined a doctrinal vision according to which the weight of non-military means had exceeded that of strictly military instruments, inverting the paradigm of the conflicts of the previous century. Galeotti (2018) subsequently tempered this interpretation, noting that Gerasimov's text reflected an observed reality rather than a prescriptive plan of action, while Thomas (2016) demonstrated that the Russian doctrine of reflexive control constitutes the theoretical substratum that unifies hybrid instruments within a coherent strategy. The developments of the period 2022-2024 provided factual confirmation of this doctrinal reading.

At the institutional level, NATO formulated an operational definition in the Warsaw Summit Communiqué (2016), reaffirmed and deepened in the Madrid Strategic Concept (2022): hybrid threats denote actions that articulate military and non-military means, conducted in a coordinated manner to destabilise a state or an alliance without reaching the threshold that would trigger a collective response

under Article 5 of the North Atlantic Treaty. Through the same document, Russia was explicitly designated as the most direct and severe threat to the Alliance, while China was characterised as a source of systemic challenges (NATO 2022). The European Union, through document JOIN (2016)18 and, more recently, through the NIS2/CRA legislative package (2022-2024), has expanded the normative framework for responding to hybrid threats (Fiott and Parreira 2020).

1.2. An updated taxonomy of hybrid threats

The debate concerning the analytical frameworks of hybrid threats reflects the rapid evolution of the field of study. PMESII, developed within the NATO doctrinal environment, structures the variables of analysis along six dimensions: Political, Military, Economic, Social, Information, and Infrastructure. The principal advantage of this framework lies in its comprehensiveness and in its capacity to integrate infrastructure vulnerabilities as an autonomous variable; its limitations relate to the complexity of operationalisation at the level of national planning (Giannopoulos, Smith, and Theocharidou 2021). DIME organises the instruments of state power along four axes: Diplomatic, Information, Military, and Economic. Its advantage consists in strategic clarity; its limitations reside in the subordination of the civil dimension to the military and diplomatic axes (Chambers 2016; Hoffman 2007). MPECI, present in certain European Union documents, explicitly distinguishes the civil component from the military and political ones, but underestimates infrastructure vulnerabilities and does not include a domain dedicated to internal mobilisation and offensive legal actions. The present study adopts a functional six-domain structure, logically compatible with PMESII, but adapted for operationalisation at the level of crisis management and national institutional resilience. This choice does not amount to a reduction of PMESII, but to a reconfiguration oriented towards a precise analytical purpose: the mapping of hybrid-threat vectors in correlation with the response capabilities of a given national framework.

Table 1 sets out the revised taxonomy, organised into six functional domains. Compared with earlier versions (Cullen and Reichborn-Kjennerud 2017; Giannopoulos, Smith și Theocharidou 2021), the present structure introduces several new elements: the use of generative artificial intelligence in information influence operations, the sabotage of submarine infrastructure, pressure on supply chains as an economic vector, and, as a sixth distinct domain, internal mobilisation and offensive legal actions, instruments empirically confirmed in recent cases but absent from the established taxonomies.

The data in Table 1 show that cyber and information instruments are the most frequently used in the documented hybrid conflicts of recent years, with a significant intensification from 2022 onwards. The use of generative artificial intelligence to produce falsified content at scale and to personalise disinformation messages makes detection and attribution significantly more difficult. The sabotage of physical infrastructure, illustrated by the incidents in the Baltic Sea (2023-2024), indicates a

TABLE 1. Taxonomy of hybrid threats: domains, instruments, and documented cases (2024)

Functional domain	Principal instruments	Recent documented cases
Cyber	Saturation attacks (DDoS); advanced persistent infiltration (APT); sabotage of industrial control systems (ICS)	Estonia (2007); Ukraine power grid (2015-16); Viasat (2022); Sandworm/Industroyer2 (2022)
Informational	Systematic disinformation; AI-generated digital forgeries; amplification through automated networks; electoral influence	Electoral interference Romania (2024); Moldova (2023-24); pro-Russian campaigns EU (2023-24)
Economic	Energy blackmail; selective trade restrictions; hostile acquisitions in sensitive sectors; coordinated diplomatic pressure	Russo-Ukrainian gas blockages (2006, 2009, 2021); reductions in gas deliveries to Europe 2021-22
Sub-threshold military	Unmarked forces; private military companies; support for separatists; physical-infrastructure sabotage	Crimea (2014); eastern Ukraine (2014-22); Baltic submarine cables (2023-24)
Social-political	Financing of extremism; exploitation of identity tensions; corruption of elites; subversion of democratic processes	Financing of European parties; Romania elections 2024
Internal mobilisation / Offensive legal actions	Recruitment of the diaspora and minorities; instrumentalisation of legal rights; orchestrated strikes and judicial blockages	Russian minority in the Baltic states (2007-present); instrumentalised judicial actions in the EU; mobilisations in Romania 2024

Source: Compiled by the author on the basis of the specialised literature (Hoffman 2007; Berzins 2014; Cullen and Reichborn-Kjennerud 2017; IISS 2023) and the reports of ENISA (2024), CCDCOE (2024), and SRI (2023).

shift towards the sub-threshold military domain. A domain insufficiently formalised in earlier taxonomies, but empirically confirmed by recent cases, is that of internal mobilisation and offensive legal actions: the recruitment and activation of a state's own citizens or of minorities within the target state, as well as the instrumentalisation of legitimate legal mechanisms, such as judicial proceedings, the right to strike, and freedom of assembly, in order to paralyse the functioning of democratic institutions (Renz 2016; Giannopoulos, Smith and Theocharidou 2021; Thomas 2016).

1.3. The comparative intensity of hybrid instruments across the cases analysed

Figure 1 presents the evolution of documented hybrid incidents within the Euro-Atlantic area over the period 2015-2024, the author's own processing on the basis of the ENISA cyber threat-landscape reports (2023, 2024) and the cyber-incidents database of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE 2024). Figure 2 presents a radial analysis of instrumental intensity across six selected cases covering the period 2007-2024, on the basis of ENISA (2023, 2024), CCDCOE (2024), SRI (2023), DNSC (2023), and Tikk et al. (2008).

Figure 1 brings into focus three trends of particular significance. On the one hand, the rapid pace of growth in the number of recorded hybrid incidents reflects both the escalation of hostile pressure and the progress achieved in identification and attribution mechanisms. Secondly, the large-scale Russian invasion of Ukraine

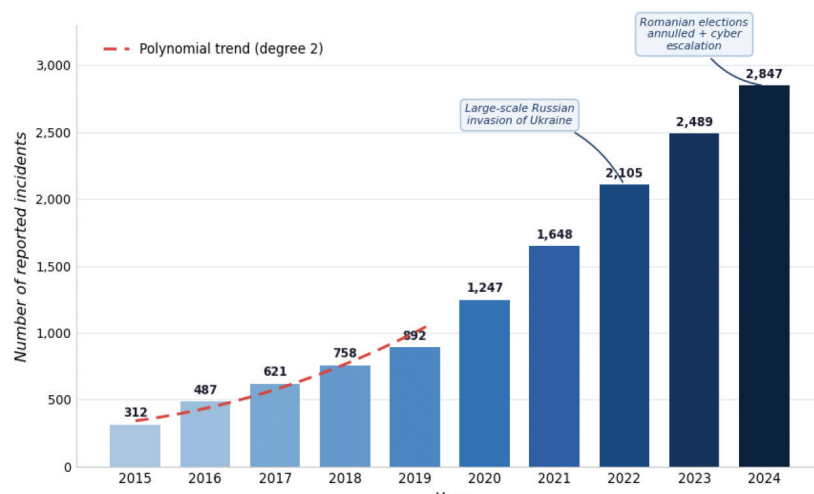


Figure 1 The evolution of hybrid incidents within the Euro-Atlantic area
 Source: the author's own processing on the basis of the ENISA Threat Landscape Report (2023, 2024) and the CCDCOE Cyber Incidents Database (2024). 2024 data: preliminary estimate based on the ENISA Q1-Q3 2024 reports.

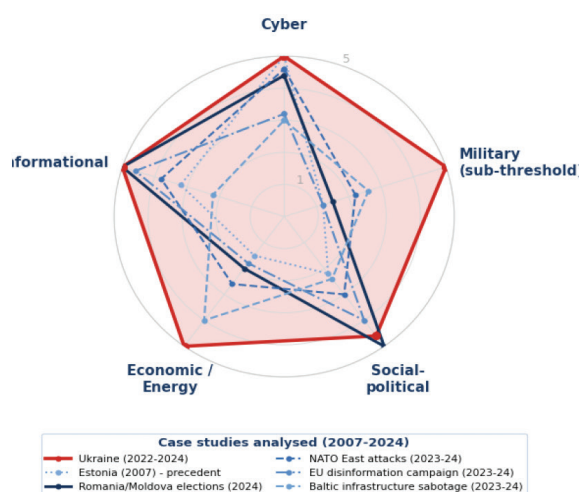


Figure 2 compiled by the author based on ENISA (2023, 2024), CCDCOE (2024), SRI (2023), DNSC (2023), and Tikk et al. (2008).

(2022) marks a qualitative rupture: the annual frequency of incidents doubled compared with 2021, and the typology of attacks diversified towards domains with direct physical impact. Thirdly, the European and national electoral cycle of 2024 confirms that democratic processes constitute a priority target of contemporary hybrid campaigns.

Figure 2 allows the identification of three profiles of hybrid engagement. The first profile, illustrated by the case of Ukraine (2022-2024), is the fully integrated one, with maximum intensity across all six functional domains. The second profile, exemplified by Romania 2024 and Moldova 2023-2024, is of an information-

electoral type, conducted without any explicit military component. It illustrates that hybrid threats are capable of producing strategic-level effects without exceeding the threshold of armed force. The third profile, illustrated by Estonia 2007 and the sabotage of Baltic infrastructure, is the cyber and physical one.

2. The integrated model for managing hybrid crises

2.1. Guiding principles

The literature on crisis management ([Boin et al. 2016](#); [Rosenthal, Boin, and Comfort 2001](#); [Ansell, Boin, and Keller 2010](#)) and the doctrinal documents of NATO and the European Union converge on a number of principles whose observance conditions the effectiveness of the response to hybrid threats. The first principle, that of anticipation, proceeds from the observation that hybrid aggressions are built up gradually, through the accumulation of small-scale disturbances which, viewed in isolation, do not exceed the level of a crisis ([Giannopoulos, Smith, and Theocharidou 2021](#)). The second principle is inter-institutional coordination: the effectiveness of the response depends on the capacity to synchronise the actions of institutions with different organisational cultures, legal mandates, and chains of command ([Strachan-Morris 2022](#); [Chambers 2016](#)). The third principle is that of coherent public communication ([Pamment et al. 2018](#)). A fourth principle, absent from the earlier literature, concerns technological adaptability: response structures are required to assimilate artificial-intelligence instruments for the detection, assessment, and attribution of threats ([Gioe, Goodman, and Omand 2022](#)).

2.2. The structure of the four-phase model

The construction of the proposed model drew on two reference frameworks well established in the literature of the field. The first is the four-phase crisis-management model elaborated by Boin et al. (2016): crisis identification, decision-making, coordination of actions, and public communication. This model, although comprehensive for classic crises, does not incorporate the cyber dimension as an autonomous prevention phase, does not integrate the recent European normative framework, and does not name responsible actors with measurable performance indicators. The second reference framework is the hybrid-threat management structure proposed by Giannopoulos et al. (2021) at the level of the European Union, organised around the stages of anticipation, prevention, detection, and response, but without an explicit recovery phase and without named actors or quantifiable indicators.

The model proposed in the present study improves on both frameworks by: (a) including the prevention phase as an autonomous stage with dedicated actors and instruments, including Directive NIS2 (2022/2555) on the security of network and information systems and Regulation CRA (2024/2847) on cyber-resilience requirements; (b) treating detection as an autonomous phase, distinct from response, with clear institutional mandates and artificial-intelligence instruments for

signal analysis; (c) naming the actors responsible for each phase; and (d) defining quantifiable and verifiable performance indicators. The treatment of detection as a stage in its own right follows from the fact that, in the earlier models (Boin et al. 2016; Giannopoulos, Smith, and Theocharidou 2021), it was subordinated to the response phase, without defined institutional mandates. The analysis of the cases in section 3 demonstrates that detection deficiencies constitute the principal explanatory factor in response failures, including in the case of the Romanian elections of 2024 (DNSC 2024; BISI 2025).

TABLE 2. The integrated model for managing hybrid crises: phases, objectives, actors, and performance indicators

Phase	Central objective	Principal actors	Performance indicator
PREVENTION	Reduction of systemic vulnerabilities; compliance with NIS2 (2022/2555) and CRA (2024/2847)	Government, DNSC, SRI, critical-infrastructure operators	GCI Index: Tier T1; ≥4 national hybrid exercises/year
DETECTION	Continuous monitoring; predictive (AI) analysis of hybrid indicators	SRI, SIE, DNSC, CRISC, OSINT structures	Detection time under 24 hours; tactical attribution: 72h
RESPONSE	Countering actions; limiting impact; strategic communication	CSAT, MAI, MAPN, NATO/EU structures, digital platforms	Impact limitation: < 48h; prevention of crisis escalation
RECOVERY	Restoration of functionality; post-crisis audit; strategic resilience	Public authorities, parliamentary committees, independent auditors	Restoration: 100%; publication of a Lessons Learned report

Source: compiled by the author on the basis of Boin et al. (2016), Giannopoulos et al. (2021), Chambers (2016), and the operational experience documented over the period 2022-2024.

2.3. The NATO and European Union normative and institutional framework for responding to hybrid threats

After 2022, the institutional framework for responding to hybrid threats underwent a process of accelerated strengthening. At the NATO level, the Madrid Strategic Concept (2022) enshrined hybrid conflict as a central planning scenario, while the Vilnius Summit (2023) adopted region-specific defence plans. The relevant centres of excellence, namely the Strategic Communications Centre of Excellence (StratCom COE, Riga), the Cooperative Cyber Defence Centre of Excellence (CCDCOE, Tallinn), and the Counter-Intelligence Centre of Excellence (CI COE, Bucharest), expanded their mandates and operational capabilities. The Tallinn Manual 2.0 (Schmitt 2017) and subsequent allied doctrine incorporate specific operational guidelines for countering cyber-attacks in the context of hybrid conflicts (NATO 2022; European Council 2023).

The European Union accelerated the adoption of its cybersecurity legislative framework: Directive NIS2 (2022/2555) on the security of network and information systems, Directive CER (2022/2557) on the resilience of critical entities, and

Regulation CRA (2024/2847) on horizontal cybersecurity requirements for products with digital elements together currently form the most comprehensive normative framework for responding to hybrid threats in the world ([Broeders, Goffin and Groothuis 2023](#); [Fiott and Parreira 2020](#)).

3. Documented cases: lessons for the management of hybrid crises

The six case studies analysed in the present research cover the temporal interval 2007-2024, with an analytical emphasis on recent events, characterised by a high degree of empirical documentation and availability of primary and secondary sources. The conceptualisation of the notion of a “documented case” operationalises the methodological requirements specific to qualitative research in the social sciences, in keeping with the case-study paradigm developed by Robert K. Yin ([2018](#)). Within this epistemological logic, each unit of analysis is rigorously delimited from a spatio-temporal perspective and investigated multidimensionally through an analytical grid structured along three complementary levels: (1) the nature, mechanisms, and vectors of the hybrid action; (2) the dynamics, coherence, and effectiveness of the institutional response; and (3) the validation of strategic prescriptions and the identification of lessons learned relevant to the consolidation of institutional and operational resilience.

Each case study is systematically integrated within the proposed conceptual taxonomy, contributing both to testing the internal consistency of the analytical model and to refining its explanatory dimensions. The case-selection strategy was grounded in the criterion of maximum typological diversity, with the aim of ensuring the full representation of the six functional domains identified within the taxonomy. Such a methodological approach facilitates a comprehensive comparative analysis of the manifestations of the hybrid phenomenon and strengthens the internal validity and explanatory capacity of the theoretical-analytical model employed.

3.1. Ukraine (period analysed: 2022-2024)

The large-scale military aggression launched by the Russian Federation against Ukraine in February 2022 represents the most extensive and most rigorously documented example of integrated hybrid conflict of the post-Cold War period. The present analysis delimits the interval 2022-2024 and examines the convergent manifestation of hostilities across three fundamental dimensions: cyber, information, and economic.

In the cyber sphere, technology was used as a multiplier of operational capability, with the aim of disrupting command, control, and communications structures. On the night of 23-24 February 2022, concurrently with the launch of conventional military operations, the Sandworm group, affiliated with Russian military intelligence, carried out a destructive cyber-attack on the Viasat KA-SAT satellite communications network.

By compromising the equipment's embedded firmware, the operation disabled thousands of ground terminals used by Ukrainian governmental institutions and armed forces. The attack was the subject of a coordinated public attribution by the United States, the United Kingdom, and the European Union (CSIS 2022; ENISA 2024). In the same year, the same structure used the Industroyer2 malware to cause damage to a Ukrainian electrical substation, an incident regarded as the first major cyber-attack on Ukraine's energy infrastructure since 2017 (CSIS 2022; Mandiant 2023).

The cyber dimension was complemented by the information component, within which the cognitive confrontation took shape through coordinated disinformation campaigns conducted in at least fifteen European states. These influence operations sought both to fragment the internal social cohesion of Ukraine and to diminish the political and societal support extended to European security in the Western space (East StratCom Task Force 2023, 2024). In parallel, on the economic dimension, the transformation of commercial dependencies into instruments of geopolitical coercion was manifested through the deliberate and asymmetric reduction of natural-gas deliveries to European states over the period 2021-2022. This strategy sought to limit the capacity of the European Union to formulate and implement a firm diplomatic and economic response (Gressel 2022; Meydan 2022).

Compared with the crisis of 2014, the reaction of the North Atlantic Alliance and of the member states demonstrated significant doctrinal and operational progress, reflected in particular in the rapidity of the public attribution processes for cyber-attacks and in the effectiveness of strategic communication. Nevertheless, the conflict highlighted the persistence of structural vulnerabilities in the European security architecture. Among these are the residual energy dependencies of certain member states, the normative and operational fragmentation of national cyber-response mechanisms (Colby and Mitchell 2020; Gressel 2022), as well as the technical limitations associated with the sharing and integration of information at the allied level.

The main conclusion drawn from the analysis of this theatre of confrontation is that societal resilience constitutes the foundation of the modern capacity for deterrence and defence. Recent comparative analyses show that the defensive viability of a state in the face of hybrid threats depends directly on the existence of a robust and redundant industrial capacity for the production of armaments and munitions, on the diversification of energy sources and the reduction of strategic dependencies, as well as on the consolidation of institutional cohesion and of society's capacity to resist actions of information manipulation, propaganda, and psychological warfare (Gressel 2022; IISS 2024).

3.2. Electoral interference in Romania (2024)

The presidential elections in Romania held on 24 November 2024 represented the first case in the history of NATO-member democracies in which a presidential ballot was

annulled after the conduct of the first round of voting. The independent candidate Călin Georgescu, credited with less than 1% in the opinion polls of October 2024, obtained 22.94% of the total votes cast (FPRI 2024; BISI 2025). The documents partially declassified by the Supreme Council of National Defence (CSAT) on 4 December 2024 revealed the existence of three principal lines of hostile action.

In the first place, more than 85,000 cyber-attacks directed against the electoral infrastructure were identified, including the compromise of digital credentials and code-injection attacks on databases (CSAT 2024; BISI 2025). Secondly, the investigations revealed the existence of coordinated networks of accounts on the TikTok and Meta platforms, which generated approximately 179 million impressions for content favourable to the candidate, through the use of automated mechanisms for the promotion and distribution of messages (OECD 2024). Thirdly, the authorities established the existence of mechanisms for the illegal financing of the electoral campaign, given that the candidate had officially declared a nil electoral budget, while subsequent investigations indicated the existence of undeclared contributions estimated at approximately one million euros originating from third-party sources (CSAT 2024; BISI 2025).

The institutional response materialised on 6 December 2024, when the Constitutional Court of Romania unanimously decided to annul the results of the first round of the presidential elections, invoking the provisions of Article 50, paragraph (3) of the electoral legislation. At the European level, the European Commission initiated proceedings against the TikTok platform under the Digital Services Act (DSA 2022). The case is extensively documented both in the specialised literature and in institutional documents drawn up by the Romanian Intelligence Service (SRI 2024), the Supreme Council of National Defence (2024), the National Cyber Security Directorate (DNSC 2024), the Bloomsbury Intelligence and Security Institute (BISI 2025), and the Foreign Policy Research Institute (FPRI 2024).

The analysis of this case empirically demonstrates that a hybrid campaign lacking a military component can generate strategic-level effects, including the annulment of a national ballot, through the exclusive use of cyber, information, and internal-mobilisation instruments. The phenomenon illustrates the sixth domain of the proposed taxonomy, defined by the instrumentalisation of legitimate legal mechanisms and the activation of internal actors in the absence of a normative and institutional framework adequate to counter such threats (DNSC 2024; BISI 2025).

3.3. Cyber-attacks on NATO infrastructure in Eastern Europe (2023-2024)

The reports drawn up by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE 2024) and by the European Union Agency for Cybersecurity (ENISA 2024) document a significant intensification of cyber-attacks against critical infrastructure in the NATO states situated on the eastern flank over the period 2023-2024. These offensive operations systematically targeted the energy,

telecommunications, financial, and transport sectors. In the particular case of Romania, the National Cyber Security Directorate (DNSC 2023, 2024) reported saturation attacks directed against energy and telecommunications networks, actions whose probable attribution points to groups affiliated with the Russian state. From a tactical standpoint, a methodical escalation could be observed, from actions of transient impact towards sustained infiltrations into industrial control networks, a dynamic characteristic of the logic of asymmetric conflicts (Wilner 2020; Lanoszka 2016).

The assessment of institutional performance carried out by the CCDCOE (2024) highlights structural disparities correlated directly with the degree of technological maturity of the defending party. Thus, the data document that states classified in Tier 1 of the Global Cybersecurity Index (GCI) demonstrated superior detection and response capabilities compared with states in Tier 2. This disparity in performance validates the thesis that strategic investments in cyber resilience are reflected directly and measurably in the defensive capacity of security structures in crises.

The escalation trend highlighted in this theatre of operations, manifested through the transition from rudimentary saturation attacks to complex and persistent infiltrations into industrial control infrastructures, generates major doctrinal implications. This evolution of threats makes it imperative to clearly separate the detection phase from the response phase within models for the management of hybrid crises. This functional delimitation constitutes, moreover, the principal foundation of the analytical and operational structure proposed in section 2 of the present research.

3.4. The sabotage of submarine infrastructure in the Baltic Sea (2023-2024)

At least eleven submarine cables and pipelines located in the Baltic Sea region were damaged over the period October 2023 - January 2025, according to documentation published by Reuters and Defense News (2025). Among the most relevant incidents confirmed by official investigations is that of 8 October 2023, when the Balticconnector pipeline, which provides the energy connection between Finland and Estonia over a distance of 152 kilometres, together with several associated telecommunications cables, was damaged by the anchor of the Chinese vessel NewNew Polar Bear, according to the conclusions formulated by the Finnish investigating authorities.

Subsequently, on 18 November 2024, the BCS East-West Interlink submarine cable, which connects Lithuania and Sweden over a distance of 218 kilometres, as well as the C-Lion1 cable, which provides the link between Finland and Germany over a length of 1,173 kilometres, were damaged almost simultaneously. In this context, the Chinese vessel Yi Peng 3 remained for several weeks under the permanent monitoring of the Royal Danish Navy. The series of incidents continued on 25 December 2024, when the Estlink 2 energy cable, which serves the Finland-Estonia

connection, together with four other submarine telecommunications lines, was severed ([Reuters 2025](#); [Defense News 2025](#)).

Despite the gravity of these incidents, the official and legal attribution of responsibility remains inconclusive in all the cases investigated. Assessing these developments, the NATO Secretary General, Mark Rutte, highlighted the complexity of the phenomenon without explicitly naming the Russian Federation, stating that hybrid actions are manifested through sabotage, cyber-attacks, and, in the current context, through aggressions directed against the critical submarine infrastructure of the North Atlantic Alliance (NATO, November 2024, cited in [Defense News 2025](#)). In response to this emerging vulnerability, the NATO Vilnius Summit initiated a programme dedicated to the protection of critical submarine infrastructure. This undertaking was consolidated in 2025 by the European Commission, which allocated almost one billion euros for the monitoring of submarine cable networks and for the constitution of a specialised fleet of vessels intended for emergency interventions and repairs.

From an analytical perspective, this succession of incidents highlights the fundamental paradox of actions conducted below the threshold of conventional military confrontation and reflects the design logic of contemporary asymmetric threats. The empirical data indicate that operations with major strategic impact on allied security are deliberately conceived so as to preserve ambiguity of attribution. By exploiting evidentiary difficulties and maintaining a high level of legal and operational uncertainty, the actors involved seek to avoid the activation of the collective-defence mechanism provided for by Article 5 of the North Atlantic Treaty.

3.5. The disinformation campaign at the European level (2023-2024)

The flow of disinformation campaigns associated with pro-Kremlin interests in the European space is systematically monitored by the EUvsDisinfo platform, coordinated by the European External Action Service since 2015. The data aggregated in the public database of this structure indicated, as of March 2024, the existence of more than 2,855 cases of disinformation directly correlated with the war in Ukraine, as well as a further 943 cases associated with the COVID-19 pandemic ([East StratCom Task Force 2024](#)).

This offensive dynamic intensified significantly in the context of the elections to the European Parliament held over the period 6-9 June 2024. The monitoring carried out by the European Digital Media Observatory (EDMO) and by the European network of fact-checking organisations highlighted a considerable increase in disinformation narratives directed against the European Union in the months preceding the ballot ([EDMO 2024](#)). With a view to limiting these threats, the Digital Services Act ([DSA 2022](#)) established the obligation for the major technology platforms to assess and mitigate the systemic risks associated with disinformation. On the basis of this normative framework, the European Commission initiated formal investigation

proceedings against the companies X and Meta for possible breaches of the rules concerning the integrity of electoral processes ([European Parliament / European Commission 2024](#)).

The response mechanisms activated by the European Union through the Digital Services Act, the EUvsDisinfo platform, and the cooperation agreements concluded with digital-service providers generated relevant operational effects, yet these remain limited relative to the scale and adaptability of the phenomenon. The instruments implemented proved insufficient for the complete neutralisation of disinformation campaigns, in the context of an asymmetric adversary that continually adapts its tactics and operational methods in order to evade the technical mechanisms for the identification, classification, and filtering of manipulative content. This evolution highlights the current limitations of the European defensive structures with respect to the consolidation of a secure and resilient information space.

The analysis of this propagandistic ecosystem offers a strategic conclusion relevant to the management of the contemporary cyber and cognitive space. The empirical data indicate that the effectiveness of information instruments used within hybrid warfare depends directly on the coherence, applicability, and firmness of the normative framework that regulates the activity of digital platforms. Consequently, resilience in the face of subversive actions is not conditioned exclusively by the existence of formal regulations, but also by the development of a robust institutional capacity for the real-time identification, analysis, and countering of manipulative narratives and coordinated influence operations.

3.6. Estonia (2007): the founding precedent and its doctrinal relevance

The cyber-attacks conducted against Estonia over the period 27 April - 18 May 2007 lasted 22 days and systematically targeted, through saturation-type attacks, governmental and ministerial portals, media institutions, internet-service providers, major banking institutions, and small private enterprises ([CCDCOE 2024](#); [Ottis 2008](#); [StratCom COE 2019](#)). From a geopolitical perspective, these aggressions coincided with the decision of the Estonian authorities to relocate the Bronze Soldier monument from the centre of the city of Tallinn. The subsequent assessments drawn up by the NATO Cooperative Cyber Defence Centre of Excellence concluded that the entire episode may conceptually be interpreted as a complex information operation coordinated by the Russian Federation, although the technical and judicial investigations did not lead to a definitive and incontestable legal attribution ([Ottis 2008](#)).

Although it exposed major structural vulnerabilities, the crisis generated far-reaching doctrinal and institutional reforms both at the national level and within the North Atlantic Alliance. The events of 2007 functioned as a catalysing factor for the elaboration of the Tallinn Manual and contributed decisively to the formal recognition of cyberspace as the fifth operational domain of NATO. These developments were consolidated in May 2008 through the official establishment

of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Domestically, this critical conjuncture accelerated the transformation of Estonia from a vulnerable state into a global reference actor in the field of cybersecurity and institutional resilience, a performance reflected in particular by its attainment of Tier 1 (T1) within the Global Cybersecurity Index (ITU 2024).

The evolution of Estonia after 2007, from the status of a state exposed to significant vulnerabilities to the position of an international benchmark in the field of cybersecurity, constitutes one of the most relevant empirical arguments in support of the idea that a security crisis, managed through coherent public policies and a long-term strategic vision, can be transformed into a durable strategic advantage (Schmitt 2017; Broeders, Goffin and Groothuis 2023). From a comparative perspective, this trajectory represents one of the most valuable doctrinal and institutional lessons for the consolidation of Romania's security architecture in relation to contemporary hybrid threats.

4. The case of Romania: vulnerabilities, institutional framework, and directions for reform

4.1. The risk profile: geopolitical positioning and structural vulnerabilities

Romania cannot be analysed from the perspective of national security without reference to its geopolitical specificity: its positioning on the Black Sea, its immediate proximity to zones of active conflict, the presence of NATO's strategic infrastructure on national territory, and the existence of a population exposed to disinformation flows propagated across two linguistic spaces with cross-border circulation. The events taking place during 2024 empirically demonstrated that Romania does not represent a peripheral actor with respect to hybrid conflict, but rather one of the member states of the Euro-Atlantic area with the highest level of direct exposure to asymmetric threats. In this context, the documented electoral interference definitively transformed Romania from a mere observer of the hybrid phenomenon into a reference case study analysed and invoked at the allied level (SRI 2024; CSAT 2024; DNSC 2024).

The risk analysis highlights the existence of four interdependent structural vulnerabilities that affect national security. The first critical dimension is represented by the cyber component, since the energy infrastructure, the telecommunications networks, and the information systems of the public administration continue to constitute constant targets of hostile cyber activities. In numerous documented situations, intrusion-identification times significantly exceed the reference threshold of 30 days established in NATO standards (DNSC 2023). This technological vulnerability is amplified by a persistent information fragility, reflected in the limited capacity of state institutions to monitor systematically and to counter rapidly the coordinated disinformation campaigns, a reality starkly highlighted in the context of the 2024 electoral process.

The third structural vulnerability concerns the level of social cohesion. Pronounced political polarisation and the persistent deficit of public trust in state institutions create a context favourable to the propagation and amplification of destabilising messages associated with hybrid actions (EIU 2023; SRI 2024). Finally, the fourth vulnerability, empirically confirmed by the political developments of 2024, concerns the limits of the institutional capacity to identify and neutralise in good time the processes of internal mobilisation and the offensive use of legal mechanisms by disruptive actors. The absence of a specific legislative framework adapted to the new forms of hybrid aggression leaves this domain insufficiently protected against strategies of institutional exploitation and political subversion (Renz 2016; Walker 2018).

4.2. An audit of the institutional and normative framework

Assessing Romania's institutional capacity to manage hybrid threats requires the analysis of two complementary and interdependent dimensions: the existence of an adequate normative framework and the effectiveness of the operational structures responsible for its application. From this perspective, institutional resilience is not determined exclusively by the formulation of strategic documents and normative acts, but also by the effective capacity of institutions to integrate, coordinate, and implement response mechanisms adapted to the multidimensional character of contemporary hybrid threats.

TABLE 3. An audit of Romania's institutional framework for the management of hybrid threats

Document / Institution	Year	Principal gap identified
SNA 2020-2024 (National Defence Strategy)	2020	Absence of a dedicated hybrid operational plan. The 2025-2030 Strategy (adopted in 2025) partially remedies this deficit by including explicit hybrid measures.
Cybersecurity Strategy 2022-2027 (GD 963/2022)	2022	Insufficient public funding, situated below the threshold of 0.05% of GDP, compared with the NATO reference threshold of 0.10%.
Law no. 51/1991 on national security (rev. 2014)	1991/2014	Structural failure to adapt to hybrid threats, a concept recognised at EU level since 2014 following the annexation of Crimea.
DNCS: National Cyber Security Directorate	2021	Configured as a coordinating rather than a commanding authority; limited data exchange with the private sector.
SRI: National CYBERINT Centre	2012	Limited flow of information and exchange of technical data with private critical-infrastructure operators.
Participation in PESCO (17 projects)	2017-present	Represents a European Union cooperation mechanism rather than a national construct; operational contribution below actual capacity.

Source: Compiled by the author on the basis of official national documents and NATO/EU assessments (SRI 2023, 2024; DNCS 2023, 2024; SEAE 2023).

Table 3 presents a comparative audit of the main strategic documents and of the institutions relevant to the national security architecture, highlighting the structural gaps identified in relation to the standards and practices consolidated at the Euro-Atlantic level. The analysis examines both the degree of conceptual and normative adequacy of the existing framework and the level of institutional interoperability, the capacity for inter-institutional coordination, and the effectiveness of the prevention, detection, and response mechanisms in the face of hybrid threats.

The adoption of the National Defence Strategy for the period 2025-2030, a document that for the first time includes explicit measures dedicated to countering hybrid threats, constitutes a relevant advance in the process of adapting the national security architecture to the new forms of conflict. The explicit introduction of the hybrid dimension within the strategic priorities reflects both the intensification of external pressures on the Euro-Atlantic area and the need to develop institutional mechanisms capable of responding to contemporary multidimensional threats.

Nevertheless, the developments of 2024 empirically confirmed the persistence of major operational vulnerabilities. The first of these concerns the absence of an integrated institutional rapid-reaction mechanism in situations of hybrid electoral interference, capable of ensuring immediate coordination among the security structures, the electoral authorities, and the actors responsible for protecting the digital infrastructure. The second vulnerability relates to the insufficient capacity for real-time monitoring and analysis of the digital space, a limitation that reduces the effectiveness of the early identification of coordinated influence and disinformation campaigns. Finally, the third structural gap consists in the non-existence of a formalised and operationalised framework of cooperation between the national security institutions and the digital platforms operating on Romanian territory, an aspect that affects the capacity for rapid reaction and the efficient exchange of relevant information (DNSC 2024; CSAT 2024).

These deficiencies highlight the fact that the modernisation of the strategic and normative framework, although necessary, is not sufficient in the absence of the development of integrated operational mechanisms, capable of functioning on a permanent basis and of responding to the dynamic and adaptive character of contemporary hybrid threats.

4.3. A comparative analysis of resilience

The table presents a comparative assessment of the principal resilience indicators in relation to hybrid threats, placing Romania's institutional performance within the context of four member states of the North Atlantic Treaty Organization relevant from a strategic and operational perspective. The comparative analysis seeks to highlight the differences in institutional capacity, degree of operational maturity, and level of integration of response mechanisms, in relation to the standards consolidated at the Euro-Atlantic level.

Tabel 4: Comparative indicators of resilience to hybrid threats: Romania and NATO reference states

Indicator	Finland	Estonia	Sweden	Poland	Romania	Ref.
GCI Tier 2024 (ITU)	T1	T1	T1	T2	T2	T1
Dedicated hybrid legal framework (year of adoption)	2017	2018	2021	2022	Absent	2016*
Cybersecurity budget (% of GDP, GD 963/2022)	n/a	n/a	n/a	n/a	below 0.05%	>0.10%
PESCO participation: active projects (SEAE 2023)	12	15	11	14	17*	-

Sources: ITU Global Cybersecurity Index 2024 (September 2024); SEAE, PESCO Progress Report 2023; GD no. 963/2022.

The data included in the table are drawn exclusively from public, official, and verifiable primary sources, being correlated with strategic documents, institutional reports, and independent assessments available in the academic and security domain. This approach ensures the methodological coherence of the comparison and permits a rigorous interpretation of the performance differences among the states analysed with respect to resilience to hybrid threats.

The data aggregated within the comparative analysis indicate the existence of a systemic gap on the part of Romania relative to the reference states included in the analytical sample. According to the Global Cybersecurity Index 2024 drawn up by the International Telecommunication Union (ITU), Romania is classified in Tier 2 (advanced), while Estonia, Finland, and Sweden are consistently situated in Tier 1 (the benchmark tier), corresponding to the highest level of performance of the index.

The absence of a normative framework dedicated to the integrated management of hybrid threats, in contrast to the institutional and legislative developments recorded in Finland (2017), Estonia (2018), and Poland (2022), represents the principal structural gap of the national security architecture. This deficiency is further highlighted by the administrative difficulties in formulating a coherent preventive response in the context of the developments of 2024.

In financial terms, the vulnerability is amplified by the relatively low level of resources allocated to cybersecurity, which remains below the threshold of 0.05% of gross domestic product (GD 963/2022), a value inferior to the reference threshold of 0.10% used in the comparative assessments of the North Atlantic Alliance.

From this perspective, the conclusion of the comparative analysis highlights that systemic and predictable investment in resilience mechanisms constitutes a fundamental condition of strategic stability, rather than a derived consequence of it.

Conclusions

The present research permits the formulation of conclusions of both theoretical and applied relevance, articulated around three major conceptual axes, which contribute to clarifying the contemporary dynamics of hybrid conflict and to understanding the conditions of systemic resilience within the Euro-Atlantic area.

The first argument concerns the structural transformation of hybrid conflict over the interval 2022-2024, a period in which asymmetric instruments evolved from complementary roles to central positions in the architecture of geopolitical competition. The analysis of the cases investigated confirms the consolidation of an operational model in which cyber, information, economic, and legal actions are integrated within a unitary logic of strategic pressure. In this context, the conceptual debate concerning “full-spectrum warfare”, “parallel warfare”, and “shadow warfare” does not indicate a mutual exclusion but an analytical complementarity, each paradigm capturing distinct dimensions of the same phenomenon: the breadth of instruments, their operational synchronisation, and the deliberate management of ambiguity of attribution.

At the same time, the results of the research highlight a significant technological discontinuity, determined by the integration of generative artificial intelligence into the ecosystem of information operations. This evolution substantially reduces the production and distribution costs of manipulative content and exponentially amplifies the speed, volume, and granularity of influence campaigns, profoundly altering the balance between institutional defensive capabilities and non-state or state offensive ones.

The second argument focuses on the determinants of national and systemic resilience. The case study concerning the institutional and political dynamics in Romania in 2024 demonstrates that vulnerabilities of a normative nature and deficits of operational capacity do not generate merely localised disturbances, but can produce strategic-level effects, with a direct impact on institutional stability. Within this framework, the research introduces and consolidates the relevance of the domain of internal mobilisation and offensive legal actions (lawfare) as an autonomous vector of hybrid power, capable of producing effects comparable to those of cyber or conventional military instruments, in the absence of the use of kinetic force.

As a counterpoint, the evolutionary trajectory of Estonia after 2007 empirically confirms the possibility of converting a security crisis into a durable strategic advantage, provided there exists coherent institutional learning and a consistent transposition into public policy. This experience constitutes a doctrinal benchmark with a high value of transferability for the processes of consolidating resilience in states exposed to hybrid threats.

The third argument validates the analytical contribution of the model proposed within the research. The application of a management cycle structured around four interdependent phases, namely prevention, detection, response, and recovery, in correlation with an operational taxonomy extended to six functional domains, made it possible to systematically identify the institutional deficits specific to each unit of analysis. The results indicate the existence of a persistent structural risk in the case of Romania across the entire crisis-management chain, with pronounced vulnerabilities in the detection and response stages, relative to the standards consolidated at the level of the North Atlantic Treaty Organization.

In summary, the research highlights the imperative necessity of adopting a unitary and specialised normative framework for the management of hybrid threats, one that explicitly integrates the cyber, information, economic, and legal-political dimensions, including the emerging components of internal mobilisation and offensive legal actions. The consolidation of such an institutional architecture constitutes an essential condition for increasing strategic resilience and for full alignment with the security standards of the Euro-Atlantic area.

Public-Policy Recommendations

The recommendations formulated in the present work are calibrated in relation to a medium- and long-term strategic-planning cycle and fall within the commitments assumed by Romania as a member state of the North Atlantic Treaty Organization and the European Union. These lines of action aim at the coherent consolidation of the national resilience architecture in the face of hybrid threats, through the integration of the normative, institutional, operational, and societal dimensions within a unitary framework of response.

The first line of action consists in the elaboration of a normative framework dedicated to hybrid threats, one that includes explicit provisions concerning the prevention and countering of electoral interference, the sabotage of critical infrastructure, and influence operations assisted by artificial intelligence. This legal framework must explicitly include the recognition of internal mobilisation and offensive legal actions (lawfare) as autonomous vectors of threat to national security. Although the National Defence Strategy 2025-2030, adopted in 2025, includes general guidelines concerning the countering of hybrid threats, its operationalisation through sectoral action plans is necessary. These subsequent instruments should define detailed crisis scenarios, clearly assigned institutional responsibilities, and pre-established escalation thresholds for the activation of response mechanisms.

The second recommendation concerns the constitution of an integrated national centre for the fusion and analysis of information flows, with the mandatory participation of the Romanian Intelligence Service, the Foreign Intelligence Service, the National Cyber Security Directorate, the Ministry of Internal Affairs, and the

Ministry of National Defence. In order to ensure operational effectiveness, this structure must be supported by an explicit legal mandate, regulating the secure exchange of classified information and the rapid-activation protocols in situations of multidimensional crisis.

The third recommendation concerns the consolidation of cooperation between the public sector and the private sphere in the field of cybersecurity, through the formal integration of critical-infrastructure operators into the national detection and response mechanisms. This approach entails adapting models of the sectoral information-sharing and analysis-centre type to the national legal and institutional framework, with a view to ensuring a bidirectional, secure, and operational flow of technical data between the state and the economic actors of the essential sectors.

The fourth recommendation concerns the consolidation of information resilience at the societal level through the introduction of education for media security into compulsory schooling, as a structural instrument for the long-term countering of disinformation and cognitive-influence operations. In a complementary respect, this measure must be supported through the development of a national programme for the certification and validation of information sources, inspired by European good practices, including the experience of Finland.

The fifth recommendation concerns ensuring the financial and human sustainability of the cybersecurity system, through the progressive alignment of budgetary allocations with the reference threshold of 0.10% of gross domestic product, used in the comparative assessments at the level of the North Atlantic Treaty Organization. This increase must be correlated with the implementation of a national programme for the training, retention, and motivation of digital-security specialists, intended to reduce the deficit of critical competences in the public sector and to consolidate the operational capacity of the responsible institutions.

FUNDING STATEMENT

The present study did not benefit from any external funding, whether public or private. The research was carried out exclusively on the basis of the author's own resources.

CONFLICT OF INTEREST STATEMENT

The author declares that there is no conflict of interest of a financial, professional, or personal nature that may have influenced the preparation of the present article.

References

- Ansell, Chris, Arjen Boin, and Ann Keller.** 2010. "Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System." *Journal of Contingencies and Crisis Management* 18 (4): 195-207. <https://doi.org/10.1111/j.1468-5973.2010.00620.x>.
- Bachmann, Sascha-Dominik, and Hakan Gunneriusson.** 2015. "Russia's Hybrid Warfare in the East: The Integral Nature of the Information Sphere." *Georgetown Journal of International Affairs* 16: 198-211.
- Berzins, Janis.** 2014. *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*. Policy Paper No. 02. Riga: National Defence Academy of Latvia. https://www.nda.mil.lv/wp-content/uploads/2020/04/PP02_Berzins_Russia_Hybrid_Warfare.pdf.
- Bloomsbury Intelligence and Security Institute (BISI).** 2025. *Invisible Influence: Romania's Presidential Election Crisis*. Londra: BISI. <https://bisi.org.uk/reports/invisible-influence-romania-presidential-election-crisis>.
- Boin, Arjen, Paul't Hart, Eric Stern, and Bengt Sundelius.** 2016. *The Politics of Crisis Management: Public Leadership under Pressure*. Ed. a 2-a. Cambridge: Cambridge University Press.
- Broeders, Dennis, Hadrien Goffin și Bart Groothuis.** 2023. "Governing Cybersecurity through Resilience: The European Approach to Systemic Risk in Critical Infrastructure." *Journal of Common Market Studies* 61 (4): 901-919. <https://doi.org/10.1111/jcms.13442>.
- CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence).** 2024. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Tallinn: CCDCOE.
- Chambers, John (ed.).** 2016. *Countering Hybrid Warfare. MCDC Project Report*. Londra: Multinational Capability Development Campaign. https://assets.publishing.service.gov.uk/media/5a82499340f0b62305b91b2a/concepts_mcdc_countering_hybrid_warfare.pdf.
- Colby, Elbridge, and A. Wess Mitchell.** 2020. "The Age of Great-Power Competition." *Foreign Affairs* 99 (1): 118-130.
- CSAT (Supreme Council of National Defence).** 2024. "Synthesis concerning the hybrid influence campaign in the Romanian presidential elections of 2024 (partially declassified document)." Bucharest: CSAT.
- CSIS (Center for Strategic and International Studies).** 2022. *Cyber Operations Tracker: Russia-Ukraine Conflict 2022*. Washington: CSIS. <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>.
- Cullen, Patrick J., and Erik Reichborn-Kjennerud.** 2017. *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*. London: Multinational Capability Development Campaign. https://assets.publishing.service.gov.uk/media/5a82499340f0b62305b91b2a/concepts_mcdc_understanding_hybrid_warfare.pdf.

Defense News. 2025. "At Least 11 Cables and Pipelines Damaged in Baltic Sea Since October 2023." *Defense News*. <https://www.defensenews.com/naval/2025/01/28/at-least-11-cables-and-pipelines-damaged-in-baltic-sea-since-october-2023/>.

DNSC (National Cyber Security Directorate). 2023. *Annual report on the state of cybersecurity in Romania: 2023*. Bucharest: DNSC.

_____. 2024. Report on cyber threats against electoral processes: 2024. Bucharest: DNSC.

East StratCom Task Force (EEAS). 2023. *EUvsDisinfo Database: Annual Report 2023*. Brussels: European External Action Service. <https://euvsdisinfo.eu/reports/>.

_____. 2024. *EUvsDisinfo Database: Quarterly Report Q1 2024*. Bruxelles: EEAS. <https://euvsdisinfo.eu>.

EDMO (European Digital Media Observatory). 2024. *EU Elections 2024: Disinformation Monitoring Report*. Florence: EDMO / European University Institute.

EEAS (European External Action Service). 2023. *PESCO: Progress Report 2023*. Brussels: EEAS.

EIU (Economist Intelligence Unit). 2023. *Democracy Index 2023: Age of Conflict*. London: EIU.

ENISA (European Union Agency for Cybersecurity). 2023. *ENISA Threat Landscape 2023*. Heraklion: ENISA. <https://doi.org/10.2824/782573>.

_____. 2024. *ENISA Threat Landscape 2024*. Heraklion: ENISA.

European Council. 2023. "Joint Declaration on EU-NATO Cooperation." 10 January 2023.

European Parliament / European Commission. 2024. *Investigation of digital platforms concerning electoral integrity in the context of the European elections of June 2024 (DSA proceedings)*. Brussels: European Parliament. <https://www.europarl.europa.eu/news/en/press-room>.

European Union. 2022a. "Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)." Official Journal of the European Union L 333: 80-152.

_____. 2022b. "Directive (EU) 2022/2557 on the resilience of critical entities (CER)." Official Journal of the European Union L 333: 164-198.

European Union. 2024. "Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (CRA)." Official Journal of the European Union L.

Fiott, Daniel, and Raluca Parreira. 2020. *Protecting Europe: The EU's Response to Hybrid Threats*. Chaillot Paper No. 151. Paris: EU Institute for Security Studies.

- Foreign Policy Research Institute (FPRI).** 2024. *Romania's Electoral Crisis: A Blueprint for Defending Democracy*. Philadelphia: FPRI.
- Fridman, Ofer.** 2018. *Russian Hybrid Warfare: Resurgence and Politicisation*. London: Hurst. <https://doi.org/10.1093/oso/9780190877095.001.0001>.
- Galeotti, Mark.** 2018. *I'm Sorry for Creating the Gerasimov Doctrine*. Foreign Policy, 5 March 2018.
- Gerasimov, Valery.** 2013. "Tsennost' nauki v predvidenii [The Value of Science in Anticipation, translated by Robert Coalson]." *Voenno-promyshlennyyi kur'er* 8 (476): 1-3.
- Giannopoulos, Georgios, Helen Smith, and Marianthi Theodoridou.** 2021. *The Landscape of Hybrid Threats: A Conceptual Model*. Luxembourg: Publications Office of the European Union. <https://doi.org/10.2760/019854>.
- Gioe, David V., Michael S. Goodman, and David Omand (eds.).** 2022. *The Routledge Companion to Intelligence Studies*. London: Routledge.
- Government Decision no. 963/2022** on the approval of the Cybersecurity Strategy of Romania 2022-2027. Official Gazette of Romania, Part I, no. 1029, 19 October 2022.
- Gressel, Gustav.** 2022. *Armies of Russia's War in Ukraine*. London: European Council on Foreign Relations. <https://ecfr.eu/publication/armies-of-russias-war-in-ukraine/>.
- Hoffman, Frank G.** 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies.
- IISS (International Institute for Strategic Studies).** 2023. *The Military Balance 2023*. London: Routledge / IISS.
- _____. 2024. *The Military Balance 2024*. London: Routledge / IISS.
- ITU (International Telecommunication Union).** 2024. *Global Cybersecurity Index 2024*. 5th ed. Geneva: ITU. <https://www.itu.int/hub/publication/d-hdb-gci-01-2024/>.
- JOIN(2016)18. European Commission and High Representative of the Union.** 2016. "Joint Framework on countering hybrid threats: a European Union response. JOIN(2016)18 final." Brussels: European Commission. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2016:18:FIN>.
- Lanoszka, Alexander.** 2016. "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe." *International Affairs* 92 (1): 175-195.
- Mandiant.** 2023. *Industroyer2: Industroyer Reloaded. Technical report*. Reston: Mandiant / Google Cloud. <https://www.mandiant.com/resources/reports/industroyer2-industroyer-reloaded>.
- Meydan, Timur.** 2022. "Hybrid Warfare and the Changing Nature of Conflict: Implications for NATO's Deterrence Posture." *Journal of Strategic Studies* 45 (5): 721-748. <https://doi.org/10.1080/01402390.2021.1972484>.
- Mumford, Andrew.** 2013. *Proxy Warfare*. Cambridge: Polity Press.

- NATO. 2022. *NATO 2022 Strategic Concept*. Adopted at the Madrid Summit, 29-30 June 2022. Brussels: NATO.
- OECD (Organisation for Economic Co-operation and Development). 2024. *AI Incidents Monitor: Case Study - Romanian Presidential Elections 2024*. Paris: OECD. <https://oecd.ai/en/incidents>.
- Ottis, Rain. 2008. *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Tallinn: CCDCOE.
- Pamment, James, Howard Nothhaft, Henrik Agardh-Twetman, and Alicia Fjallhed. 2018. *Countering Information Influence Activities: A Handbook for Communicators*. Lund: Lund University.
- Presidential Administration of Romania. 2020. "National Defence Strategy for the period 2020-2024." Bucharest: Presidential Administration.
- _____. 2025. "National Defence Strategy for the period 2025-2030." Bucharest: Presidential Administration.
- Renz, Bettina. 2016. "Russia and Hybrid Warfare." *Contemporary Politics* 22 (3): 283-300.
- Reuters. 2025. "Baltic Sea Underwater Infrastructure: Timeline of Incidents 2023-2025." *Reuters*. <https://www.reuters.com/world/europe/baltic-sea-cable-damage-timeline-2025-01/>.
- Rosenthal, Uriel, Arjen Boin, and Louise K. Comfort (eds.). 2001. *Managing Crises: Threats, Dilemmas, Opportunities*. Springfield, IL: Charles C Thomas.
- Schmitt, Michael N. (ed.). 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.
- SRI (Romanian Intelligence Service). 2023. *Activity report: 2023*. Bucharest: SRI.
- _____. 2024. *Report on hybrid threats to the electoral process in Romania (2024)*. Bucharest: SRI.
- Strachan-Morris, David. 2022. "Understanding Hybrid Warfare: Lessons for Intelligence Analysis." *Intelligence and National Security* 37 (3): 389-405. <https://doi.org/10.1080/2684527.2021.2016672>.
- StratCom COE. 2019. *Hybrid Threats: 2007 Cyber Attacks on Estonia*. Riga: NATO Strategic Communications Centre of Excellence. <https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86>.
- Thomas, Timothy. 2016. "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and Ambiguous Warfare." *Journal of Slavic Military Studies* 29 (1): 147-174.
- Tikk, Eneken, Kadri Kaska, Kristel Runnimeri, Mari Kert, Anna-Maria Taliharma, and Liis Vihul. 2008. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Tallinn: CCDCOE.
- Walker, Christopher. 2018. "What Is Sharp Power?" *Journal of Democracy* 29 (3): 9-23. <https://doi.org/10.1353/jod.2018.0041>.

- Warden, John A.** 1995. "Enemy as a System." *Airpower Journal* 9 (1): 40-55.
- Wilner, Alex S.** 2020. "US Cyber Deterrence: Practice Guiding Theory." *Journal of Strategic Studies* 43 (2): 245-280. <https://doi.org/10.1080/01402390.2018.1563779>.
- Yin, Robert K.** 2018. *Case Study Research and Applications: Design and Methods*. 6th ed. Thousand Oaks: SAGE.



EDITOR

„Carol I” National Defence University Publishing House
(Publishing house with recognized prestige validated
by the National Council for Attestation of University
Degrees, Diplomas and Certificates)
Address: Panduri Street, no. 68-72, Bucharest, 5th District
e-mail: buletinul@unap.ro
Phone: +4021.319.48.80 / 0365; 0453



Signature for the press: 30.06.2026
The publication consists of 312 pages.